Kiberdiplomácia

Szerkesztette
Molnár Anna és Molnár Dóra

LUDOVIKA
EGYETEMI KIADÓ

Kiberdiplomácia

Kiberdiplomácia

Szerkesztők
Molnár Anna
Molnár Dóra

LUDOVIKA
EGYETEMI KIADÓ
Budapest, 2022

A kutatás az Innovációs és Technológiai Minisztérium mint Támogató által
a TUDFO/51757-1/2019-ITM iktatószámon meghozott támogatói döntése alapján,
az NKFIH-830-8/2019. számú Megállapodásban foglaltak szerint, a 2019. évi
Tématerületi Kiválósági Program céljainak elérése érdekében költségvetési támogatásból
valósult meg.

Szerzők
Mártonffy Balázs
Molnár Anna
Molnár Dóra
Nyáry Gábor

Szakmai lektor
Prof. em. Dr. Gazdag Ferenc

Kiadja a Nemzeti Közszolgálati Egyetem
Ludovika Egyetemi Kiadó
A kiadásért felel: Deli Gergely rektor

Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: kiadvanyok@uni-nke.hu

Felelős szerkesztő: Karácsony Fanni
Olvasószerkesztő: Tomka Eszter
Korrektor: Pokorádi Zsófia
Tördelőszerkesztő: Kőrösi László

Nyomdai kivitelezés: Pátria Nyomda Zrt.
Felelős vezető: Orgován Katalin vezérigazgató

DOI: https://doi.org/10.36250/01008_00

ISBN 978-963-531-649-6 (nyomtatott)
ISBN 978-963-531-650-2 (elektronikus PDF) | ISBN 978-963-531-651-9 (ePub)

Tartalom

Molnár Dóra

Előszó

A kötet már címében is jelzi, hogy a változó világ hogyan ötvözi a régmúlt hagyományait a modern kor vívmányaival. Míg a diplomáciának hosszú évszázadokra visszanyúló hagyományai vannak, addig a „kiber" fogalom valódi tartalommal való megtöltésére a 21. századig várni kellett.

A kötet betekintést nyújt a kiberdiplomácia alapjaiba. Rávilágít az olyan alapvető, a kérdéskör megértéséhez elengedhetetlenül szükséges fogalmak közötti különbségekre, mint a kiberdiplomácia, a digitális diplomácia vagy az e-diplomácia. Elemzi az Európai Unió kiberdiplomáciai lépéseinek elméleti hátterét, és felfedi az egyes uniós lépések mögötti mozgatórugókat is. A nemzetközi élet legfontosabb szereplői közé azonban az államok tartoznak, ezért mindenképp szükséges néhány állami kiberdiplomáciai gyakorlatot ismertetni. Az olvasó részletesen megismerkedhet a három nagyhatalom kiberpolitikájának alapjaival, valamint a három vezető európai állam utóbbi években elért kiberdiplomáciai eredményeivel is. Köztudott, hogy a biztonság egyes szektorai szorosan kapcsolódnak egymáshoz – így a kiberbiztonság is elválaszthatatlan a politikai, gazdasági, katonai, társadalmi és más szektoroktól. Tekintettel arra, hogy valamennyi kiberdiplomáciai lépés mögött tetten érhetők a gazdasági érdekek, a kötet külön kitér a külgazdasági kapcsolatok kiberdiplomáciai vonatkozásaira, valamint olyan új típusú problémákat is felvillant, amelyek az adatbiztonsággal vagy a mesterséges intelligenciával kapcsolatosak.

A kötet hasznos olvasmány lehet nemcsak a területen jártas és a kiberbiztonság iránt érdeklődő szakközönség számára, hanem mindenkinek, aki a világ problémáit és a mögöttes mozgatórugókat szeretné megérteni, különösen ebben az új, ötödik geopolitikai dimenzióban.

[Vákát oldal]

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.

Nyáry Gábor

Kiberdiplomácia: hatalom, politika és technológia a geopolitika ötödik dimenziójában

Bevezetés[1]

Kiberháború, kiberbűnözés, kiberelrettentés: a szaksajtó és a közbeszéd felkapott, gyakran használt szavai és fogalmai lettek. A kibertér, ez a nehezen meghatározható, de mindenütt ott érzett közeg hovatovább az állandó konfrontáció, de legalábbis a mindig ott lebegő fenyegetés egyfajta szinonimájaként jelenik meg gondolatvilágunkban. A technicizálódó társadalmakban a konfliktusok (legyenek azok akár személyköziek, vagy a másik végletben, államok közöttiek) lassan betöltik a kiberteret. Pontosíthatunk: a kiberteret *is*. Hiszen az elmúlt két-három évtized egyik leginkább érezhető jelensége a feszültségek és összecsapások szaporodása és erősödése. Megjelent, vagyis inkább újra megjelent egy kifejezés, amely a politológia és az újságírás világában legalább annyira közkedveltté és agyonhasználttá vált, mint a „kibertér" a technikai, informatikai szakbeszédben. Ez a „geopolitika". Képlékeny, de valahogy mindenki által „érzett" tartalmú, jelentésű kifejezés. A környezet, a földrajzi tér jelentőségét hangsúlyozza az államok életében. Arra utal, hogy a környező nagyvilágban ismét előtérbe került az érdekek leplezetlen, néha egyenesen könyörtelen érvényesítése. Majd e két kifejezés összekapaszkodott, és újabb szóösszetétel for-

[1] A kibertérrel, a virtuális világ geopolitikai összefüggéseivel, az informatikai biztonság és a gazdaság intim kapcsolódásával rendkívül használható, jó áttekintést adó forrás áll az érdeklődők és kutatók rendelkezésére magyar nyelven is: Pintér István (szerk.): *Műhelymunkák. A virtuális tér geopolitikája. 2016/1.* Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016. Ugyanakkor a kibervédelem, kiberdiplomácia és az internetgazdaság metszéspontjának egyes részkérdéseire szinte enciklopédikus segédkönyvként használható Christopher Whyte – Brian Mazanec: *Understanding Cyber Warfare: Politics, Policy and Strategy* (New York, Routledge, 2019) a későbbiekben még idézett monográfiája. A kibertér geopolitikájának, hatalmi rendszereinek, védelmi problémáinak és technológiai modernizációjának friss szemléletű elméletalkotó „mesterműve" is jó bevezetést adhat: P. J. Blount: *Reprogramming the World. Cyberspace and the Geography of Global Order.* Bristol, E-International Relations Publishing, 2019.

https://doi.org/10.36250/01008_02

májában lendületet kapott: beszélünk már, mert okkal beszélhetünk, a „kibertér geopolitikájáról". Ebben a körbepillantásban fontos szerepet kap majd egy új keletű pozíció (talán hivatal, vagy már lassan egyenesen önálló szakma): a kiberdiplomatáé. Mert az egyik legfontosabb mondandónk az lenne, hogy a világháló szövevényes útjait, drótjait, számítógépeit, az azokon futó programokat és persze a velük dolgozó vagy játszó embereket felölelő „kibervilág" korántsem csak a kiberharcosok, hackerek, kiberbűnözők élettere. Konfliktusok persze gyakran támadnak ebben a még kialakulófélben levő, és ezért néha rendezetlen és szabályozatlan térben. Éppen ezek megoldásán, elsimításán, szabályozásán dolgoznak a kiberdiplomácia szakemberei.

A geopolitika beköszön a kibertérbe

A „geopolitika" napjaink egyik legtöbbet emlegetett szava, és ennek megfelelően képlékeny a jelentéstartalma és használata is.[2] Sokszor egyszerűen csak a „hatalmi politika", a „külpolitikai érdekérvényesítés" szinonimájaként használják. Hosszú időn át, a 20. század második felében, lényegében szalonképtelenné vált éppen e felfogás miatt: a szakmai közvélekedés a század első felének autoriter rendszereit megalapozó (egyik) elméletet látta benne, ezért a geopolitika koncepciója, fogalma, szóhasználata jó időre feledésbe merült.[3] Valójában használatának – a pontos jelentéstartalmaktól csaknem függetlenül – közös jellegzetessége az a felismerés, hogy a 2000-es évek eleje óta valami érezhetően megváltozott a nemzetközi kapcsolatokban: mintha addig csendben meghúzódó szereplők hirtelen a színpadra pattantak volna, hogy nagyon is aktív játékba kezdjenek.[4] És valóban: a hidegháború hosszú és külpolitikai szempontból meglehetősen világos és egyértelmű évtizedei után az 1990-es évek elejétől a szinte meglepetésre, „ajándékba kapott" amerikai hegemónia teremtett állóvizet a külkapcsolatok világában. Ez volt az „unipoláris pillanat", az a szűk évtized, amikor az országok

[2] A geopolitika egyik legjobban használható, sok szempontot és megközelítést felvillantó alapmunkájának továbbra is Saul Bernard Cohen: *Geopolitics: The Geography of International Relations* (Lanham, Rowman and Littlefield, 2015) című munkája tekinthető.

[3] Furcsa paradoxonként egy olyan korszakban, az ún. hidegháború időszakában, amikor a hatalmi politizálás cseppet sem „ment ki a divatból", ellenkezőleg: az egész korszakot a hatalmi szembenállás határozta meg.

[4] A kifejezés a legendás amerikai politikus, Zbigniew Brzezinski könyvcíme nyomán vált közismertté. Zbigniew Brzezinski: *A nagy sakktábla*. Budapest, Európa, 1999.

viszonyrendszerében lényegében egyetlen hatalom, az USA diktált, és mindenki más igazodott. A helyzet nem volt túl szép – viszont egyszerű és egyértelmű volt. A 21. század első évtizedének végére azonban már tagadhatatlan tényként látszott ennek a rendnek a felbomlása, az új, multipoláris világ egyre gyorsabb formálódása. Nem csupán Oroszország és Kína lépett (újra) a nagyhatalmi politizálás porondjára; középhatalmak, India, Törökország, az EU, sőt kisebb államok is egyre aktívabb szereplőként tűntek fel a nemzetközi küzdőtéren. Fő szabálynak a szabálynélküliség, az igazodási pontok sokasága látszik. A nemzeti érdekérvényesítés sokszor kaotikusnak látszó, aktív korszakára mondják: visszatért a geopolitika.[5]

A földrajz bosszúja

A korábbi évtizedek elvi alapú, ideológiai szempontok alapján szerveződő nemzetközi kapcsolatait felváltotta az egyes nemzetek érdekeire koncentráló, „önző" érdekérvényesítés politikája.[6] Szigorúbban véve a kifejezés arra utal, hogy a nemzetek egymás közötti viszonyát, érdekérvényesítési mozgásait nagymértékben befolyásolják bizonyos hosszú távon állandó struktúrák. Elsősorban persze maga a környezet, a fizikai tér: az ország elhelyezkedése, domborzati viszonyai, vízrajza, népesedésföldrajza (benne a népesség nagysága és demográfiai mozgásai).[7] Érdemes persze elgondolkodni azon is, hogy a korábbi bő hetven év nagy ideológiái, az amerikai „szabadságeszme", majd „az emberi jogok", vagy a Szovjetunió „egyenlőség és igazságosság" ideája, „népek felszabadítása" külpolitikai narratívája mögött is alapvető nemzeti érdekek húzódtak meg; a tartós

[5] Merje Kuus: *Geopolitics Reframed. Security and Identity in Europe's Eastern Enlargement.* New York, Palgrave MacMillan, 2007.

[6] A „pőre" nemzeti érdekeket érvényesítő külpolitikai gondolkodás legjelentősebb alakjának tekinthető amerikai Henry Kissinger hatásosan foglalja össze a világrendszer „tektonikus" átalakulását egyik fő művében: Henry Kissinger: *Világrend*. Budapest, Antall József Tudásközpont, 2016. A nemzeti érdekek kölcsönös felismerésén és elismerésén alapuló külpolitizálás mint a nagyhatalmi konfrontáció elkerülésének eszköze jelenik meg a volt amerikai külügyminiszter gondolkodásában. *„The Key Problem of Our Time": A Conversation with Henry Kissinger on Sino-U.S. Relations* (2018).

[7] A földrajzi tér erejét, meghatározó szerepét felismerő külkapcsolati felfogás egyik kiváló összefoglalóját adja az ismert amerikai külpolitikai elemző, Robert D. Kaplan: *A földrajz bosszúja* (Budapest, Antall József Tudásközpont, 2019) című monográfiája; e fejezet fő gondolatát is innét kölcsönöztük.

önérdek-érvényesítés értelmében felfogható „geopolitika" tehát valójában sohasem tűnt el, legfeljebb diszkréten meghúzódott a háttérben. Az igazi újdonság mostani korunkban: az érdekek immár nyílt megfogalmazása, az aktív szereplők sokasága és a nemzeti érdekérvényesítési küzdelem dimenzióinak bővülése. Ugyanakkor így már jól láthatóvá válik a „geopolitika" egy másik fontos jellegzetessége: a koncepció alapvetően látásmódot, tudományos megközelítést, vizsgálati módszert takar.[8] Olyat, ami a nemzetek közötti kapcsolódás, viszonyulás egyik (vagy éppen legfontosabb) meghatározójának tekinti a térbeliséget, illetve a fogalmat szélesebben értelmezve, a fizikai környezet tényezőit.[9] A politikai nyelvben, a közbeszédben polgárjogot nyert, gyakorta használt frappáns megfogalmazás a földrajz „bosszújáról" arra utal, hogy tévesnek bizonyultak azok a külpolitika-elméletek, amelyek – különösen az 1989–1991-es esztendők, tehát az addigi kétpólusú világ hirtelen lebomlása után – úgy vélték, hogy az államok földrajzi elhelyezkedésében, fizikai adottságaiban (és ezek történeti dinamikájában) gyökerező érdekalapú külpolitizálást felváltja egy idealisztikusabb alapokon – az emberi jogok univerzális érvényesülésén, általában a jogállamiságon nyugvó – kapcsolatrendszer. A fizikai környezet hosszú távú elemei és tényezői szívósabbnak bizonyultak, és „visszatértek" a nemzetközi viszonyok alakításába.

A viszonyok és felfogások gyorsuló ütemű, jelentős átalakulására példa az Európai Unió hivatalos külpolitikai koncepciójának átformálódása. A 2019-ben hivatalba lépett új vezető testület, az Európai Bizottság nagy feltűnést keltett a nemzetközi kapcsolatok alakítására vonatkozó koncepciójával, az aktív uniós külpolitizálás elveinek megfogalmazásával. A Bizottság elnöke, Ursula von der Leyen szóhasználata a „geopolitikus EU"-ról[10] meghökkenést (sőt néhol egyene-

[8] Szilágyi István: *A geopolitika elmélete* (Budapest, Pallas Athéné, 2018) a magyar nyelven elérhető talán legjobb áttekintése a geopolitika mint tudományos diszciplína felfogásának.

[9] Élénk vita zajlott és zajlik a mai napig arról, hogy jogos-e a fizikai-földrajzi környezet ilyen *determináló* szerepét feltételezni a nemzetközi kapcsolatok alakításában. A koncepció használhatósága mellett kiállók azzal érvelnek, hogy a fizikai-földrajzi környezet hosszú távú, strukturálisan meghatározó szerepe nem azonos egy determinisztikus felfogással. A viszonyok aktuális alakításába más tényezők (illetve rövidebb élettartamú társadalmi-politikai struktúrák) is beleszólnak. A koncepció egyébként a történettudományban, a 20. század második harmadát meghatározó francia Annales-iskola követőinek munkásságában kapott széles és nagy ívű társadalmi megalapozottságot. Vö. Fernand Braudel „hosszú időtartam" *(longue durée)* elméletével.

[10] Etienne Bassot: *The von der Leyen Commission's priorities for 2019–2024*. 2020.

sen megdöbbenést) váltott ki,[11] hiszen ez a fogalom az alapvetően a multilateralizmus elveire építő európai közösség vezető tisztviselőjétől (ráadásul éppen egy német politikus szájából[12]) egyenesen istenkáromlásnak hathatott. A politikus (aki egészen pontosan „geopolitikus Európai Bizottságot" ígért beiktatásakor) láthatóan új, dinamikusabb szerepet szánt a sokak által nehezen mozgó, erőtlen külpolitikai aktornak látszó uniónak.[13] Az európai vezetés koncepciójának elmozdulását különösen jól jelezte az unió másik meghatározó politikusának, Josep Borellnek e témában közreadott dolgozata, amely eloszlatott minden kételyt afelől, hogy az európai politikai beszédbe visszakerült „geopolitika" valójában hogyan értendő. Az EU külügyi és biztonságpolitikai főképviselője (azaz az unió külügyi szervezetének irányítója, de facto „külügyminisztere") megkerülhetetlen külpolitikai stratégia, sőt valójában külpolitikai filozófiaváltás szükségességéről beszélt. Eredetileg az EU alapvető céljaként, létrehozásának értelmeként a hatalmi politizálás eltörlése, a multilateralizmus, a nyíltság és a kölcsönösség elvein alapuló együttműködési rendszer kiépítése szerepelt. Mára azonban a világ megváltozott. Régi és új, felemelkedő hatalmak rivalizálnak egymással is az elsőségért. Borell leszögezte: Európának szemléletváltásra van szüksége. Ha a kontinens nem akarja az elsőségért vetélkedő USA és Kína közé szorulva vesztesként végezni, akkor bizony „meg kell tanulnia az erő nyelvén beszélni".[14] Ennél világosabban kevesen fogalmazták meg a „geopolitikai Európai Bizottság, a geopolitikus Európa" közkeletű értelmét, jelentéstartalmát.

[11] Az európai szakmai-politikai eliteken belüli erős ellenkezésre több fajsúlyos megszólalás is világosan utal. Marius Müller-Hennig: *A Truly Geopolitical EU Commission? Rather than Playing Geopolitical Games Itself, von der Leyen's Commission Should Be Critical of the Very Notion of Geopolitics.* 2019.

[12] A klasszikus geopolitika egyik jelentős gondolkodója, a német Friedrich Ratzel a közkeletű (ám sokak által vitatott) felfogás szerint munkásságával a náci Németország ideológiájához járulhatott hozzá.

[13] Az unió külpolitikai teljesítményének ellentmondásosságát jól összegzi Stefan Lehne: *Is There Hope for EU Foreign Policy?* Brussels, Carnegie Endowment, 2017. A szakmai közvélekedést azonban a legkíméletlenebb pontossággal talán maga az EU foglalja össze: „[Az EU-t] multilaterális szinten általában pozitív, de ineffektív szereplőnek tekintik. Bilaterális kapcsolataiban pedig olyan aktorként érzékelik, amelyből hiányzik a koherencia." *A Global Actor in Search of a Strategy. European Union Foreign Policy between Multilateralism and Bilateralism.* 2014.

[14] Josep Borell: *HR/VP Josep Borell: Embracing 'Geopolitical' Europe's Power.* Amihez a politikus hozzátette: Európából eddig sem az erő hiányzott, hanem a politikai akarat, hogy ezt az erőt érvényesítse a nemzetközi porondon.

Kibertér: a nemzeti érdekérvényesítés 5. dimenziója

A politika és a szaktudományok sokszor elméleti vitáit félretéve jól látható, hogy a földrajzi tér alapvető kiterjedései, a szárazföldek és vizek ősidőktől az államok közötti érdekérvényesítési küzdelmek állandó színterei. A 20. század első harmadától felzárkózott melléjük a levegő, majd a hidegháború korszakában az űr dimenziója is. A 21. század újdonságaként ez a sokrétű geopolitikai világ kibővült egy újabb aspektussal, egy vadonatúj versengési területtel. A formálódó kibertér lett a geopolitikai szembenállás, érdekérvényesítés ötödik dimenziója.[15] Az informatika, a számítógépes hálózatok, mobiltechnológiák rohamos fejlődése szülte ezt az új „érdekmezőt", ebben az értelemben tehát tényleg ízig-vérig korunk terméke. Mint annyi fogalom, a „kibertér" is sok értelmezést, értelmezési árnyalatot takar.

Maga a kifejezés nem új keletű: William Gibson íróhoz kötődik, aki egy 1982-ben kiadott novellájában használta első ízben ezt a fordulatot, egy számítógép által kreált virtuális valóságmező bemutatására. Igazi népszerűségre azonban 1984-ben tett szert, a szerző következő, *Neuromancer* című novellája révén. Azóta természetesen a kifejezés kilépett az irodalom képzeletbeli mátrixvilágából, és ma már a tudomány tereinek egyik elfogadott kifejezése. Közkeletű szakmai használatában lényegében az internet (és hasonló technológiák) világot körbefonó számítógépes hálózatainak szinonimájaként a leggyakoribb talán. Az információs és kommunikációtechnológiák (IKT) virtuális univerzumának egyfajta metaforája, ami egyre inkább kezdi felváltani az internetre korábban elterjedt (és különösen a politikusok által előszeretettel használt) információs szupersztráda metaforát.[16] Itt érdemes kiemelni azt a mozzanatot, amely már a „sima" geopolitika térkoncepciójánál sem hagyható figyelmen kívül: a terek nem valami merev, mozdulatlan, statikus létezők, hanem ellenkezőleg: állandó mozgásban, folytonos változásban lévő dinamikus viszonyrendszerek, amelyek állandó kölcsönhatásban állnak csatlakozó (társadalmi) komponenseikkel.[17]

[15] A kibertér geopolitikai jellegének egyik első megfogalmazását Szilágyi István: *A geopolitika elmélete* című kiváló munkája adja.

[16] Vasillys Fourkas: What is 'cyberspace'? *Media Development* 3. (2004), 6–7. Az így meggyökeresedett kifejezés mellett egyébként még több ilyen metafora született az IKT-jelenségkör egy-egy fontos mozzanatának köznyelvi megragadására: például közismert a digitális „könyvtár", az elektronikus „posta" vagy a virtuális „piactér", hogy csak a leggyakrabban használtakat idézzük fel.

[17] Ez az a fontos, sőt meghatározó jellegzetesség, amelyet a geopolitika fogalomrendszerének kritikusai figyelmen kívül hagynak, amikor a geopolitikai megközelítésmódot egyfajta merev (térbeli) determinizmussal vádolják.

A kibertér „térbeli" mivoltával kapcsolatban a szakirodalom nem egységes. Egyes szerzők, különösen a kiberhadviselés problematikájával foglalkozó stratégiatudományi szakértők a sokdimenziós geopolitikai közeg fokozatos (és egyre gyorsuló) virtualizálódásáról beszélnek. E szerint a hagyományos tereket a csupán átvitt értelemben létező, konkrét alakot nélkülöző tér, egyfajta „térnélküliség" váltja a geopolitika összefüggésrendszerében, éppen a kibertér mint 5. geopolitikai dimenzió előtérbe kerülésével.[18] Olyannyira, hogy a stratégiatudományok egyik legelismertebb kortárs képviselője, az amerikai Colin Gray egyenesen „ellenföldrajzi" kiterjedésű térként definiálja, ezzel is hangsúlyozva a kibertér megfoghatatlan, képlékeny valóságát.

Másfelől viszont a kiberkomplexum technológiai aspektusaival vagy a digitalizáció társadalmi összefüggéseivel foglalkozó kutatóknál hangsúlyosan merül fel a kibertér térjellege, azaz nagyon is valóságos, fizikai térstruktúrákhoz integránsan kapcsolódó mivolta. Ebben a felfogásban a kibertérfogalom térbelisége különböző szinteken jelenik meg. Szokás ezzel kapcsolatban legalább három ilyen térbeli jelentésréteget lehámozni. A fogalomnak elsőként is van egy technikai jelentésszintje, amely a kibertérnek nevezett fogalom együttes technológiai infrastruktúráját írja le. A fogalomnak van ugyanakkor egy tényleges földrajzi jelentésrétege is, amely az IKT-hálózatokat és azok csomópontjainak valóságos térbeni kiterjedését öleli fel. A fogalom ugyanakkor tartalmaz egy harmadik, társadalmi jelentésréteget is, amely az IKT-hálózatokat használó emberek térbeli szerveződéseit írja körül. A fentiekből látható tehát, hogy a kibertér, ez a sokszor virtuálisnak nevezett világ nagyon is valóságos (nem csupán metaforikusan értelmezhető) térbeliséggel rendelkezik. Kijelenthető, hogy a „kibertér" valóságos térbeli rendszer: a hálózati topológiája alapvetően függ annak térbeli rögzületeitől, és fejlődését is döntően a rendszerkörnyezet gazdasági és technológiai fejlődésének földrajza befolyásolja.

Összegezve tehát: nagyjából közös fogalmi keretként úgy tekinthetünk a kibertérre, mint az internet, a számítástechnikai eszközök, a rajtuk futó szoftverek, sőt az őket használó, mindinkább hálózatokba szerveződő alkalmazók összességére. Alapvető jellegzetessége, hogy kezdetben merőben technikai problématerületként tűnt fel, mára azonban egyértelműen egy, a politikum által hatalmába kerített térré változott, ahol eltérő (nemzeti) érdekek, eltérő normák és eltérő értékek formálják a viszonyokat. Ma már nem sokan vonnák kétségbe, hogy ez a kibertér a geopolitikai érdekérvényesítés egyik dimenziója, éppen úgy,

[18] Szilágyi (2018): i. m.

mint a szárazföldek, a tengerek, a levegő vagy az űr. Sőt ma már abban is egyre nagyobb a konszenzus, hogy a nemzetek közötti érdekellentéteknek és érdekérvényesítésnek a kibertér nem csupán egyik dimenziója, hanem „a" meghatározó színtere.[19]

Geopolitikai mozgások a kibertérben

A geopolitika fogalmi rendszerének általános bemutatásánál utaltunk rá, hogy a 2010-es évtized egyértelmű fejleménye a rendszerváltásokat követő Amerika-központú, unilaterális világrend felbomlása. Tudósok és politikai szakértők egyre gyakrabban említik az így kialakulóban lévő szisztémát egyfajta multipoláris világrendként.[20] Érdemes azonban hangsúlyozni, hogy a hidegháború időszakára jellemző klasszikus (egyfelől az USA, másfelől a Szovjetunió köré épülő) bipolaritás valóban nem tekinthető jellemzőnek napjainkra, és ebben az értelemben indokolt egyfajta multipoláris világrend-szerveződésről beszélni.[21] A nemzetközi tér eseményei azonban egyre inkább abba az irányba fordulnak, hogy a nemzetközi kapcsolati tér meghatározó szervező erejévé a majd' három évtizede globális hegemónként vezető Egyesült Államok és a vezető szerepért immár egyértelműen bejelentkezett Kínai Népköztársaság közötti rivalizálás válik.

Az USA és Kína közötti stratégiai jellegű geopolitikai vetélkedés (ahogy természetesen a többi nagy- és regionális hatalom közötti geopolitikai rivalizálás is) egy „megvalósítási eszközskála mentén" több különálló, de egységes rendszerbe kapcsolódó, és egyre gyakrabban formálisan is jórészt összemosódó eszközt

[19] Alix Desforges: Representations of Cyberspace: A Geopolitical Tool. *Hérodote,* 152–153. (2014), 1–2. 67–81., továbbá a kibertér, a földrajz és a hatalmi politika modern kapcsolódási rendszereire az egyik vitathatatlanul legérdekesebb, mostanában napvilágot látott munka Blount (2019) kötete.

[20] Alapos, rendszeres áttekintését adja a hatalompolitikai átrendeződés folyamatának és következményeinek az Európai Parlament kutatószolgálata által kiadott *Global Trends to 2035. Geo-politics and International Power,* 2017. Hasonlóan jó összefoglalót ad Megan Dee: *The European Union in a Multipolar World. World Trade, Global Governance and the Case of the WTO* (London, Palgrave MacMillan, 2015) is.

[21] Amit egy némileg cinikus, de a valóságtól néha nem túl távol álló megfogalmazással úgy jellemeznek, hogy amíg a bipoláris világban a két szemben álló nagyhatalom köré tömörült államok szövetségi rendszerei néztek egymással farkasszemet, addig a multipoláris világban inkább a „mindenki mindenki farkasa".

használ a valós (vagy annak vélt) nemzeti érdekek külvilágbeli érvényesítésére. A lehetőségek tárházából még ma is gyakorta veszik elő az államok a háború (vagy talán pontosabb: a fegyveres erőszak) eszközét. Az utóbbi évtized fejleményei azonban azt mutatják, hogy már ez az előbbi pontosítás sem írja le elég hűséggel a valóságot. A kibertér „geopolitizálódásával" párhuzamosan ugyanis éppen a hagyományos fegyvereken – és az azok által előidézett „kinetikus" összecsapásokon – alapuló külpolitikai érdekérvényesítés helyébe az erőszak új – fegyvertelen, de semmiképpen sem „békés" – eszközei lépnek.[22] Ez a kiberhadviselés, a kiberháborúk feljövő korszaka. A geopolitikai pozíciók megszerzésére vagy éppen azok megvédésére a megfelelő technológiai képességekkel rendelkező országok kiberhadviselési potenciálokat építenek ki.

A geopolitikai küzdelmek meghatározó szembenállásának tekinthető amerikai–kínai viszonylatban a két rivális fél mindegyike elkötelezte magát a kibertérben alkalmazható erőszakos érdekérvényesítő eszközök, rendszerek kifejlesztése, telepítése és alkalmazása mellett.[23] Szokás úgy fogalmazni, hogy ugyan kezdetben Kína és az USA más és más stratégiai keretrendszerben (Amerika alapvetően informatikai és egyéb infrastruktúráinak megóvása érdekében, tehát a védekezés céljával, míg Kína offenzív jelleggel) látott hozzá a kiberképességek kiépítéséhez, és ezért azok jellegükben is eltértek egymástól,[24] később mindkét hatalom támadóeszközökkel is felszerelt kiberarzenállal operál a nemzetközi kibertérben.[25] A 2010-es évtizedben (az előző évtizedek kezdeményezéseiből kinőve) gyorsított ütemben megkezdődött a kiberhadviseléssel foglalkozó, szakosított katonai szervezetek (operatív alakulatok és irányító parancsnokságok) kiépítése mindkét egymással versengő nagyhatalomnál. A kezdeti stratégiai különbségek a kapacitások kiépítésében is éreztették hatásukat: míg Kína kezdettől egysé-

[22] A téma, a nemzetközi kapcsolatok, illetve a külpolitika és a kibertér erősödő összefonódásának különösen jó áttekintését adja Nazil Choucri: *Cyberpolitics in International Relations.* Cambridge, MIT Press, 2012.

[23] A kínai szándékokra és képességekre lásd Jiang Tianjiao: From Offense Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar. *Chinese Journal of International Review,* 1. (2019), 2. 1–23. Az amerikai kiberstratégia katonai komponensére (ami nem azonos a szintén abban az évben publikált amerikai Nemzeti Kiberstratégiával!): *US Department of Defense Cyber Strategy 2018* (2018).

[24] Francis C. Domingo: Conquering a New Domain: Explaining Great Oower Competition in Cyberspace. *Comparative Strategy*, 35. (2016), 2. 154–168.

[25] Azaz az amerikai kiberstratégiában is (annak radikális átszabása nyomán) megjelent az infrastruktúra-védelem prioritása mellett a kibertérben biztosítandó katonai erőfölény megszerzésének célja is.

ges irányítás alatt szervezte meg támadó és védekező kiberképességeit, addig az Egyesült Államok csak számos szervezeti kísérletezés nyomán, az évtized végére jutott el a hasonlóan hatékony kiberhadviselési struktúrák kialakításáig.[26] A kibertérben zajló katonai akciókról – azok jellegénél fogva – kevés megbízható információ lelhető fel a szabadon hozzáférhető (nyílt) irodalomban. Érdekességként megemlíthetjük, hogy a kibertérben végrehajtott hadviselési műveletek jóval régebbiek, mint azt gondolhatnánk: az első (nyilvánosságra került) ilyen akció a hidegháború időszakába vezet vissza, a szovjet transzszibériai gázvezeték vezérlőrendszerei elleni kiberműveletig.[27] Jellemző szakmai vélekedésnek látszik ugyanakkor, hogy az ezredfordulótól sokasodó katonai akciókban a kínai kiberhadviselési alakulatok – miközben komoly, különösen kinetikus jellegű károkat nem okoztak – általában jól fedték fel az ellenfelek (elsősorban az USA) digitális hálózatainak, rendszereinek sérülékenységeit. Erre utaltak a 2010-es évtizedben az amerikai kormányzati rendszerek ellen sűrűsödő kínai támadások, amikor a cél többnyire érzékeny információk megszerzése volt.[28]

Az államok közötti kiberkonfliktusok (incidensek) négy fő kategóriába sorolhatók: az első a már említett információszerző műveletek csoportja. Célozhatják ugyanakkor a kiberakciók az ellenfél hálózatainak, rendszereinek megzavarását, lassítását, bénítását, elpusztítását. A kibertérben folytatott akciók szolgálhatják valamilyen, a szokásos katonai környezetben történő akció támogatását. És végül a kibertámadások célja lehet az ellenfél információs környezetének megzavarása, manipulálása.[29]

[26] Domingo (2016): i. m. 162. Míg Kína kezdettől a Kínai Népi Felszabadító Hadsereg vezérkarának Harmadik- és Negyedik Igazgatósága alá rendelve – egységes parancsnoki rendszerbe szervezve – építette kiberkapacitásait, addig az USA csupán a 2010-es évtized végére, a US Cyber Command (USCYBERCOM) felállításával érte el a kínaiakéhoz hasonló integrált vezetési és irányítási szervezetet.

[27] Az akcióra 1982-ben került sor, és állítólag a CIA állt a hadművelet hátterében, ami egy digitális kártevővel fertőzött szoftver révén tette tönkre a rendszer vezérlését. A beavatkozás egyébként kinetikus hatásokkal járt, kolosszális méretű gázrobbanást idézve elő. Whyte–Mazanec (2019): i. m.

[28] 2003 és 2012 között legalább hat jelentősebb – amerikai kormányzati célpontok elleni – támadást írnak a Kínai Népköztársaság számlájára, amiből kettő különösen veszélyesnek bizonyult. 2005: Titan Rat hadművelet, az amerikai Hadügyminisztérium, Külügyminisztérium és Belbiztonsági Minisztérium rendszerei ellen. 2009: Shady Rat hadművelet a Lockheed Martin, Northrop és BAE hadiipari beszállítók rendszerei ellen. A cél mindenhol titkos információk megszerzése volt. Domingo (2016): i. m. 162.

[29] Whyte–Mazanec (2019): i. m. 100.

Az elmúlt évtizedek kiberincidenseinek kronológiája és különösen a két versengő nagyhatalom kibertérbeli rivalizálásai alapján a kibervilágnak mint geopolitikai „hadszíntérnek" a következő jellegzetességei látszanak kirajzolódni. A proliferáció (a kiberhadviselésre alkalmas informatikai eszközök és eljárások elterjedése) nehezen látszik megállíthatónak. Ennek nyomán a (roppant hatékony, akár stratégiai csapásmérésre is alkalmas) kiberhadviselési képességek gyors ütemben terjednek majd a közepes hatalmak, de akár a kevésbé jelentős hatalmi szereplők körében is. Ugyanakkor azonban továbbra is a nagyhatalmak dominálják majd a kiberteret (is), mivel komplex, bonyolult támadások kivitelezésére továbbra is csak komoly technológiai háttérrel rendelkező országok képesek. Végül, különösen nyugtalanító fejleményként, a szakemberek elképzelhetőnek tartják, hogy a kibertámadások a csapások-ellencsapások eszkalálódásával valóságos („kinetikus") károkozássá fajulhatnak el.[30]

Diplomáciától a kiberdiplomáciáig

A geopolitika általános fogalmairól és kereteiről szólva említettük: a földrajz, domborzat, demográfia, történelem dinamikus rendszert alkotó terében létező államok vélt vagy valós nemzeti érdekeiket igyekeznek érvényesíteni. Néha (nem is olyan ritkán) egymás rovására, máskor egymással együttműködésben. Az előző fejezetrészben azt villantottuk fel, hogyan használják az államok (egy speciális dimenzióban, az úgynevezett kibertérben) az érdekeik érvényesítésére rendelkezésre álló *egyik* eszközkészletet: az erőszakot. A hangsúly itt most azon van, hogy ez az *egyik* lehetséges eszközrendszer. A paletta (vagy inkább egyfajta eszközskála) másik végén egy *másik,* szintén jól ismert eszközt találunk, a diplomáciát. A külpolitikát tehát sajátos cselekvési terepnek foghatjuk fel: egy állam sajátos nemzeti érdekeinek, értékeinek, céljainak érvényesítése, méghozzá egy (többnyire bonyolult) kapcsolatrendszerben. A külpolitika ugyanis mindig csak viszonyként értelmezhető: más, hasonló államokkal való interakcióban. A diplomácia tehát, fogalmaztuk meg kicsit magasabb szinten, a külpolitika érvényre juttatásának másik lehetséges eszközcsoportja. Olyan tevékenység, amelynek sajátos funkciói és hasonlóan egyedi eljárásai vannak. A hadviselésétől jócskán elütő eszközkészletét jellemzően a tárgyalás és a megegyezés alkotják. A kibertér mint geopolitikai struktúra vonatkozásában pedig sajátos válfaja,

[30] Domingo (2016): i. m. 166.

a kiberdiplomácia kap egyre inkább teret. Bizonyos értelemben azonban már maga a kifejezés is okozhat némi fejtörést a szemlélőnek.

A terminológia őserdejében

Ha az államigazgatás digitalizációja, úgy általában, ma még a fogalmi tisztázatlanságok jellegzetes terepe, akkor ez végképp igaz a diplomáciával kapcsolatos elnevezési helyzetre. A nemzetközi szakmai közbeszédben egyelőre szinte átláthatatlan, kaotikus örvénylésben kavarognak a külszolgálatok digitalizálását leírni kívánó konstrukciók: „kiberdiplomácia", „e-diplomácia", hogy a korábban leggyakoribb összetételeket idézzük, de ott van még az elmúlt fél évtized különösen kedvelt megfogalmazása, a „Twitter-diplomácia", más néven „közösségimédia-diplomácia" vagy „Facebook-diplomácia" elnevezése is. A sor pedig korántsem ért véget. Felbukkant már az „algoritmikus diplomácia" összetétel is, aztán gyakorta találkozhatunk a „technodiplomácia" fogalmával is, de bizonyos összefüggésekben előjön az „adatdiplomácia" szóösszetétel is. És persze létezik a „digitális diplomácia" kifejezés is, amely lassan, de biztosan kezd általános érvényű használatot kivívni magának.[31]

A fogalomhasználat áttekintése és elemzése nyomán a következő főbb megállapításokat tehetjük:

- A diplomáciai, nemzetközi kapcsolatokhoz kötődő IKT-fejlesztések leírására használt fogalomrendszer különböző elemei az esetek jelentős többségében csupán szinonimaként szerepelnek a szakmai közbeszédben is.
- Ebben a használati módban a kifejezések sokszor nyelvi divatciklusok szerint váltják, követik egymást (anélkül, hogy a kifejezések váltása mögött bármiféle komoly szemantikai szándék állna).

Ugyanakkor történtek már kezdeti lépések a fogalmak szisztematikus elemzésére, egy általánosan használható fogalmi háló kialakítására (a nyelvi-elméleti

[31] A diplomácia legutóbbi évtizedekben felgyorsuló fejlődésének problémáit lásd Cathryn Clüver Ashbrook: *21st Century Diplomacy.* 2014. A téma talán legelismertebb szakértője, az Oxfordban tanító román tudós, Corneliu Bjola írásai megkerülhetetlenek a technicizálódó külkapcsolatok és általában a 21. századi diplomácia tanulmányozásához. Corneliu Bjola: *Digital Diplomacy: From Tactics to Strategy*. é. n., valamint: Corneliu Bjola: Digital Diplomacy 2.0. Trends and Counter-Trends. *Revista Mexicana de Política Exterior,* (2018), 113. 35–52.

alapvetések általánossá válásának azonban továbbra sem lehetünk tanúi a szakirodalomban, még kevésbé a nyilvános közbeszédben).[32]

Szűkebb témánk, a kiberdiplomácia ismertetése előtt érdemes – a nemzetközi szakmai gondolkodás eredményeit figyelembe véve – a terminológia rendszerszerű tisztázására kísérletet tenni. Mielőtt azonban ezt röviden felvázoljuk, mindenképpen fontosnak tartjuk még egy további fogalmi kitérő bejárását is.

A diplomácia értelmezése és átértelmezése

Talán meglepő, de a külügyek IKT-fejlesztései témájában a nemzetközi szakmai közbeszédben szinte alig merül fel magának a diplomáciának a definíciós igénye. Miközben ezt tehát látszólag mindenki magától értetődőnek veszi, mi azt gondoljuk, hogy érdemes a jelenség tartalmának alaposabb vizsgálata. Ez szolgáltatja ugyanis azt a kontextust, amelyben a digitalizáció folyamatai, eszközei, megoldásai egyáltalán értelmezhetővé válnak. A szakma külföldi művelői általában így summáznak: „A digitális diplomácia vagy e-diplomácia az a terület, ahol a korszerű IKT-eszközrendszert mozgósítják egy állam külpolitikai céljainak szolgálatára."[33] Összefoglalónak megteszi, de mindenképpen érdemes egy kicsit a tartalmi mélységekbe is bepillantani. Meggyőződésünk, hogy a külügyek digitalizációját vizsgálva semmi sem visz minket közelebb a jelenségek megértéséhez, mint a „diplomácia" funkcionális vizsgálata. Ez a szemrevételezés ad ugyanis választ a hogyanokra és a holokra is. Hogyan (illetve pontosan melyik résztémában) szolgálja a diplomácia szervezete és folyamatrendszere egy állam külpolitikai céljainak érvényesítését? A megközelítés azért is érdekes és fontos,

[32] A diplomácia IKT-alapú átalakulásának fogalmi kereteivel legtöbbet két kiemelkedő szakmai műhelyhez köthető kutatók foglalkoztak. Kiemelkedő szerepet játszik az Oxford Digital Diplomacy Research Group, a másik fontos elméleti-fogalmi tisztázó munkát végző szakmai műhely pedig a Holland Külügyminisztérium háttérintézete, a híres Clingendael. Vö.: Corneliu Bjola: *Digital Diplomacy*. London – New York, Routledge, 2015. 71–89. Továbbá Jan Melissen: *Diplomacy in the Digital Age*. The Hague, Clingendael, é. n. 27–51.

[33] A fiatal generáció legkiemelkedőbb kutatóegyénisége, a Bjola professzor mellett Oxfordban dolgozó izraeli Ilan Manor érdeme a szakterület definíciós tisztázására tett első erőfeszítés. Ilan Manor: *What is Digital Diplomacy, and How Is It Practiced around the World?* 2016. és Ilan Manor: *Exploring Digital Diplomacy. Toward Clarification of a Fractured Terminology.* 2017.

mert ezen a ponton esetlegességekről aligha lehet szó.[34] Az egyes államok diplomáciai testületeinek munkáját ugyanis, ilyen funkcionális megközelítésben, egyenesen egy nemzetközi megállapodás rögzíti és részletezi:

- képviseleti funkció,
- információs funkció (tájékoztatás, illetve tájékozódás),
- kapcsolatépítési funkció,
- tárgyalási funkció,
- állampolgári érdekképviseleti (konzuli) funkció.[35]

Úgy gondoljuk: ezt a felosztást, működési tartalmat kell szem előtt tartani ahhoz, hogy értelmezni tudjuk a külügyek terén megvalósuló IKT-fejlesztések pontos szerepét és valóságos súlyát.[36]

Még egy fogalmi kérdés van, amelyre mindenképpen ki kell térnünk. Gyakorta kerül elénk a köznapi szóhasználatban és a hivatali nyelvben is a „közdiplomácia" fogalma. Úgy véljük, kulcsfogalom ez – s így különösen zavaró, hogy némileg félreértett módon használják. 19. századi előzmények után 1965-től jelölik ezzel az angolul *public diplomacynak* mondott szóösszetétellel azt az átalakulást, ami a modern diplomáciatörténet legnagyobb változását hozta.[37] Az eredetileg államok (vagy azok hivatalos szereplői) közötti kapcsolatokra szorítkozó diplomácia a 20. század drámai társadalmi-politikai átalakulásai nyomán váltott paradigmát: fokozatosan az államok (vagy azok hivatalos szereplői) és más államok közösségei (szervezetei, de akár egyénei) közötti kapcsolatok váltak a diplomáciai működés meghatározó mozzanatává. Ez az átalakulás mindennél fontosabb az államigazgatás e területének digitális transzformációja szempontjából is: a két folyamat kéz a kézben jár. Egymás nélkül elképzelhetetlenek, sőt bizonyos mértékig érthetetlenek is. Éppen ezért a szakmai tisztánlátást

[34] A modern diplomácia funkcióira, szervezetrendszerére, működési formáira, fontosabb problématerületeire ad jó áttekintést Ronald Peter Barston: *Modern Diplomacy* (New York, Routledge, 2013) munkája.

[35] Az úgynevezett Bécsi diplomáciai szerződés (a diplomáciai kapcsolatokról szóló 1961. évi bécsi szerződés). Vö. Bába Iván – Sáringer János: *Diplomáciai lexikon. A nemzetközi kapcsolatok kézikönyve.* Budapest, Éghajlat, 2018. 71–75. és 110.

[36] A diplomáciai tevékenységeknek ez a klasszikus funkcionális keresztmetszete az erőteljes digitalizáció korszakában is érvényesnek tekinthető, és a szakma elemzésének alapvető kiindulási pontját jelenti. Kishan S. Rana: *21st Century Diplomacy. A Practicioner's Guide*. London – New York, The Continuum International, 2011.

[37] Vö. *Public diplomacy stratégiák.* Budapest, Századvég, é. n. 8.

is nehezíti, hogy ma még a „közdiplomácia" a külügyminisztériumokon belüli részterületnek számít, mintha a public diplomacy a diplomáciai működésnek egy lehetséges válfaja, szakmai terepe lenne csupán, nem pedig az egész ágazat legújabb kori transzformációjának fémjele.[38]

Értelmezési keretrendszer

A diplomácia digitalizációs jelenségeivel kapcsolatban a fogalmi rendszer tisztázására (akár egyfajta szakmai „munkanyelv" elemeiként) egy áttekinthető, egyszerűsítő rendszerezést javasolunk. Alapvetően négy fogalmat ajánlunk megtartásra, azzal a megkötéssel, hogy tulajdonképpen három szerkezettel is leírható valamennyi fontos jelenség ezen a szakmai területen.

1. táblázat: A digitális diplomácia javasolt fogalmi keretrendszere[39]

Fogalom		Tartalma
(magyarul)	(angolul)	
Kiberdiplomácia	cyber diplomacy	A kibertérre, az online jelenségekre, a nagy globális technológiai cégekre vonatkozó nemzetközi szabályozó és irányító tevékenységekre vonatkozó államok közötti (diplomáciai) tevékenységek.
Techno-diplomácia	techno diplomacy	A kibertérre, az online jelenségekre, elsősorban a nagy globális technológiai cégekre vonatkozó szabályozó és irányító tevékenységek. Államok és globális technológiai cégek közötti kapcsolat.
E-diplomácia	e-diplomacy	A diplomácia digitalizálása a hagyományos működések gyökeres átalakítása nélkül.
Digitális diplomácia	digital diplomacy	A diplomácia hagyományos folyamatainak gyökeres („transzformatív") átalakítása az IKT-technológiák következtében.

Forrás: a szerző szerkesztése

[38] A digitális diplomácia eszközeinek és eljárásainak evolúciójára lásd *History of Digital Diplomacy and Main Milestones,* é. n.

[39] Nyáry Gábor: A digitális állam a külpolitikai térben. A Twittertől az adattudományig. *Új Magyar Közigazgatás,* 12. (2019), 2. 78.

Az egyik legfontosabb fogalmi tisztázás arra vonatkozik, hogy a digitális diplomácia alapvetően két elkülönülő aspektust ölel fel (nagyon hasonlóan a digitális államigazgatás fogalmának kettős jelentéséhez). E szerint a „digitális diplomácia" egyfelől a digitális térre vonatkozó diplomácia, másfelől a diplomácia digitalizált formája. Ez a legelső, legfontosabb kettősség. A tisztánlátás kedvéért mi a továbbiakban az előbbi aspektust (tehát az online terek, működések és szereplők szabályozásával kapcsolatos) diplomáciai, államközi tevékenységeket fogjuk „kiberdiplomáciának" nevezni. A „digitális diplomácia" fogalmat pedig megőrizzük a diplomáciai működés IKT-alapú transzformációja jelölésére.

Használatra javasoljuk még a „technodiplomácia" kifejezést, amely nagyon hasonló jelenségre vonatkozik, mint a kiberdiplomácia, ám egy fontos különbséggel: itt államok lépnek interakcióba kvázi államszerűen fellépő gigantikus magáncégekkel. A jelenség még ritkaság, de erősen terjed.[40] Továbbá használhatónak tartjuk az e-diplomácia kifejezést, elsősorban a diplomáciai szervezetek „üzemszerű" működésének korszerű IKT-eszközökkel történő támogatására, modernizálására. Itt a kulcsmozzanat az, hogy a digitális eszközök beállítása nem hozza maga után a támogatott hagyományos diplomáciai működések, folyamatok gyökeres átalakulását.

Kiberdiplomácia: kialakulás, tartalmak, fejlődési irányok

A kiberdiplomácia végső soron nem más, mint a diplomácia erőforrásainak, eljárásainak felhasználása a nemzeti érdekek, értékek és célok érvényesítésére, méghozzá egy speciális közegben vagy dimenzióban: nevezetesen a kibertérben. Érdemes megemlíteni, hogy amíg egy ország külpolitikájának fő vonásait valamilyen általános stratégiai dokumentum (nemzetstratégia, nemzeti biztonsági stratégia, védelmi stratégia, külpolitikai stratégia) határozza meg, addig az országok kibertérben érvényesítendő sajátos érdekeit, értékeit és céljait egy speciális stratégiai anyag, az úgynevezett kiberstratégia (vagy kiberbiztonsági stratégia) tartalmazza. A kiberdiplomácia működési terepe jó néhány különálló ügyterületet, speciális témát felölelhet. A legfontosabb, szinte folyamatosan terítéken levő kérdések a kiberbiztonság, a kiberbűnözés problémája. Ugyancsak

[40] Képviselői, motorjai az úgynevezett technodiplomaták, akiknek őstípusát a dán Casper Klynge képviseli, akit országa külügyminisztériuma 2017-ben nevezett ki erre a posztra, és akit nem valamely nemzetállam kormányánál akkreditáltak, hanem a Szilícium-völgyben.

fontos, állandó ügy a bizalomépítés kulcsfontosságú kérdése (mint még látni fogjuk, a diplomácia, a békés kapcsolatrendezés e fontos összetevője a kibertér sajátos viszonyai közepette csak jelentősen korlátozott formában jelenhet meg). Fontos tárgyalási terület az internet szabadságának kérdése, illetve (az előző szemponttal szoros összefüggésben) egyre nagyobb súllyal jelenik meg ma már a nemzetek közötti viszonyrendszerben a kiberszuverenitás kérdése is.

Szeretnénk hangsúlyozni: a „kiberdiplomácia" nem valami metafora csupán, hanem valóságos külkapcsolati terület és államközi interakciós terep. A kiberdiplomáciát valóságos diplomaták művelik, formáját tekintve pedig – ahogy a diplomácia „hétköznapi", klasszikus válfaja is – felölelhet bilaterális viszonyt (mint például az USA és Kína között 2015-ben kötött kiberbiztonsági megállapodás), illetve a nemzetközi rendezések multilaterális formáját is (például jellemzően az ENSZ általános vagy szakosított keretrendszerén belül).[41]

A kiberdiplomácia mint önálló, de legalábbis jól elkülönülő diplomáciai terep és tevékenység, az új évezred első évtizedének a vége felé jelenik meg.[42] A kibertérben meghatározó szerepet játszó (vagy játszani kívánó) hatalmak egymás után rukkolnak elő a kibertérre vonatkozó stratégiai dokumentumaikkal, ahogy egyre nyilvánvalóbbá kezd válni a kiberdomén geopolitikai értelemben meghatározó szerepe. Az USA 2009-ben publikálta a *Cyberspace Policy Review* (Kibertér-szakpolitikai áttekintés)[43] című dokumentumot; ugyanabban az évben jelent meg a brit *Cybersecurity Strategy* (Kiberbiztonsági stratégia), illetve a rá következő évben Kína is előállt a *White Paper on the Internet in China* (Fehér könyv a kínai internetről) című stratégiai dokumentummal. Ezek a dokumentumok kivétel nélkül a kiberbiztonság belföldi aspektusaira fókuszáltak (kibervédelmi kapacitások kiépítése, a kibervédelemmel kapcsolatos kormányzati koordináció erősítése), és a téma nemzetközi összefüggéseit legfeljebb csak érintőlegesen említették. Ezekkel a fejleményekkel párhuzamosan azonban multilaterális keretek között is megindultak az első tapogatózások a kibertér

[41] A kiberdiplomácia egyik legérdekesebb szemléletmódú bemutatását a digitális diplomácia kutatási terület egyik legjelesebb kutatójának, Shaun Riordannak köszönhetjük. Shaun Riordan: *Cyberdiplomacy. Managing Security and Governance Online.* Cambridge, Polity Press, 2019.

[42] André Barrinha – Thomas Renard: Cyber-Diplomacy: The Making of an International Society in the Digital Age. *Global Affairs,* 3. (2017), 4–5. 353–364. 358.

[43] A nemzeti kiberstratégiák fejlődése szempontjából az egyik legfontosabb ösztönző és egyben minta az amerikai kormányzat úttörő jellegű dokumentuma volt. Vö.: *Cyberspace Policy Review* (é. n.).

sajátos problémáinak feltárására, illetve a terület nemzetközi szabályozásának előkészítésére (lásd lejjebb).[44]

A szorosan vett kiberdiplomáciai tevékenységet, illetve gyakorlatot a 2010-es évtized legelejére datálhatjuk. Ekkor, 2011-ben jelent meg az Egyesült Államok kormányának az *International Strategy for Cyberspace* (Kibertér nemzetközi stratégiája) című korszakos dokumentuma. Korszakos azért, mivel ez az első olyan kormányzati dokumentum, amely koherens módon, önálló tématerületként tárgyalja a kibertér problematikájának nemzetközi összefüggéseit.[45] A stratégia azonosít néhány olyan problématerületet, amellyel kapcsolatban a nemzetközi szabályozás kialakítása kívánatos lehet: gazdaság, hálózatvédelem, rendvédelem, hadügyek, internetkormányzás, nemzetközi fejlesztéspolitika és az internet szabadsága. A fenti problémákkal foglalkozásra első ízben jelöli meg (a katonai és a fejlesztéspolitikai eszközökkel együttesen) a diplomáciát mint a kibertérrel kapcsolatos kérdések megoldásának lehetséges eszközét. A dokumentum, az irányelvek lefektetésével párhuzamosan, gondoskodik a megvalósítási intézményrendszer felállításáról is: az USA Külügyminisztériumán belül megalakult a Kibertérügyi Koordinátor Hivatala (Office of the Coordinator for Cyber Issues).[46]

Miközben a 2010-es évtized folyamán egyre több ország dolgozott ki és fogadott el a nemzeti kiberstratégiájára vonatkozó dokumentumot, a fenti amerikai kezdeményezéshez hasonló, kifejezetten a kibertér nemzetközi aspektusaira fókuszáló kormányzati dokumentumot csak elvétve szültek ezek az évek. A kivételek között szerepel a japán kormány által 2013-ban elfogadott *International Strategy on Cybersecurity Cooperation* (Nemzetközi kiberbiztonsági együttműködési stratégia).[47] Szintén a fontos mérföldkövek közé számíthatjuk az EU Tanácsa által 2015-ben elfogadott *Council Conclusions on Cyber Diplomacy*t (Európai tanácsi következtetés a kiberdiplomáciáról), amely első ízben használta – hivatalos dokumentumban – a „kiberdiplomácia" kifejezést az unió intézményrendszerében. Az elsősorban nemzeti fókuszú *French National Digital Security Strategy*ben (Francia nemzeti digitális biztonsági stratégia)

[44] A téma áttekintésére haszonnal forgatható Berzsenyi Dániel – Krasznay Csaba: *Nemzetközi kapcsolatok a kibertérben*. Budapest, Nemzeti Közszolgálati Egyetem, 2019.

[45] *International Strategy for Cyberspace,* 2011.

[46] *Office of the Coordinator of Cyber Issues* (é. n.).

[47] Barrinha–Renard (2017): i. m. 359.

külön fejezet foglalkozik a kibertér nemzetközi együttműködési kérdéseivel.[48] A stratégiai tervezéssel párhuzamosan több országban is felállítottak, általában a külügyminisztérium keretén belül, a kiberdiplomácia kérdéseire szakosodott szervezeti egységet (például Németországban, Belgiumban). Az önálló kiberrészleg felállítása mögött az a felismerés húzódott meg, hogy a külügyi tárcákon belül korábban sokfelé elaprózva, több ügyosztályhoz is hozzárendelve kezelték a kibertér egyes részterületeihez kapcsolódó problémákat, ami a koordináció hiányához és kevéssé hatékony működéshez vezetett.[49]

A kibertér szabályozása és igazgatása *(cyber governance)*

A kibertér kihívásai, szabályozási keretek és kezdeményezések

A kibertérhez közvetlenül vagy áttételesen kapcsolódó problémákat szemügyre véve jól érzékelhető, hogy ennek a „geopolitikai dimenziónak" van egy különös (a hatalmi viszonyok érvényesülésére szolgáló többi térelemre – a szárazföldre, a vízre, a levegőre és az űrre – nem mindig jellemző) sajátossága: szinte hívogatja a diplomáciát mint a kérdések rendezésének célszerű és kívánatos eszközét. Talán furcsán hangzik ez, hiszen a szakmai közbeszédben (hogy a politikát és a közvéleményt már ne is említsük) az erőszak (a kibertámadás) jelenik meg általában a kibertérbeli államközi interakciók bonyolítására szolgáló eszközként. Pedig a kiberdomén néhány jellegzetessége miatt igenis kívánatos terepnek számít a békés tárgyaláson, egyezkedésen, kölcsönös megállapodáson alapuló diplomáciai rendezések számára. Nézzünk ezek közül legalább néhányat![50]

Elsőként érdemes mindjárt előrebocsátani a korábban már megismert, de fontos alapelvet: a kiberdomén valóságos globális „tér". Olyan, ami egyszerre összeköti a nemzeteket, ugyanakkor természetesen a közöttük való súrlódásoknak is gyakori terepe. A kiberteret egyfajta „globális közlegelőnek" *(global commons)* szokták tekinteni.[51] Azaz olyan nemzetközi vagy még inkább nemzetek feletti

[48] *French National Digital Security Strategy,* 2015.

[49] *French National Digital Security Strategy,* 2015 és Barston (2013): i. m. 112.

[50] A kibertér szabályozására, irányítására vonatkozó nemzetközi koncepciók és törekvések áttekintését adja Sash Jayawardane: *Cyber Governance: Challenges, Solutions and Lessons for Effective Global Governance.* The Hague, The Hague Institute for Global Justice, 2015.

[51] Davinder Kumar: Securing Cyberspace: A Global Commons. *Indian Defense Review,* 30. (2015), 2.

erőforrásnak tekinthetjük, amilyen például a világtenger vagy a légkör, illetve maga a világűr is. Az ilyen közlegelők igazgatása rendszerint óhatatlanul felbukkanó dilemmával néz szembe. A közös és osztatlan erőforrást használó szereplők (államok) egy része abban érdekelt, hogy a közösen használt erőforrásra vonatkozóan éppen csak minimális nemzetközi szabályozás létezzen; olyan, ami a szabad hozzáférést, akadálytalan felhasználást és kiaknázást nem korlátozza lényegesen. Ezzel ellentétesen azonban, a hatalmi rivalizálást a geopolitika valamennyi (általuk elérhető) dimenziójára kiterjeszteni akaró hatalmak abban érdekeltek, hogy sajátos vízióikat, értékeiket és érdekeiket maradéktalanul kivetíthessék a hálózatos térbeli közlegelőre is. Ez a helyzet, a benne feszülő ellentétek miatt, fontos terepet kínál az egyeztetés, az érdekek békés összehangolása szakértőinek számító diplomaták számára.

A kibertér másik jellegzetessége, ami az erőszakos eszközökkel szemben inkább a diplomácia békés eszköztárának bevetését teszi indokolttá, az úgynevezett attribúció közmondásos nehézsége ebben a közegben. Röviden tehát: a kibertér struktúrája, működése folytán nehéz egyértelműen azonosítani az egyes kibertámadások elkövetőit.[52] Ez jelentősen hozzájárul a közbizalom aláásásához, az agresszív viselkedési normák bátorításához, ami végső soron egyik közlegelő-használónak sem érdeke.[53]

További jellegzetesség (és az előző pontban említett sajátosság tulajdonképpen így nyer értelmet), hogy a kibertérben nem (vagy csak elenyésző mértékben) működik a klasszikus geopolitikai konfrontációs helyzetek egyik legfontosabb eleme: az elrettentés. A kibertérben végrehajtott erőszakos akciók jellegüknél fogva rejtve maradnak, vagy a valódi elkövető kiléte marad homályban. Ennek következtében nem tudják betölteni az egyedi erőszakos (fegyveres) állami akciók egyik legfontosabb funkcióját: azt tudniillik, hogy a potenciális ellenfelet elriasszák az erőszakhoz való folyamodástól. A kibertér ezen sajátosságai tehát abba az irányba hatnak, hogy az erőszakos akciók – más geopolitikai dimenziókkal, potenciális csatateremekkel összevetve – kevésbé vonzó alternatívát kínáljanak az államközi viszonyok diplomáciai rendezése helyett.

[52] Legalábbis a hivatalos álláspont szerint. A kibervédelemmel foglalkozó titkosszolgálati szakemberek egy része ugyanakkor – háttérbeszélgetések során – állítja: a jelentős kiberkapacitásokkal és tapasztalattal rendelkező hatalmak igen jó pontossággal tudják azonosítani az online terekben végrehajtott támadó akciók tényleges kiindulási forrásait.

[53] Barrinha–Renard (2017): i. m. 357.

Globális normák, szabályozási törekvések

Feljebb már említettük, hogy az első kormányzati kiberstratégiai dokumentumok kidolgozásával lényegében egy időben multilaterális keretek között is megindultak a munkálatok a kibertér sajátos problémáinak feltárására, illetve a terület nemzetközi szabályozásának előkészítésére. Ebben az összefüggésben különösen fontosak voltak az ENSZ Kormányzati Szakértői Csoportjainak[54] ülései 2010-től kezdve, amelyek azt tűzték ki célul, hogy a nemzetközi közösség összefogásával a kibertámadások fenyegetéseinek csökkentésére vonatkozó, illetve általánosságban véve a felelősségteljes állami magatartás önkéntes normáit kidolgozzák a kibertér vonatkozásában. A csoport, aminek felállításáról egy jóval korábban Oroszország által beterjesztett javaslat[55] alapján döntött a világszervezet, olyan munkaterepet nyitott az egymással rivalizáló nagyhatalmak számára, ahol azok megpróbálhattak valamiféle találkozási pontokat kialakítani, elsősorban a területen égetően szükséges bizalomerősítés szférájában. A munkaszervezetben a nagyhatalmak képviselői kaptak helyet, és a hatalmi rivalizálások végül erősen rányomták bélyegüket a csoport tevékenységére.

A kibertér problémáinak feltérképezésére, a követendő normarendszerek kidolgozására a világszervezet egy másik kezdeményezést is útjára indított. Részben a UN GGE csoport tapasztalatai alapján, tanulva annak relatív sikertelenségéből (a szervezet nem volt képes munkáját a szokásos jelentés formájában összegezni), egyébként ismét orosz kezdeményezésre, 2017-ben az ENSZ egy nyílt végű munkacsoport felállításáról határozott. A valamennyi tagállam számára nyitott formátumtól azt várták, hogy a közös szabályrendszerek kidolgozásába képes lesz majd bevonni az ENSZ olyan tagjait is, amelyek a korábban felállított Kormányzati Szakértői Csoportból óhatatlanul kimaradtak.[56]

A multilaterális szinten történő egyeztetések, normakidolgozások területén említésre méltó kezdeményezés volt még az úgynevezett Kibertér-stabilitási Globális Bizottság (Global Commission on the Stability of Cyberspace), amit két magán-kutatóintézet *(think tank)* hívott életre 2019 novemberében. A cél

[54] UN Group of Governmental Experts (UN GGE). A multilaterális szabályozási törekvések jó összefoglalóját adja közre Eneken Tikk – Mika Kerttunen: *Parabasis. Cyber Diplomacy in Stalemate.* Oslo, Norwegian Institute of International Affairs, 2018.

[55] Az ENSZ Közgyűlés 66/24 sz., 2011-ben elfogadott határozata. Barrinha–Renard (2017): i. m. 359.

[56] Christian Ruhl: *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at Crossroads.* Washington, Carnegie Endowmwent, 2020. 7.

az volt, hogy széles körből merítve a résztvevőket, a kormányzat mellett a tudományos élet, az ipar és a civil világ képviselőit is bevonja a kibertér nemzetközi normáinak kialakítását célzó közös gondolkodásba. A testület által közreadott *Szingapúri normacsomag* című dokumentumban foglalt ajánlások végül bekerültek egy másik nemzetközi szabályalkotó grémium, az úgynevezett Párizsi felhívás dokumentumai közé is.[57]

Az ugyancsak 2019 novemberében életre hívott *Paris Call for Trust and Security in Cyberspace*[58] (Párizsi felhívás) a francia kormányzat kezdeményezése, amely mögé a Microsoft vállalat is beállt főtámogatónak. Aláírói (több mint ezer különféle kormányzati és magánszervezet, tudományos és szakmai entitás) kilenc önkéntesen vállalt norma mellett tették le a voksukat. Az alapelvek (amelyek között hangsúlyosan szerepel az egyének és a kritikus infrastruktúrák védelme, az internet nyilvános magjának védelme, valamint az online választói folyamatok kiemelt védelme) a korábbi megelőző multilaterális egyeztetések eredményeire építettek.[59]

Végezetül érdemes röviden megemlíteni az EU szerepét, törekvéseit.[60] Az unió 2016-ban elfogadott alapvető biztonságpolitikai dokumentuma a tagállamokra leselkedő veszélyek között kiemelt helyen említi a kibertér fenyegetéseit.[61] A dokumentum leszögezi: az EU-nak a jövő felé tekintő kiberszereplővé kell válnia a kiberdiplomácia terén.[62] Az unió koncepciójában – miközben a szervezet egyértelműen tudatában van a kiberdomén veszélyeztetettségének rohamos növekedésével – a kiberbűnözéssel, kiberkárokozással szembeni küzdelemben egyértelműen a kiberdiplomácia jelenik meg központi pillérként.

Kitekintés

Változnak az idők – és a jelek szerint velük változnak a „terek" is. Tanulmányunk elején igyekeztünk végigkövetni az utat, amelynek során a földgolyó országainak egymáshoz való kapcsolódási hálója, a manapság ismét sokat emlegetett világrend fokozatosan átalakult: a második világháború nem csupán emberéletekben

[57] Ruhl: (2020): i. m. 7.
[58] Ruhl: (2020): i. m. 7.
[59] *Paris Call for Trust and Security in Cyberspace,* továbbá Ruhl (2020): i. m. 7.
[60] Az Európai Unió kiberbiztonsági politikáival a könyv külön fejezete foglalkozik részletesen.
[61] *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy,* 2016, 22.
[62] Tania Latici: *Cyber: How Big Is The Threat?* 2019.

és anyagi értékekben okozott rettenetes pusztítást, de egyben a hatalmi viszonyokat is drámaian átszabta, megágyazva egy olyan kétpólusú berendezkedésnek, ahol a világban csupán két óriás számított, az USA és a Szovjetunió. A hidegháború végével, az 1990-as évek legelejére, a riválisnagyhatalom és maga köré épített blokkjának felbomlása nyomán Amerika hirtelen egyedül maradt a hatalom porondján. Ez volt a szakértők által említett „unipoláris pillanat", amikor a világ a liberális demokráciák élén álló USA vezetésével egypólusúvá alakult. A megnevezés találó, mert mára jól látszik, hogy ez a hatalmi konstrukció – történelmi léptékkel mérve – valóban csupán egy pillanatig tartott. A 2000-es évek első évtizedétől, régi és új hatalmak bejelentkezésével és emelkedésével fokozatosan látszik kiépülni egy újabb, immár multipoláris világrend. Olyan hatalmi konstrukció, ahol helyi-regionális és természetesen világhatalmi ambíciókkal rendelkező államok egész sora alkot erőközpontokat, egymást sokszor keresztülszelő hatalmi hálókat. A hálómetafora használata kétszeresen is indokoltnak látszik. A hatalmi erőegyensúlyban, geopolitikai viszonyrendszerben ugyanis egyre meghatározóbbá válik a kibertér dimenziója.[63] Az a számítógépes rendszerekből, szoftverekből és az azokat használó emberekből a világháló révén összefont struktúra tehát, amit röviden kibertérnek nevezünk. Jól látható már az állami kiberképességek erőkompenzáló funkciója: kicsi (tehát a szokványos hatalomdefiníciók szerint meghatározó szerepre alkalmatlan) országok is, hálózatos technológiai kapacitásaik kiépítésével olyan világpolitikai szereplőkké válnak, amelyekkel számolni kell.[64]

Ez az egyszerre virtuális és ugyanakkor kézzelfoghatóan valóságos tér maga is változóban van. Éppen azért, mert a geopolitikai átrendeződések visszahatnak erre az egyre fontosabb vetélkedési területre is. A kiberteret születésekor, létrejötte pillanatától a nyugati világ elvei és koncepciói formálták.[65] Liberális

[63] André Barrinha – Thomas Renard: Power and Diplomacy in the Post-Liberal Cyberspace. *International Affairs,* 96. (2020a), 3. 756.

[64] Barrinha–Renard: (2020a): i. m. 756. A legismertebb példa a kis nemzetek ilyen „erejükön felüli" pozicionálására, köszönhetően a kiberképességeik színvonalának és nagyságának: Szingapúr és különösen Észtország esete.

[65] A nyugati világban (elsősorban az Egyesült Államokban) születtek a számítástechnika jelentős technológiai fejlesztései, az eszközöktől a szoftvereken át az ott megálmodott világhálóig. Ezt az előnyt, monopolhelyzetet erősítette tovább az iparág (kezdve a számítástechnikai ipartól az internetes iparokig, közösségi hálózati szolgáltatásokig) szinte teljes Amerika-központúsága (amihez a szintén a nyugati szövetséghez tartozó Japán, Dél-Korea, illetve skandináv államok adtak további koncentráló erőt).

elvek szerint szerveződött, nyugati technológiák és intézmények dominálták. Ahogy a világ változik, jól láthatóan változni kezdett ez a tér is. A multipoláris világrend feltörekvői bejelentkeztek a kibervalóság „átvételére" is, de legalább a korábbi nyugati (amerikai) monopolhelyzet felszámolására. Ami a szemünk előtt formálódik tehát, az egy sokkal kevésbé nyugatos, és sokkal inkább „poszt-liberális" kibervilág.[66] Ebben az átalakulásban, a kibertér drámai átrajzolásában egyre meghatározóbb szerepet kapnak a kiberdiplomaták. Ezeken a vidékeken, amelyek korábban az informatikusok, számítástechnikai mérnökök, hálózattudósok felségterületének számítottak, ma már egyre inkább a külkapcsolat-építés hivatásosai mozognak otthonosan. Szakdiplomaták – akik ugyanakkor eligazodnak a modern kibervilág technológiai, jogi és etikai kérdéseiben is.

Felhasznált irodalom

A Global Actor in Search of a Strategy. European Union Foreign Policy between Multilateralism and Bilateralism. Brussels, European Union, 2014.

Bába Iván – Sáringer János: *Diplomáciai lexikon. A nemzetközi kapcsolatok kézikönyve.* Budapest, Éghajlat, 2018.

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

Barrinha, André – Thomas Renard: Power and Diplomacy in the Post-Liberal Cyberspace. *International Affairs,* 96. (2020a), 3. 749–766.

Barrinha, André – Thomas Renard: *The Emergence of Cyber Diplomacy in an Increasingly Post-Liberal Cyberspace*. 2020b. június 16. Online: www.cfr.org/blog/emergence-cyber-diplomacy-increasingly-post-liberal-cyberspace.

Barston, Ronald Peter: *Modern Diplomacy.* New York, Routledge, 2013.

Bassot, Etienne: *The von der Leyen Commission's Priorities for 2019–2024*. 2020. június 8. Online: www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)646148.

Berzsenyi Dániel – Krasznay Csaba: *Nemzetközi kapcsolatok a kibertérben*. Budapest, Nemzeti Közszolgálati Egyetem, 2019.

Bjola, Corneliu: *Digital Diplomacy.* London – New York, Routledge, 2015.

[66] André Barrinha – Thomas Renard: *The Emergence of Cyber Diplomacy in an Increasingly Post-Liberal Cyberspace.* 2020b.

Bjola, Corneliu: Digital Diplomacy 2.0. Trends and Counter-Trends. *Revista Mexicana de Política Exterior,* (2018). 35–52.

Bjola, Corneliu: *Digital Diplomacy: From Tactics to Strategy*. é. n. Online: www.americanacademy.de/digital-diplomacy-tactics-strategy/.

Blount, P. J.: *Reprogramming the World. Cyberspace and the Geography of Global Order.* Bristol, E-International Relations Publishing, 2019.

Borell, Josep: *HR/VP Josep Borell: Embracing 'Geopolitical' Europe's Power.* 2020. április 22. Online: www.eubulletin.com/10653-hr-vp-josep-borrell-embracing-geopolitical-europes-power.html.

Brzezinski, Zbigniew: *A nagy sakktábla*. Budapest, Európa, 1999.

Choucri, Nazil: *Cyberpolitics in International Relations.* Cambridge, MIT Press, 2012.

Clüver Ashbrook, Cathryn: *21st Century Diplomacy.* 2014. Online:www.belfercenter.org/publication/21st-century-diplomacy

Cohen, Saul Bernard: *Geopolitics: The Geography of International Relations.* Lanham, Rowman and Littlefield, 2015.

Cyberspace Policy Review (é. n.). Online: https://fas.org/irp/eprint/cyber-review.pdf.

Dee, Megan: *The European Union in a Multipolar World. World Trade, Global Governance and the Case of the WTO.* London, Palgrave MacMillan, 2015.

Desforges, Alix: Representations of Cyberspace: A Geopolitical Tool. *Hérodote,* 152–153. (2014), 1–2. 67–81.

Domingo, Francis C.: Conquering A New Domain: Explaining Great Power Competition in Cyberspace. *Comparative Strategy*, 35. (2016), 2. 154–168.

French National Digital Security Strategy. 2015.

Fourkas, Vassilys: What is Is 'Cyberspace'? *Media Development,* 3. (2004), 6–7.

Global Trends to 2035. Geo-politics and International Power. Brussels, European Parliamentary Research Service, 2017.

History of Digital Diplomacy and Main Milestones (é. n.). Online: http://diplomacydata.com/history-of-digital-diplomacy-and-main-milestones/.

International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. 2011.

Jayawardane, Sash: *Cyber Governance: Challenges, Solutions and Lessons for Effective Global Governance.* The Hague, The Hague Institute for Global Justice, 2015.

Kaplan, Robert D.: *A földrajz bosszúja.* Budapest, Antall József Tudásközpont, 2019.

Kissinger, Henry: *Világrend*. Budapest, Antall József Tudásközpont, 2016.

Kumar, Davinder: Securing Cyberspace: A Global Commons. *Indian Defense Review,* 30. (2015), 2. Online: www.indiandefencereview.com/news/securing-cyberspace-a-global-commons/.

Kuus, Merje: *Geopolitics Reframed. Security and Identity in Europe's Eastern Enlargement.* New York, Palgrave MacMillan, 2007.

Latici, Tania: *Cyber: How Big Is The Threat?* 2019. Online: www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2019)637980.

Lehne, Stefan: *Is There Hope for EU Foreign Policy?* Brussels, Carnegie Endowment, 2017.

Manor, Ilan: *What is Digital Diplomacy, and How Is It Practiced around the World?* 2016. Online: www.researchgate.net/publication/310952363_What_is_Digital_Diplomacy_and_how_is_it_Practiced_around_the_World_A_brief_introduction/link/583b591708ae3a74b4a06b2f/download.

Manor, Ilan: *Exploring Digital Diplomacy. Toward Clarification of a Fractured Terminology.* 2017. Online: https://digdipblog.com/countries-on-twitter-and-facebook/.

Melissen, Jan: *Diplomacy in the Digital Age.* The Hague, Clingendael, é. n.

Müller-Hennig, Marius: *A Truly Geopolitical EU Commission? Rather than Playing Geopolitical Games Itself, von der Leyen's Commission Should Be Critical of the Very Notion of Geopolitics.* 2019. Online: www.ips-journal.eu/regions/europe/article/show/a-truly-geopolitical-eu-commission-3918/.

Nyáry Gábor: A digitális állam a külpolitikai térben. A Twittertől az adattudományig. *Új Magyar Közigazgatás,* 12. (2019), 2. 75–82.

Office of the Coordinator of Cyber Issues (é. n.). Online: www.state.gov/bureaus-offices/bureaus-and-offices-reporting-directly-to-the-secretary/office-of-the-coordinator-for-cyber-issues/.

Paris Call for Trust and Security in Cyberspace. 2018. Online: https://pariscall.international/en/call.

Pintér István (szerk.): *Műhelymunkák. A virtuális tér geopolitikája. 2016/1.* Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016.

Public diplomacy stratégiák. Budapest, Századvég Politikai Iskola Alapítvány, é. n.

Rana, Kishan S.: *21st Century Diplomacy. A Practicioner's Guide*. London – New York, The Continuum International, 2011.

Riordan, Shaun: *Cyberdiplomacy. Managing Security and Governance Online.* Cambridge, Polity Press, 2019.

Ruhl, Christian: *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at Crossroads.* Washington, Carnegie Endowment, 2020.

Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. 2016.

Szilágyi István: *A geopolitika elmélete.* Budapest, Pallas Athéné, 2018.

„The Key Problem of Our Time": A Conversation with Henry Kissinger on Sino-U.S. Relations. 2018. Online: www.wilsoncenter.org/article/the-key-problem-our-time-conversation-henry-kissinger-sino-us-relations.

Tianjiao, Jiang: From Offense Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar. *Chinese Journal of International Review,* 1. (2019), 2. 1–23.

Tikk, Eneken – Mika Kerttunen: *Parabasis. Cyber Diplomacy in Stalemate.* Oslo, Norwegian Institute of International Affairs, 2018.

US Department of Defense Cyber Strategy 2018. 2018. Online: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Whyte, Christopher – Brian Mazanec: *Understanding Cyber Warfare: Politics, Policy and Strategy*. New York, Routledge, 2019.

[Vákát oldal]

Molnár Anna

A kiberdiplomácia fejlődése az Európai Unióban

Bevezetés

Noha az Európai Unió (a továbbiakban: EU) már a kilencvenes évek második felétől megkezdte a számítástechnikával és az elektronikus kommunikációval kapcsolatos tevékenységeinek fejlesztését, az átfogó megközelítésre építő kiberbiztonsági szakpolitikai keret- és intézményrendszer kiépítése valójában csak az elmúlt évtizedben kezdődött el. Az egyénekkel, vállalatokkal és a kritikus infrastruktúrákkal szembeni növekvő számú kibertámadások egyre inkább felhívták a figyelmet a kibertérrel kapcsolatos fenyegetésekre és kockázatokra. Tekintettel arra, hogy a számítógépes bűnözés nem ismeri a nemzeti határokat, e területen is szükségessé vált az uniós szintű együttműködés feltételrendszerének kiépítése. Ezt a folyamatot jogi intézkedések elfogadása (például az információs rendszerek elleni támadásokról szóló 2005. évi tanácsi kerethatározat) és új intézményi struktúrák létrehozása (például az Európai Hálózat- és Információbiztonsági Ügynökség – ENISA 2004-ben és az Europolban a számítástechnikai bűnözéssel foglalkozó európai központ, az EC3 megalapítása 2013-ban) jelezte.[1] E tanulmány célja, hogy átfogó képet nyújtson az EU-s kiberdiplomáciával összefüggő intézményi struktúrákról és stratégiai keretekről.

2007 után az észt magán- és közintézmények, illetve infrastruktúra ellen elkövetett orosz eredetű elosztott szolgáltatásmegtagadással járó támadásokat (DDoS) követően az EU egyre nagyobb hangsúlyt fektetett az információ- és hálózatbiztonság megerősítésére. Napjainkra a kibertér a nemzetközi kapcsolatok kiemelt területévé vált, és az uniós külpolitika szerves részét képezik a kiberdiplomáciával kapcsolatos területek. Az Európai Unió is megkezdte a kiberdiplomáciával és a kibervédelemmel összefüggő eszköz- és intézményrendszerének kiépítését.

[1] Helena Carrapico – Andre Barrinha: European Union Cyber Security as an Emerging Research and Policy Field. *European Politics and Society,* 19. (2018), 3. 299–303.

https://doi.org/10.36250/01008_03

Az uniós intézmények és infrastruktúra elleni egyre célzottabb és nagyszabású kibertámadások arra késztették a döntés-előkészítőket és döntéshozókat, hogy a hatáskörükbe tartozó főbb tevékenységek mindegyikére kiterjedő átfogó kiberbiztonsági politikát fejlesszenek. Az EU-ról szóló szerződés 3. cikke sorolja fel az unió céljait és tevékenységeinek főbb területeit. Ezek közül kiemelhető az egységes piac megvalósítása, a szabadság, biztonság és jog térségének kialakítása és a közös kül- és biztonságpolitika megvalósítása. A 2010-es évektől megkezdődött a kiberbiztonsággal és kibervédelemmel összefüggő többszintű kormányzás uniós szintű eszköz- és intézményrendszerének a kiépülése.[2] Ennek fontos elemeként a kiberdiplomáciával összefüggő tevékenységek elsősorban a közös kül- és biztonságpolitikát, és az annak szerves részét képező közös biztonság- és védelempolitika területeit érintik, de a közös piaccal és a szabadság, biztonság és jog térségének kialakításával összefüggő kiberbiztonsági kérdések nemzetközi szintű képviselete is ide tartozik.

Számos, az EU kiberbiztonságát és kiberdiplomáciáját befolyásoló tényező, mint például az egyre nagyobb számban jelentkező kiberfenyegetések és kibertámadások között megemlíthetjük az Egyesült Királyság kilépését az EU-ból. Noha a brexit valószínűsíthetően e területen is negatív hatást gyakorol, az EU és az EK közötti kölcsönös egymásrautaltság a szoros kapcsolatok fenntartását fogja eredményezni.[3]

Kiberdiplomácia

A kiberdiplomácia fogalmára számos definíció található a szakirodalomban. Ezek közül megemlíthetjük André Barrinha és Thomas Renard meghatározását, amely szerint a kiberdiplomácia a kibertérrel összefüggő diplomácia, vagyis diplomáciai erőforrások felhasználása és diplomáciai feladatok ellátása a kibertérrel kapcsolatos ügyek és a nemzeti érdekek biztosítása érdekében. Az ezzel összefüggő érdekeket és célokat a kiberbiztonsági stratégiák fektetik le. A kiberdiplomácia napirendjén szereplő legfontosabb kérdések között megemlíthetjük a kiberbiztonság, a kiberbűnözés, a bizalomépítés, az internet szabadsága

[2] George Christou: The Collective Securitisation of Cyberspace in the European Union. *West European Politics,* 42. (2019), 2. 278–301. 1–24. 1–2.

[3] Tim Stevens – Kevin O'Brien: Brexit and Cyber Security. *The RUSI Journal,* 164. (2019), 3. 22–30.

és az internet irányítása területeit. A kiberdiplomácia legfontosabb szereplői közé a hagyományos diplomaták, illetve az e szakpolitikai területen meghatározó szerepet játszó különböző intézmények, testületek és ügynökségek képviselői tartoznak.[4] Mivel napjainkban a kibertérben egyre gyakoribbak az egyes szereplők, és ebből következően a nagyhatalmak közötti feszültségek, egyre nagyobb szükség van az ilyen típusú konfliktusok rendezését célzó nemzetközi tárgyalások folytatására és megállapodások kötésére. Az elmúlt évtizedekben az EU nem csupán a saját tagállamai közötti integrációs folyamat mélyülése következtében, hanem a kiberbiztonsággal és kibervédelemmel összefüggő nemzetközi viták rendezése érdekében is egyre aktívabb szerepet töltött be.[5]

Noha az IKT- (információ- és kommunikációtechnológiai) eszközök használata egyre elterjedtebb a külügyi igazgatási szintek különböző szereplői körében, a kiberdiplomácia és az e-diplomácia – amelyet elektronikus vagy digitális diplomáciának is nevezünk – két különböző fogalomként határozható meg. Annak ellenére, hogy a két fogalom használata sokszor keveredik, esetenként egymás szinonimáiként is használják azokat, a két fogalom között jelentős különbség van. A legfőbb különbséget abban határozhatjuk meg, hogy az e-diplomácia kizárólag a digitális eszközök használatát jelenti a diplomaták, a külügyi alkalmazottak és külügyminiszterek által. Tom Fletcher szerint az e-diplomácia hivatalosan 1994-ben született, amikor a svéd külügyminiszter, Carl Bildt elküldte első hivatalos diplomáciai e-mailjét Bill Clintonnak. A svéd diplomata így gratulált az amerikai elnöknek a Vietnámmal szemben alkalmazott embargó megszüntetésének alkalmával.[6] Ezzel szemben Smith és Sutherland a kiberdiplomácia kifejezést az egyre intenzívebb, a digitális eszközök segítségével megvalósuló diplomáciai tevékenységek meghatározásaként is használják.[7]

[4] 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. 3.

[5] Thomas Renard: EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain. *European Politics and Society,* 19. (2018), 3. 321–337.

[6] Barrinha–Renard (2017): i. m. 4.

[7] Gordon Smith – Allen Sutherland: The New Diplomacy: Real-Time Implications and Applications. In Evan H. Potter (szerk.): *Cyber-diplomacy: Managing Foreign Policy in the Twentyfirst Century.* Quebec, McGill-Queen's University Press, 2002. 151–177. 155.

Az uniós kiberdiplomácia fejlődése

Stratégiai keretek

A 2000-es évektől egyre több uniós dokumentum foglalkozott a kiberbiztonság szerteágazó kérdésével. Az első átfogó kiberbiztonsági stratégia kidolgozására 2013-ban került sor, az új dokumentum a *Nyílt, megbízható és biztonságos kibertér* címet viselte.[8] A stratégia elkészítésében az EU külügyi és biztonságpolitikai főképviselője, Chatherine Ashton irányításával az Európai Külügyi Szolgálat és az Európai Bizottság is együttműködött. E dokumentum említette először az EU nemzetközi kiberbiztonsági politikáját és kibervédelmi céljait. A NATO hasonló stratégiáival összehasonlítva (2008, 2011) az uniós dokumentum nem csupán a saját informatikai hálózatának védelmére szorítkozott, hanem szinte minden uniós kompetenciába tartozó területre kiterjedt.[9]

A 2013-as stratégia az EU nemzetközi kiberpolitikájával kapcsolatos céljait is meghatározta. Az új szakpolitika a szabad és nyitott internet védelme mellett célul tűzte ki a felelősségteljes állami magatartás nemzetközi jogi normáinak és a bizalomépítő intézkedések előmozdítását a kibertérben és az EU stratégiai partnereivel történő együttműködés javítását. Az uniós kiberdiplomácia részeként tárgyalások kezdődtek az Egyesült Államokkal, Kínával, Japánnal, Dél-Koreával, Indiával és Brazíliával. A részt vevő felek a tárgyalások során többek között érintették a kibertérben zajló nemzetközi biztonság, az ellenálló képesség, a kiberbűnözés, az internet szabályozása és a kiberbiztonsági előírások területeit.

Kiberdiplomácia

2015-ben fontos mérföldkő volt az EU kollektív erőfeszítéseinek elősegítése érdekében a kiberdiplomáciáról szóló tanácsi következtetések elfogadása.[10] Barrinha és Renard szerint ez volt az első olyan hivatalos kormányzati dokumentum, amely

[8] Európai Bizottság: Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér JOIN/2013/01 final. 2013.

[9] Jochen Rehrl (szerk.): *Handbook on Cyber Security. The Common Security and Defence Policy of the European Union*. Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2018. 18.

[10] Rehrl (2018): i. m. 23.; Myriam Dunn Cavelty: Europe's Cyber-power. *European Politics and Society,* 19. (2018), 3. 1–17, 10.

a kiberdiplomácia kifejezést használta.[11] 2015-től – a tanácsi következtetésekkel és az általános külpolitikai célokkal összhangban – az EU a kiberdiplomácia területén is elő kívánta mozdítani és védeni az emberi jogokat.

A kiberdiplomácia

> „az unió alapvető értékein, vagyis a demokrácián, az emberi jogokon és a jogállamiságon, ezen belül a véleménynyilvánítás szabadságához való jogon, az információhoz való hozzáférés szabadságán és a magánélethez való jogon alapul. Az unió célja annak biztosítása, hogy ne lehessen az internet nyújtotta lehetőségekkel visszaélni gyűlöletkeltés és erőszakra való felbujtás céljával, valamint hogy az internet – az alapvető szabadságok teljes tiszteletben tartásával – továbbra is a szabad véleménynyilvánítás fóruma maradjon a jog maradéktalan betartása mellett. A célok között megjelenik a nemek közötti egyenlőséget is figyelembe vevő kiberpolitika előmozdítása. Az EU ösztönzi az európai növekedést, jólétet és versenyképességet, valamint védi a legfontosabb uniós értékeket, többek között a kiberbiztonság erősítése és a számítástechnikai bűnözés elleni küzdelem terén folytatott együttműködés javítása révén. Az uniós diplomáciai és jogi eszközök igénybevétele révén hozzájárul a kiberbiztonságot fenyegető veszélyek mérsékléséhez, a konfliktusmegelőzéshez és a stabilitás növekedéséhez a nemzetközi kapcsolatok terén. Mindemellett segíti az internet irányítására vonatkozó többérdekeltes modell erősítésére irányuló erőfeszítéseket. Az EU ösztönzi a nyitott és virágzó társadalmak kialakulását harmadik országokban olyan kiberkapacitás-építési és -fejlesztési intézkedéseken keresztül, amelyek hozzájárulnak a véleménynyilvánítás és az információhoz való hozzáférés szabadságához való jog előmozdításához és védelméhez, és amelyek lehetővé teszik a polgárok számára, hogy teljes mértékben a javukra fordítsák a kibertér társadalmi, kulturális és gazdasági előnyeit, többek között a digitális infrastruktúrák biztonságosságának fokozása révén. Az Európai Unió célja, hogy előmozdítsa a felelősség megosztását az érintett érdekelt felek között, többek között a köz- és a magánszektor, valamint a kutató- és tudományos intézetek között a kibertérrel kapcsolatban folytatandó együttműködés révén."[12]

Kiberbiztonság és a digitális egységes piac

A 2010-es években az európai gazdaságok egyre szélesebb körű digitalizációja sürgette a biztonságos kibertér támogatását célzó uniós szintű stratégiák és intézkedések kidolgozását. A 2015-ös digitális egységes piaci stratégia a gazdaság digitalizációjával összefüggő kérdések mellett a kibertér biztonságát, azaz

[11] Barrinha–Renard (2017): i. m. 7.

[12] Európai Unió Tanácsa: *A Tanács következtetései a kiberdiplomáciáról*. Brüsszel, 2015. február 11.

a kritikus infrastruktúra és a hálózatok védelmét is hangsúlyozta.[13] A 2015-ös uniós belső biztonsági stratégia és a hibrid fenyegetések elleni fellépést szorgalmazó európai bizottsági és külügyi szolgálati dokumentum is stratégiai irányelveket fogalmazott meg a kiberbűnözéssel és a kiberbiztonsággal kapcsolatban.[14] Az unió 2016-ban meghozta az első kiberbiztonságra vonatkozó uniós jogi aktust, a hálózati és információs rendszerek biztonságáról szóló (EU) irányelvet (NIS).[15]

Kiberdiplomáciai eszköztár

Az Európai Unión belüli, kiberbiztonsággal összefüggő szakpolitikai területek mélyülése következtében az e területekkel összefüggő érdekeket képviselő diplomáciai eszköztár megerősítése is szükségessé vált. Az unió politikai, biztonsági és gazdasági érdekeinek átfogó védelme érdekében 2017-ben az EU Tanácsa megállapodott arról, hogy kidolgozza az állami és nem állami szereplők részéről mutatkozó rossz szándékú és tudatos kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretét, az úgynevezett kiberdiplomáciai eszköztárat (EU Cyberdiplomacy Toolbox). Az új eszköztár az EU közös kül- és biztonságpolitikai eszköztárára támaszkodik. A tanácsi döntéssel összhangban azon információs és kommunikációs technológiák (IKT) felhasználásával végrehajtott tevékenységekkel szemben, amelyek kimeríthetik a nemzetközi jogot sértő cselekmény fogalmát, az EU kész a közös kül- és biztonságpolitikai intézkedésekkel, ideértve a korlátozó intézkedéseket is, fellépni.[16]

Az EU kiberdiplomáciai megközelítésével összhangban a közös intézkedések elősegítik a konfliktusmegelőzést, a kiberbiztonságot fenyegető veszélyek mérséklését, és a stabilitás növekedését a nemzetközi kapcsolatok terén. A Tanács célul tűzte ki, hogy a közös uniós diplomáciai intézkedések kerete segíti az együttműködést, előmozdítja a veszélyek csökkentését, valamint hatással lesz

[13] Európai Bizottság: *Európai digitális egységes piaci stratégia*. Brüsszel, 2015. május 6. COM(2015) 192 final.

[14] Christou (2018): i. m. 2.

[15] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve: *Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről* (HL L 194., 2016. július 19., 1.).

[16] Európai Unió Tanácsa: *Informatikai támadások: az EU készen áll az ellenintézkedésekre, ideértve a szankciókat is*. 2017a. június 19.

a potenciális támadók magatartására. Döntés született arról is, hogy ezekben az esetekben teljeskörűen alkalmazni fogják a közös kül- és biztonságpolitika területéhez tartozó intézkedéseket, beleértve a korlátozó, esetleg szankciós intézkedéseket is. Az alkalmazott intézkedéseknek – a nemzetközi joggal összhangban – arányosnak kell lenniük a rossz szándékú „kibertevékenység hatókörével, léptékével, időtartamával, intenzitásával, összetettségével, kifinomultságával és hatásaival". Az EU egyúttal megerősítette, hogy „elkötelezett a kibertérben folyó nemzetközi viták békés úton történő rendezése mellett". Ezzel összefüggésben minden erőfeszítése arra irányul, hogy hozzájáruljon a kibertér biztonságához és stabilitásához, illetve hogy csökkentse az IKT használatából eredő félreértések, konfliktusok kialakulásának és terjedésének kockázatát.[17]

A Politikai és Biztonsági Bizottság 2017. október 11-én a kiberdiplomáciai eszköztárra vonatkozóan végrehajtási iránymutatásokat fogadott el. A dokumentum a kiberdiplomáciai eszköztáron belül öt intézkedéskategóriát sorolt fel: 1) a megelőző intézkedéseket, 2) az együttműködési intézkedéseket, 3) a stabilitást szolgáló intézkedéseket, 4) a korlátozó intézkedéseket és 5) a lehetséges uniós támogatást a tagállamok jogszerű válaszaihoz. A dokumentum tartalmazza az ezen intézkedések bevezetésére vonatkozó eljárást is.[18]

A megelőző intézkedések közé sorolhatjuk az EU által támogatott bizalomépítő intézkedéseket, az uniós politikákkal kapcsolatos tudatosság fejlesztését és az EU támogatását a kiberterületen megvalósuló kapacitásépítés érdekében a harmadik országokban. Az együttműködési intézkedések tartalmazzák az EU által vezetett politikai és tematikus párbeszédeket vagy az EU küldöttségeinek részvételével folytatott diplomáciai lépéseket. A stabilitást szolgáló intézkedések közé a főképviselő vagy az EU Tanácsa nevében tett nyilatkozatok, a tanácsi következtetések vonatkozó részei, az uniós küldöttségek diplomáciai lépései és az EU által vezetett politikai és tematikus párbeszédek révén megfogalmazott jelzések tartoznak. A korlátozó intézkedések magukban foglalhatnak többek között utazási tilalmakat, fegyverembargót, pénzeszközök vagy gazdasági források befagyasztását. A lehetséges uniós támogatások között a dokumentum

[17] *Informatikai támadások: az EU készen áll az ellenintézkedésekre, ideértve a szankciókat is* (2017).

[18] Council of the European Union: *Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities — Approval of the Final Text.* (2017a). Brüsszel, 2017. október 9. (OR. en); Tanács (KKBP) 2019/797 határozata (2019. május 17.) *az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről*.

a lisszaboni szerződés kölcsönös segítségnyújtási klauzuláját (42.7 cikk) is megemlíti.[19]

Közös biztonság- és védelempolitika

2017-ben a globális stratégia végrehajtásával megkezdődött az európai védelmi együttműködés elmélyítését szolgáló kezdeményezések gyakorlati megvalósítása: így az állandó strukturált együttműködés (PESCO) alkalmazása, a védelmi kiadások koordinált éves felülvizsgálata (Co-ordinated Annual Review on Defence, CARD), a Katonai Tervezési és Végrehajtási Szolgálat (MPCC) létrehozása, illetve az Európai Bizottság által készített Európai Védelmi Cselekvési Terv (European Defence Action Plan, EDAP) alapján az Európai Védelmi Alap (EDF) felállításának előkészítése. Az Európai Védelmi Alap létrehozásával kapcsolatos tervek is kiemelt prioritásként tekintettek a kibervédelemi intézkedések és a kiberbiztonsággal kapcsolatos uniós kezdeményezések és így az unió különböző szakpolitikái közötti szinergiák támogatására.[20]

2016-tól kiemelt szerepet kapott a védelmi területen történő állandó strukturált együttműködés (Permanent Structured Cooperation – PESCO) megvalósítása. A 2017-től induló összesen 47 PESCO-projekt közül nyolc a kibertér kérdésköréhez kapcsolódik:

- a biztonságos európai szoftverirányítású rádió (European Secure Software Defined Radio – ESSOR);
- a kiberfenyegetésekre és kiberbiztonsági eseményekre való reagálással kapcsolatos információmegosztási platform (Cyber Threats and Incident Response Information Sharing Platform);
- kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok, valamint kölcsönös segítségnyújtás a kiberbiztonság területén (Cyber Rapid Response Teams and Mutual Assistance in Cyber Security);
- stratégiai vezetési és irányítási (C2-) rendszer a KBVP-missziók és -műveletek vonatkozásában (Strategic Command and Control [C2] Systems for CSDP Missions and Operations);

[19] Council of the European Union (2017a): i. m.

[20] Javaslat. Az Európai Parlament és a Tanács rendelete az Európai Védelmi Alap létrehozásáról. Brüsszel, COM(2018) 476, 2018/0254(COD).

– európai magas légköri léghajóplatform – kitartó hírszerzési, megfigyelési és felderítési képesség (European High Atmosphere Airship Platform [EHAAP] – Persistent Intelligence, Surveillance and Reconnaissance [ISR] Capability);
– egyetlen, taktikai vezetési és vezetés-irányítási (C2-) állomás a bevethető különleges műveleti egységek számára a kisebb együttes műveletekben (One Deployable Special Operations Forces [SOF] Tactical Command and Control [C2] Command Post [CP] for Small Joint Operations [SJO] – [SOCC] for SJO).[21]

Kibervédelmi szakpolitikai keret

A 2018-as kibervédelmi szakpolitikai keret szerint a korábbi évek eseményei még inkább rávilágítottak arra a tényre, hogy a nemzetközi közösségnek együtt kell működnie a konfliktusok megelőzése és a kibertér stabilitásának erősítése érdekében.

> „Az EU más nemzetközi szervezetekkel, elsősorban az ENSZ-szel (Egyesült Nemzetek Szervezete), az EBESZ-szel (Európai Biztonsági és Együttműködési Szevezet) és az ASEAN (Délkelet-ázsiai Nemzetek Szövetsége – Association of Southeast Asian Nation) regionális fórummal együtt elő kívánja mozdítani egy olyan, a konfliktusmegelőzésre, az együttműködésre és a kibertér stabilitásának erősítésére vonatkozó stratégiai keretet, amely magában foglalja a következőket: a nemzetközi jognak és különösen az ENSZ Alapokmányának teljes körű alkalmazása a kibertérben; a kibertérben tanúsított felelősségteljes állami magatartásra vonatkozó egyetemes, nem kötelező erejű normák, szabályok és elvek tiszteletben tartása; regionális bizalomépítő intézkedések kidolgozása és végrehajtása. Ezt a törekvést az uniós kibervédelmi szakpolitikai keretnek is támogatnia kell."[22]

Korlátozó intézkedések

2019-ben az EU jelentős előrehaladást ért el a rossz szándékú kibertevékenységekkel szembeni közös uniós kiberdiplomáciai eszköztár működőképessé és hatékonnyá

[21] PESCO Projects (2020).
[22] Európai Unió Tanácsa: *Uniós kibervédelmi szakpolitikai keret* (2018. évi, naprakésszé tett változat). Brüsszel, 2018. november 19. (OR. en). 14413/18. 8.

tétele érdekében. Az Európai Tanács 2018. júniusi és 2018. októberi következtetéseiben megfogalmazott célok elérése érdekében olyan uniós korlátozó intézkedések bevezetéséről döntött, amelyek segítik a kibertámadásokkal kapcsolatos reagálási és elrettentési képesség javítását. 2019. május 17-én döntés született az uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló KKBP-határozatról[23] és a tanácsi rendeletről.[24] A határozat a rossz szándékú és szándékos kibertevékenységekkel szembeni közös uniós korlátozó intézkedések alkalmazhatóságáról döntött, a rendelet pedig a jelentős hatású kibertámadások esetén szankciók alkalmazását teszi lehetővé az EU részéről.

Az új jogi keret így már lehetővé tette az EU számára, hogy szankciókat is kivethessen (például eszközök befagyasztása, utazási tilalom) az unióra vagy a tagállamaira külső fenyegetést jelentő kibertámadásoktól való elrettentés, valamint az azokra való reagálás érdekében.[25] A szankcióknak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük (a Tanács [EU] 2019/796 rendelete 15. cikk).

> „Az EU az alábbi elvek alapján fogja folytatni a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretének kidolgozását:
> – védeni kell az EU, az uniós tagállamok és az uniós polgárok sértetlenségét és biztonságát;
> – figyelembe kell venni az érintett állammal fennálló uniós külkapcsolatok tágabb összefüggéseit;
> – biztosítani kell a KKBP-célkitűzések elérését, az Európai Unióról szóló szerződésben foglaltakkal és az e célkitűzések elérése érdekében meghatározott megfelelő eljárásokkal összhangban;
> – az intézkedéseknek a tagállamok által közösen kialakított helyzetismereten kell alapulniuk, és meg kell felelniük az adott helyzet támasztotta igényeknek;
> – az intézkedéseknek arányosnak kell lenniük a kibertevékenység hatókörével, léptékével, időtartamával, intenzitásával, összetettségével, kifinomultságával és hatásaival;
> – tiszteletben kell tartani az alkalmazandó nemzetközi jogot és nem szabad alapvető jogokat és szabadságokat sérteni."[26]

[23] Tanács (KKBP) 2019/797 határozata.

[24] Tanács (EU) 2019/796 rendelete *a Tanács (EU) 2019/796 rendelete, (2019. május 17.), az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről.*

[25] Európai Bizottság: *Jelentés a dezinformációval szembeni közös cselekvési terv végrehajtásáról, közös közlemény az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának.* Brüsszel, 2019. június 14. JOIN (2019) 12 final. 9.

[26] Európai Unió Tanácsa: *Tervezet – a Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről („Kiberdiplomáciai eszköztár").* Brüsszel, 2017b. június 7. (OR. en).

Az EU–NATO-együttműködés

A lisszaboni szerződés hatálybalépését követően és az uniós diplomáciai intézményrendszer, a képességek és hatáskörök bővülésének köszönhetően az EU nemzetközi jelenléte és szerepe folyamatosan erősödött. Az Európai Unió a hagyományos normatív szerepén túl a kiberdiplomácia területén megvalósított stratégiai partnerségi kapcsolatok kialakításában is érdekeltté vált. E bilaterális kapcsolatok jelentős szerepet játszanak a multilaterális együttműködési formák megerősítésében.[27] Napjainkban az együttműködésen alapuló, a nyugati inspirációjú multilaterális keretekre épülő nemzetközi rendszer szétfeszülni látszik. Mivel a kibertérben is új regionális és globális hatalmak felemelkedése várható, az EU továbbra is a multilaterális együttműködési formák fenntartásában és megerősítésében érdekelt.

A 2015-ös, kiberdiplomáciáról szóló tanácsi következtetésekkel összhangban az EU a legfontosabb partnerekkel és a nemzetközi szervezetekkel stratégiai együttműködést kíván kialakítani, és hangsúlyozza, hogy a kibertérrel kapcsolatos kérdésekben hozott szakpolitikai döntések többsége szükségessé teszi az aktív nemzetközi párbeszédet, együttműködést és koordinációt.[28] Mindezzel összefüggésben a NATO-val kiépített kapcsolatok jelentősége is fokozatosan növekedett.

Az EU és a NATO közötti együttműködés területén kialakított folyamat valódi lendületet 2016-tól kapott. Az EU globális stratégiájának elfogadását követő végrehajtási folyamatban a két nemzetközi biztonsági szervezet között a kiberbiztonság és kibervédelem területén egyre intenzívebb kapcsolat jött létre.[29] A globális stratégia hangsúlyozza, hogy míg a NATO a kollektív védelem elsődleges keretét biztosítja a legtöbb tagállam számára, addig az EU elsősorban az olyan belső és külső kihívásokkal szemben kíván fellépni, mint a terrorizmus, a hibrid fenyegetések, a kiber- és energiabiztonság, a szervezett bűnözés és a külső határok igazgatása.

2016. július 8-án a NATO-csúcson Varsóban az EU részéről az Európai Tanács elnöke és az Európai Bizottság elnöke, illetve a NATO főtitkára együttes nyilatkozatot írt alá az EU és a NATO közötti együttműködésről. A nyilatkozat

[27] Renard (2018): i. m. 5.

[28] Európai Unió Tanácsa (2015): i. m.

[29] Európai Külügyi Szolgálat: *Közös jövőkép, közös fellépés: Erősebb Európa. Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan.* 2016.

aláírását követően a két szervezet közötti együttműködés új lendületet kapott, és kiterjed a hibrid fenyegetések elleni küzdelemre; a kiberbiztonság és -védelem területeire is.[30] Az együttes nyilatkozat konkrét célkitűzéseket fogalmazott meg a kibervédelmi együttműködés előmozdítása érdekében: megerősíteni a kibervédelmi interoperabilitást a missziók és műveletek során; az együttműködés erősítése a képzéseken és a gyakorlatokon; a kibervédelmi kutatásokkal és technológiai innovációval kapcsolatos együttműködés előmozdítása; valamint a kibernetikus szempontok beépítése a válságkezelésbe.[31]

2016 februárjában az EU és a NATO képviselői aláírták az EU hálózatbiztonsági vészhelyzeteket elhárító csoportja (Computer Emergency Response Teams – CERT) és a NATO hálózatbiztonsági incidenskezelő csoportja (NATO's Computer Incident Response Capability – NCIRC) közötti technikai megállapodást. A megállapodás célja a technikai információk megosztásának megkönnyítése a számítógépes események megelőzése érdekében, illetve a kiberbiztonsági események felderítése és az azokra való reagálás erősítése mindkét szervezetben. Az e területeken megvalósuló tevékenységek mind a mai napig a két szervezet közötti együttműködés alapját képezik.

Az együttműködés másik legfontosabb eredménye, hogy – finn kezdeményezésre, de az EU és a NATO támogatásával – 2017-ben Helsinkiben létrejöhetett a Hibrid Fenyegetések Elleni Kiválósági Központ (European Centre of Excellence for Countering Hybrid Threats), amelynek feladata az elsősorban Oroszország felől érkező kiberbiztonsági kihívások, a dezinformációs műveletek és a stratégiai kommunikáció elemzése, valamint a kihívásokra hatékony és közösen koordinált válaszok kidolgozása.[32] Az új központ felállítása lehetőséget biztosított az Észak-atlanti Tanács és az uniós Politikai és Biztonsági Bizottság közötti informális találkozók megszervezésére, és így a hibrid fenyegetéssel szembeni koordinált fellépés kidolgozására.[33]

A 2017. novemberi második előrehaladási jelentésben első helyen szerepelt az új központ felállítása. A jelentés emellett kiemelte a tengerbiztonsági, valamint a kiberbiztonsági és a védelmi fejlesztési területeken elért eredményeket, illetve ezek közül a képzések és gyakorlatok területén megvalósuló együttmű-

[30] Európai Unió Tanácsa: *EU–NATO együttműködés: A Tanács következtetéseket fogadott el az együttes nyilatkozat végrehajtása céljából.* (2016. december 6.).

[31] Council of the European Union (2016): i. m.

[32] Hybrid CoE: *European Centre of Excellence for Countering Hybrid Threats* (é. n. a).

[33] Hybrid CoE (2018): *Hybrid CoE Supports Informal NAC-PSC Discussion* (2018. szeptember 28.).

ködések fontosságát. A NATO-alkalmazottak például részt vehettek az uniós ügynökség, az ENISMA (European Union Agency for Cybersecurity, Európai Uniós Kiberbiztonsági Ügynökség, a továbbiakban: ENISMA) kiberbiztonsági gyakorlatán. A fejlesztési duplikációk elkerülése érdekében folyamatossá vált az együttműködés.[34]

Az önállóan működő központ munkájába 2020 májusáig Ausztria, Ciprus, a Cseh Köztársaság, Dánia, az Egyesült Királyság, Észtország, Finnország, Franciaország, Görögország, Hollandia, Kanada, Lengyelország, Lettország, Litvánia, Luxemburg, Magyarország, Montenegró, Németország, Norvégia, Olaszország, Portugália, Románia, Szlovénia, Spanyolország, Svédország, Törökország és az USA kapcsolódott be. Fontos megjegyezni, hogy az új együttműködési forma a semleges EU-tagállamok (Ausztria, Finnország és Svédország), illetve a nem uniós NATO-tagok (USA, Kanada és Norvégia) számára is lehetővé tette a csatlakozást. A meglévő ellentétek következtében kezdetben Ciprus és Törökország nem vett részt a megvalósításban.[35]

2017-ben és 2018-ban a NATO és az Európai Unió párhuzamos és összehangolt gyakorlatokat folytattak egy hibrid forgatókönyvre reagálva, annak érdekében, hogy javítsák az EU válaszadási képességét a hibrid fenyegetés esetén, és tovább fejlesszék az EU és a NATO közötti együttműködést. 2017-ben NATO-irányítással, 2018-ban pedig az unió vezetésével hajtották végre a gyakorlatokat. A 2018-as „EU-HEX-ML 18 (PACE)" gyakorlat jelentősen segítette a szervezetek személyi állományai közötti együttműködést.[36] 2019-ben a jól bevált gyakorlat folytatódott, és a NATO CMX 19 gyakorlat is kiterjedt a személyi állományok közötti együttműködésre az EU intézményeivel (EKSZ, EK és a Tanács).[37]

[34] Council of the European Union: *Second progress report on the implementation of the common set of proposals endorsed by NATO and EU.* (2017b. november 29.).

[35] Hybrid CoE: *European Centre of Excellence for Countering Hybrid Threats. What is Hyrid CoE?* (É. n. b).

[36] European External Action Service 2018.

[37] George Allison: NATO Conducts Crisis Management Exercise. *UK Defence Journal.* 2019.

Következtetések

Az EU döntéshozói kezdetben elsősorban gazdasági kérdésként tekintettek a digitalizációval és az IKT-eszközök használatával kapcsolatos kérdéskörre. A 2010-es évek elejétől azonban megkezdődött e terület biztonságiasításának folyamata, amelyben mérföldkőnek a 2013-as kiberbiztonsági stratégia tekinthető.[38]

Mivel az IKT-eszközök használata az élet minden területére kiterjed, így nem véletlen, hogy napjainkban a kibertér a nemzetközi kapcsolatok kiemelt területévé vált. A nagyhatalmakhoz hasonlóan az uniós külpolitika szerves részét képezik a kiberdiplomáciával kapcsolatos területek. Az elmúlt évtizedekben az ENSZ, a NATO vagy akár az EBESZ hasonló törekvéseivel párhuzamosan az Európai Unió is megkezdte a kiberdiplomáciával és a kibervédelemmel összefüggő eszköz- és intézményrendszerének kiépítését.

Nemzetközi szinten az EU a kibertérben a konfliktusmegelőzés és a stabilitás érdekében a speciálisan alkalmazandó nemzetközi jog, különösen az ENSZ Alapokmánya és a nemzetközi humanitárius jog szigorú alkalmazását és a felelősségteljes állami magatartás nem kötelező érvényű egyetemes számítógépes normáinak, szabályainak és alapelveinek teljes végrehajtását határozta meg legfőbb stratégiai céljai között.[39]

Felhasznált irodalom

Allison, George: NATO Conducts Crisis Management Exercise. *UK Defence Journal*, 2019. május 9. Online: https://ukdefencejournal.org.uk/nato-conducts-crisis-management-exercise/.

Barrinha, André – Thomas Renard: Cyber-diplomacy: The Making of an International Society in the Digital Age. *Global Affairs,* 3. (2017), 4–5. 1–13. Online: https://doi.org/10.1080/23340460.2017.1414924.

Carrapico, Helena – Andre Barrinha: European Union Cyber Security as an Emerging Research and Policy Field. *European Politics and Society,* 19. (2018), 3. 299–303. Online: https://doi.org/10.1080/23745118.2018.1430712.

[38] Christou (2018): i. m. 13.

[39] Rehrl (2018): i. m. 25.

Cavelty, Myriam Dunn: Europe's Cyber-power. *European Politics and Society,* 19. (2018), 3. 1–17. Online: https://doi.org/10.1080/23745118.2018.1430718.

Christou, George: The Collective Securitisation of Cyberspace in the European Union. *West European Politics,* 42. (2019), 2. 1–24. Online: https://doi.org/10.1080/01402382.2018.1510195.

Council of the European Union: *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation*. 2016. Online: www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf.

Council of the European Union: *Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities – Approval of the Final Text.* Brussels, 9 October 2017 (OR. en). 2017a. Online: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf.

Council of the European Union: *Second Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU.* 2017b. Online: www.consilium.europa.eu/media/35577/report-ue-nato-layout-en.pdf.

Európai Bizottság: *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér.* JOIN/2013/01 végleges. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52013JC0001.

Európai Bizottság: Európai digitális egységes piaci stratégia. Brüsszel, COM(2015) 192 végleges (2015. május 6.). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52015DC0192&from=HU.

Európai Bizottság: *Jelentés a dezinformációval szembeni közös cselekvési terv végrehajtásáról. Közös közlemény az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának.* Brüsszel, JOIN (2019) 12 végleges (2019. június 14.). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52019JC0012&from=EN.

Európai Külügyi Szolgálat: *Közös jövőkép, közös fellépés: Erősebb Európa. Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan*. 2016. Online: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_hu_.pdf.

Európai Parlament és a Tanács (EU) 2016/1148 irányelve az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19.).

Európai Unió Tanácsa: *A Tanács következtetései a kiberdiplomáciáról,* Brüsszel, 2015. február 11. Online: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf.

Európai Unió Tanácsa: *EU–NATO-együttműködés: a Tanács következtetéseket fogadott el az együttes nyilatkozat végrehajtása céljából*. (2016. december 6.). Online: www.consilium.europa.eu/hu/press/press-releases/2016/12/06/eu-nato-joint-declaration/.

Európai Unió Tanácsa: *Informatikai támadások: az EU készen áll az ellenintézkedésekre, ideértve a szankciókat is* (2017a. június 19.). Online: www.consilium.europa.eu/hu/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.

Európai Unió Tanácsa: *Tervezet – a Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről („Kiberdiplomáciai eszköztár").* Brüsszel, 2017. június 7. (OR. en). Online: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/hu/pdf.

Európai Unió Tanácsa: *Uniós kibervédelmi szakpolitikai keret (2018. évi naprakésszé tett változat).* Brüsszel, 2018. november 19. (OR. en) 14413/18. Online: http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/hu/pdf.

European External Action Service: *Crisis preparedness: EU launches civil-military crisis management exercise,* Brüsszel, 2018. november 16. – 15:25, UNIQUE ID: 181116_7. Online: https://eeas.europa.eu/headquarters/headquarters-Homepage/53926/crisis-preparedness-eu-launches-civil-military-crisis-management-exercise_en.

Hybrid CoE: *Hybrid CoE Supports Informal NAC-PSC Discussion* (2018. szeptember 28.). Online: www.hybridcoe.fi/news/hybrid-coe-supports-informal-nac-psc-discussion/.

Hybrid CoE: *European Centre of Excellence for Countering Hybrid Threats* (é. n. a). Online: www.hybridcoe.fi/.

Hybrid CoE: *European Centre of Excellence for Countering Hybrid Threats. What is Hyrid CoE?* (é. n. b). Online: www.hybridcoe.fi/what-is-hybridcoe/.

Javaslat az Európai Parlament és a Tanács rendelete, az Európai Védelmi Alap létrehozásáról. Brüsszel, COM(2018) 476, 2018/0254(COD). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52018PC0476.

PESCO: *PESCO Projects* (2020). Online: https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/.

Rehrl, Jochen (szerk.): *Handbook on Cyber Security. The Common Security and Defence Policy of the European Union*. Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2018. Online: https://publications.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1.

Renard, Thomas: EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain. *European Politics and Society,* 19. (2018), 3. 321–337. Online: https://doi.org/10.1080/23745118.2018.1430720.

Smith, Gordon – Allen Sutherland: The New Diplomacy: Real-Time Implications and Applications. In Evan H. Potter (szerk.): *Cyber-diplomacy: Managing Foreign Policy in the Twentyfirst Century.* Quebec, McGill-Queen's University Press. 2002. 151–177.

Stevens, Tim – Kevin O'Brien: Brexit and Cyber Security. *The RUSI Journal*, 164. (2019), 3. 22–30. Online: https://doi.org/10.1080/03071847.2019.1643256.

A Tanács (EU) 2019/796 rendelete, (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.LI.2019.129.01.0001.01.HUN&toc=OJ:L:2019:129I:TOC 4.).

Tanács (KKBP) 2019/797 határozata (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019D0797&from=EN.

[Vákát oldal]

Molnár Dóra

Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon

A világ domináns hatalmai meghatározó szerepet játszanak a biztonság valamennyi területének formálásában, s nincs ez másképp a kiberbiztonságot illetően sem. Jelenleg azonban nincs olyan átfogó nemzetközi egyezmény, amely az államok kibertérben tanúsítandó magatartási szabályait rögzítené és a kibertér használatát érintő kérdéseket szabályozná. Bár kétségkívül hatalmas diplomáciai siker volna egy nemzetközi kiberegyezmény megalkotása, kérdés, hogy egyáltalán szükséges-e? A szakértők egy csoportja úgy véli, hogy erre nem fog sor kerülni a gyors technológiai változások okozta újabb és újabb kihívások miatt, valamint azért, mert nehezen lehet ellenőrizni az egyezményben foglaltak betartását. Helyette az informális együttműködést és a stratégiai elrettentést tartják járható útnak. A szakértők másik csoportja viszont kitart egy nemzetközi egyezmény megalkotásának szükségessége mellett, és sikeres példaként említi a 20. századi fegyverzetkorlátozási megállapodásokat. Egy nemzetközi kiberrezsim ugyanis lehetőséget teremtene az államoknak a fő kérdések megvitatására, és hozzá tudna járulni a hatékony kiberelrettentéshez.

A kiberrezsim ellen számos érv hozható fel.[1] Az egyik, hogy lehetetlen beépíteni monitoring- és kényszerítő mechanizmusokat a kiberfegyverek tulajdonságai miatt. Ugyanis az ellenőrzésnek még a fegyverek fejlesztésének időszakában meg kellene kezdődnie, és nem magát a fegyverhasználatot kellene ellenőrizni.[2] További ellenérvek a tárgyalási időszak hosszúsága, a gyors technológiai változásokhoz való alkalmazkodóképesség hiánya, valamint az, hogy korai volna még egy ilyen egyezmény megalkotása. Az egyezmények ugyanis azt követően

[1] Farad Nabeel: International Cyber Regime: A Comparative Analysis of the US-China-Russia Approaches. *Strategem,* 1. (2018), 2. 8–27.

[2] Minderre Eilstrup-Sangiovanni az ex-ante és ex-post kifejezéseket használja. Lásd Mette Eilstrup-Sangiovanni: Why the World Needs an International Cyberwar Convention. *Philosophy & Technology,* 31. (2018), 3. 399.

https://doi.org/10.36250/01008_04

szoktak köttetni, hogy az adott technológiákat már használták. Ezenkívül egy ilyen egyezménynek csak az igazán elkötelezett államok válnának részeseivé, és még számukra is egyfajta kényszerítést jelentene a részvétel.

Elképzelhető, hogy a nemzetközi kiberrezsim lazább szabályozási struktúrák kialakítása mentén is felépíthető lehet. Ez esetben a *bizalomépítő intézkedéseknek* lehet központi szerepe, amelyet az EBESZ és az ASEAN[3] elmúlt évtizedes gyakorlata is bizonyít.

2009-től, miután az Obama-adminisztráció bejelentette új nemzetközi kiberpolitikáját, az Egyesült Államok vált az EBESZ kiberagendája vezető államává. A szervezet kibertevékenysége és a stratégiai kiberbiztonsági párbeszéd alapjait 2010 júniusában rakták le a Biztonsági Együttműködési Fórum és az Állandó Tanács közös találkozóján. Az Egyesült Államok már ekkor javaslatot tett az állami viselkedési normák tárgyalására, majd egy évvel később a bizalomépítő intézkedések formálására. Ezzel párhuzamosan az Egyesült Államok és Oroszország tárgyalásokat folytatott a kiberbizalom-építő intézkedések kezdeti körét illetően,[4] majd 2013-ban mindezt egyezségben is rögzítették. A megállapodás lényegi elemei a következők:[5]

- a CERT-ek között kommunikációs csatornák létrehozása és információmegosztási megállapodások megkötése a kritikus információs rendszerek védelme érdekében;
- az országok nukleáriskockázat-csökkentési központjai közötti közvetlen kommunikációs csatorna használatának engedélyezése (az Egyesült Államok washingtoni Külügyminisztériuma és Oroszország moszkvai Védelmi Minisztériuma között);
- közvetlen biztonságos telefon-összeköttetés megteremtése az amerikai kiberbiztonsági koordinátor és az orosz Biztonsági Tanács főtitkárhelyettese között, valamint
- egy hónapon belül egy kétoldalú munkacsoport felállítása az infokommunikációs technológiára leselkedő veszélyekre.

[3] Az ASEAN esetében a Regionális Fórum (ASEAN Regional Forum) keretein belül tárgyalják a kérdéskört.

[4] Katharina Ziolkowski (szerk.:): *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*. NATO CCDCOE Publication, Tallinn, 2013. 519.

[5] The White House: *Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building* (2013. június 17.).

Az EBESZ keretein belül kialakítandó lépések körét illetően az egyes államok különböző javaslatokkal álltak elő. Németország a bizalomépítő intézkedések két nagy csoportját különböztette meg: az átláthatósággal és a stabilitással összefüggő intézkedések körét. Míg az előbbi körébe tartozott a kockázatok csökkentése és az információcsere (az alkalmazandó nemzetközi jog, a szervezeti struktúrák, a stratégiák és a partnerek vonatkozásában), addig az utóbbi körben a közös kibergyakorlatokat, valamint a válságkommunikációs csatornák és a CERT-ek felállítását nevesítették.[6]

Oroszország szélesebb körű listát készített. A 2011-ben kiadott, az *Orosz Föderáció fegyveres erejének információs térben való tevékenységére vonatkozó fogalmi kérdések (Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space)* című dokumentum alapján a fegyveres erők feladata az információs tér katonai alkalmazására vonatkozó bizalomépítő intézkedések körének meghatározása, majd 2012-ben egy újabb dokumentumban tovább részletezték az intézkedések körét. Ezek közt szerepel a nemzeti szabályok harmonizálása, egy nemzetközileg elfogadott információbiztonsági terminológia-rendszer kidolgozása, valamint a rendőri szervek közötti nemzetközi együttműködés szervezeti kereteinek megteremtése.[7]

Mindezek komoly erőfeszítések a nemzetközi közösség részéről, azonban nem szabad megfeledkezni arról, hogy egy nemzetközi kiberrezsim is csak akkor lehet sikeres, ha az államok minél szélesebb köre vesz benne részt. A kiberbiztonság vezető államainak részvétele elengedhetetlenül szükséges, jelenleg azonban még komoly csatározások zajlanak a nyugati világ és a Kína vezette feltörekvő államok között a rezsim legalapvetőbb kérdéseit illetően is. Elég, ha arra gondolunk, hogy 2018 novemberében több mint 50 állam (valamint 130 magánvállalat és 90 tudományos testület) aláírta a kiberhadviselés szabályai megalkotásának szükségességéről szóló nemzetközi kiberbiztonsági paktumot, azonban az Egyesült Államok, Kína, Oroszország, Észak-Korea, Izrael, Irán, Ausztrália és Szaúd-Arábia, valamint a Huawei és a ZTE[8] nem voltak az aláírók között.[9] Jelen tanulmány célja, hogy bemutassa, mit jelentenek

[6] *Cyber Security: Confidence and Security-Building Measures (CSBMs)* (é. n.).

[7] Sergey Fedosov: *Statement by the Russian Participant at the UNIDIR Cyber Security Conference 'What does a Stable Cyber Environment Look Like?* UNIDIR, Geneva, 2012. november 8–9.

[8] A Huawei és a ZTE Kína két legnagyobb távközlési cége, egyúttal a világ vezető információs és kommunikációs technológiai vállalatai.

[9] *UK and 50 Nations Sign Cyber Security Pact*. (2018. november 13.).

a gyakorlatban a kiberdiplomáciai manőverek az egyes országok vonatkozásában. A tanulmány a három vezető kiber-világhatalom, az Egyesült Államok, Kína és Oroszország főbb kiberdiplomáciai lépéseit elemzi, majd a következő fejezetben kitér az „öreg kontinens" vezető államainak ez irányú lépéseire is.

Az Egyesült Államok mint kiberdiplomáciai óriás

Az Egyesült Államok kiberdiplomáciáját bemutató rész rövidebb a további két országot ismertető részhez képest. Ennek indoka egyrészt az, hogy a másik két állam tárgyalása kapcsán számos, az amerikai kiberpolitikával kapcsolatos kérdést érintek, másrészt pedig az amerikai kiberdiplomácia olyan kiterjedt elméleti hátterű, és olyan széles körű a gyakorlata, hogy annak részletes bemutatása meghaladná jelen fejezet terjedelmi korlátait. Ezért a hivatalosan 2009-ben útjára indított amerikai kiberdiplomáciai folyamatoknak csak a legfontosabb állomásait foglalom össze.[10]

Az amerikai kiberdiplomácia sarokkövét a 2011 májusában az ország kibertérre vonatkozó nemzetközi stratégiájának[11] elfogadása jelentette. A stratégia kiadásával az Egyesült Államok a kiberdiplomácia kérdését szilárd alapokra helyezte, és felállította a szervezeti struktúrát is. A dokumentum maga is definiálja a kiberdiplomácia fogalmát: felöleli az amerikai érdekek széles spektrumát a kibertérben – ez nemcsak a kiberbiztonságot és az internetszabadságot foglalja magában, hanem az internetkormányzást, valamint az internet, az innováció és a gazdasági növekedés katonai célú használatát is. A Külügyminisztériumban létrehozták a Kiberkoordinátori Hivatalt (Office of the Coordinator for Cyber Issues), amelynek első (és egyben utolsó) vezetője Christopher Painter lett. A hivatal az amerikai elsőség bizonyítékaként szolgálhatott a kibertérben (ahogy általában a globális erőtérben is). Ez volt a világon az első ilyen szervezet, amelyet azóta más országok külügyi apparátusai is mintaként követtek. A kiberdiplomácia az amerikai kül- és nemzetbiztonsági politika kritikus kom-

[10] A digitalizáció az Egyesült Államok közigazgatásában hosszú múltra tekint vissza, de igazi fordulópontot e tekintetben is a 2001. évi terrortámadás jelentett. A Külügyminisztériumban 2003-ra készült el az első átfogó koncepció az e-diplomácia fejlesztésére, amelyet további fejlesztések és számos előrelépés követett. Részletesebben lásd Nyáry Gábor: A digitális állam a külpolitikai térben. A Twittertől az adattudományig. *Új Magyar Közigazgatás,* 12. (2019), 2. 75–82.

[11] *International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World.* (2011. május).

ponensévé vált. A hivatal hat és fél éves működése alatt számos két- és többoldalú partneri kapcsolatot épített ki, és világszerte tárgyalt formálisan vagy informális módon a kiberkérdések széles körét érintve.[12] Több szakértői javaslat is napvilágot látott a további kiberdiplomáciai építkezés szükségességéről, ám a Trump-adminisztráció másképp vélekedett e kérdés jövőjéről, és Tillerson külügyminiszter a hivatal megszüntetéséről (és az alkalmazottaknak a minisztérium Gazdasági és Üzleti Ügyek Irodájába történő áthelyezéséről) döntött. Ezzel hatalmas űr keletkezett, amelyet egy 2017. májusi elnöki rendelettel[13] elrendelt új kiberstratégia megalkotásával kívántak betölteni, annak elmaradása azonban további bizonytalanságokhoz vezetett a diplomáciai testületek körében. Az amerikai kiberpolitikai-kiberdiplomáciai szervezet átalakításai valójában belső szervezeti-hatalmi érdekcsoportok küzdelmének eredői. Leegyszerűsítve azt mondhatjuk, hogy a 2010-es évek második felében komoly küzdelem indult meg az amerikai külügyi államigazgatáson belül azért, hogy az ország kiberpolitikájának alakításában melyik érdek, melyik ágazat, melyik szempont legyen a döntő. A széles körű szakmai-politikai viták és egyeztetések nyomán 2017 szeptemberében kétpárti megegyezéssel sikerült a kérdést szabályozni hivatott törvényt (Cyber Diplomacy Act of 2017) megalkotni, majd 2019. január 24-én beterjeszteni a Kongresszus elé, azonban azt sem a Képviselőház, sem a Szenátus nem fogadta el a külügyi bizottság támogatása ellenére sem. Ennek oka az volt, hogy valójában nem sikerült a szemben álló érdekcsoportok közötti ellentéteket feloldani benne. A törvényjavaslat szerint az ország hozzá kíván járulni egy nyitott, interoperábilis, megbízható, korlátlan és biztonságos internethez, amelyet a többszereplős *(multi-stakeholder)* modell alapján kormányoznak. Az Egyesült Államok tehát továbbra is kitart a multilaterális megközelítés elvetésében, szembehelyezkedve ezzel a Kína és Oroszország vezette másik táborral. A stratégia mindezt tovább tetézi azzal, hogy olyan országokat és csoportokat nevesít, amelyek fenyegetést jelentenek a kibertérben: első helyen Oroszország, majd Kína, Irán és Észak-Korea, a terrorista, valamint a bűnözői csoportok állnak. A dokumentum ugyanakkor kiemeli a kétoldalú kapcsolatok fontosságát, és nevesíti

[12] Christopher Painter: The Rise of the Internet and Cyber Technologies Constitutes One of the Central Foriegn Policy Issues of the 21st century. *The Foreign Service Journal,* 2018. június.

[13] *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (2017. május 11.).

a 2014 és 2018 között megkötött bilaterális kiberszerződéseket.[14] A szervezeti téren keletkezett anomália helyreállítására új központi kiberszervként fel kell állítani a Nemzetközi Kiberpolitikai Hivatalt (Office of International Cyberspace Policy), amelyet az elnök által kinevezett kibernagykövet fog irányítani.

A folytatást illetően annyi bizonyos volt, hogy nem lesz elég egy új stratégia megalkotása és egy új hivatal felállítása az országot a kibertérben érő konfrontációk és dilemmák megválaszolására, a részletkérdések kidolgozása azonban még várat magára. Ha az Egyesült Államok sikereket kíván elérni e téren is, a nyílt konfrontáció mindenképp kerülendő mind Kínával, mind Oroszországgal; ezen államokkal konzisztens politikát kell folytatni, amelyet kommunikálni kell a szövetségesek és világ más államai felé is. A megoldás az lehet, ha az Egyesült Államoknak sikerül rábírnia az európai, az afrikai, dél-amerikai és a közép-, dél-, délkelet-ázsiai államokat, hogy válasszanak néhány vezető államot a térségükből – ellensúlyozva ezzel a kínai és orosz dominanciát.[15]

Kína és a kiberdiplomácia: egy újabb sikertörténet?

Nem túlzás azt állítani, hogy Kína a diplomácia területén is átvette a vezető szerepet. Ezt jelzi a diplomáciai hálózat kiterjedtsége, amely egyúttal a globális befolyás fokmérője is. 2019-re Kínának világszerte 276 diplomáciai állomáshelye lett, megelőzve ezzel az addig vezető Egyesült Államokat is, amelynek „csak" 273 kirendeltsége van.[16] Ez a nagyhatalmi versengésnek is fordulópontja lehet, mert Kína minden bizonnyal készen áll arra, hogy globális erejét ténylegesen is alkalmazza. Egyes vélemények szerint Kína már nem pusztán kibernagyhatalommá, hanem az elmúlt pár évben kiber-szuperhatalommá nőtte ki magát.[17] Mindez nem lehet véletlen, ha a kínai elnök 2016-ban elhangzott szavaira tekintünk: kiberbiztonság nélkül nincs nemzeti biztonság, és informatizáció nélkül nincs modernizáció.[18]

[14] Az országok között szerepel többek között Kína, Japán, az Egyesült Királyság, Franciaország, Izrael, Dél-Korea és Ausztrália.

[15] Justin Chapman: *Threats and Opportunities of Cyber Diplomacy at PolicyWest*. 2019. december 24.

[16] Bonnie Bley: *The New Geography of Global Diplomacy. China Advances as the United States Retreats*. 2019. november 27.

[17] Adam Segal: *Year in Review: Chinese Cyber Sovereignity in Action*. 2018. január 8.

[18] *Xi Jinping Gives Speech at Cybersecurity and Informatization World Conference* (2016. április 19.).

A diplomáciai lépések megalapozását a 2017 márciusában kiadott *Együttműködés a kibertérben nemzetközi stratégia* (International Strategy of Cooperation on Cyberspace)[19] című új kiberbiztonsági dokumentum képezi. A stratégia már nevében is azt sugallja, hogy Kína a kibertérbeli konfliktusok megoldását elsősorban az együttműködésre építve, békés eszközökkel képzeli el – s e körben kiemelt szerepe van a kiberdiplomáciának.

A stratégia rögzíti, hogy a kibertér jövője valamennyi ország kezében van, s bár nő a digitális szakadék az egyes országok és régiók közt, a nemzetközi közösségnek mégis egységes egészként kell együttműködnie a kölcsönös tisztelet és a kölcsönös megértés szellemében, hogy biztosítsák az internet világának szuverenitását. S itt eljutunk a kulcsfogalomig, a szuverenitás fogalmához. A szuverenitás a négy alapelv egyikeként jelenik meg a dokumentumban (a béke, a megosztott kormányzás és a megosztott előnyök mellett), s ezzel összefüggésben az internet szuverenitásának fontossága áthatja a stratégia egészét – nem meglepő módon, hiszen Kína esetében egy demokratikusnak látszó köntösbe bújt autoriter rezsimmel állunk szemben, így nem véletlen, hogy a be nem avatkozás elve mint egyik elsődleges vezérlő elv van jelen. A stratégia definiálja az internetszuverenitás (vagy kiberszuverenitás) fogalmát is: az államoknak tiszteletben kell tartaniuk egymás jogát, hogy maguk válasszák meg a kiberfejlődés útját, a kiberszabályozás modelljét és az internetre vonatkozó politikájukat, és biztosítani kell, hogy egyenlő mértékben részt vehessenek a nemzetközi kibertér kormányzásában. Egyik állam sem törhet kiberhegemóniára, nem avatkozhat be más állam belügyeibe, és nem támogathat más állam nemzetbiztonságát aláásó kibertevékenységet. A szuverenitás kérdésköre a stratégiai célok között is előkerül, mégpedig az első helyen mint a „szuverenitás és a biztonság garantálása". Az ország kiemelten a békés eszközök igénybevételével képzeli el ezen stratégiai céljának elérését, és célja annak elkerülése, hogy a kibertér új hadszíntérré váljon. Ennek némiképp ellentmond, ugyanakkor nem véletlen, hogy Kína a védelmi kiberképességeit a továbbiakban is fejleszteni (és minden bizonnyal használni is) fogja, és a hadseregnek fontos szerepet szán a kibertéri feladatok ellátásában. Önálló kibererő létrehozását is tervezi.

A stratégiai célok közül kiemelem a másodikként nevesített nemzetközi szabályrendszer megalkotását, valamint a harmadikként szereplő tisztességes internetkormányzás kérdéskörét. Az előbbi vonatkozásában Kína kiáll amellett,

[19] *International Strategy of Cooperation on Cyberspace.* A Kínai Népköztársaság Külügyminisztériuma, 2017. március 1.

hogy az ENSZ keretein belül létre kell hozni egy egyetemlegesen elfogadott nemzetközi szabály- és magatartásinorma-rendszert, amely az államok kibertérbeli magatartásának kereteit rögzíti. Az utóbbival összefüggésben pedig úgy fogalmaz a stratégia, hogy egy „multilaterális, demokratikus és transzparens", az egyenlő részvétel és a közös döntéshozatal elvére épülő globális internetkormányzásra van szükség. A multilaterális jelző kiemelést érdemel, ugyanis ez jelenti az egyik fő nézeteltérést a nyugati hatalmakkal, akik az internetkormányzás többszereplős *(multi-stakeholder)* modelljét kívánják megvalósítani.

A kínai külpolitikának három fő célja van: csökkenteni a fenyegetést, amelyet az internet és az információáramlás jelenthet a belső stabilitásra és a rendszer legitimációjára; oly módon formálni a kiberteret, hogy az ország politikai, katonai és gazdasági befolyása növekedjen; valamint ellensúlyozni az amerikai túlsúlyt, Kína mozgásterének növelése mellett.[20] Ebbe a célrendszerbe illeszkednek az ország kiberdiplomáciai lépései is. Kína Hszi Csin-ping elnöksége alatt változtatott korábbi reaktív és védekező kiberpolitikáján, és az aktív kiberdiplomácia alkalmazása mellett döntve igen rövid idő alatt építette ki kiberdiplomáciai csatornáit, amelyeket nagyon eredményesen használ céljai eléréséhez. A kiberbiztonság Peking számára egyszerre képes biztosítani a terrorizmus jelentette fenyegetés ellensúlyozását, a regionális befolyás garantálását és a kétoldalú kapcsolatainak építését az olyan fontos partnerállamokkal, mint az Egyesült Államok. Kína 2014-ben rendezte meg az első wuzheni internet-világkonferenciát. Akkor Kína elnöke mindössze egy üdvözlő üzenetet küldött a rendezvény résztvevőinek. Egy évvel később Hszi Csin-ping személyesen vett részt a konferencián és beszédet mondott, jelezve ezzel a kiberbiztonsági kérdések megnövekedett fontosságát Kína számára. A kínai elnök beszédének középpontjában az internetszuverenitás kérdése mellett a globális internetkormányzás kérdésköre, azon belül is a multilateralitás propagálása állt. Nem kis diplomáciai gesztusnak számított, hogy Dmitrij Medvegyev orosz elnök konferenciabeszédében azonnal reagált a kínai elnök szavaira, és támogatásáról biztosította őt.[21] A két ország egyébiránt igen jelentős sikert tudhatott magának már a konferenciát megelőző napon, amikor sikeres lobbitevékenységüknek köszönhetően a 70/125. sz. ENSZ

[20] Adam Segal: Chinese Cyber Diplomacy in a New Era of Uncertainty. A Hoover Institute Essay. *Aegis Paper Series,* (2017), 1703. 1.

[21] David Bandurski: *China's Cyber-diplomacy*. 2015. december 21.

közgyűlési határozat szövegébe bekerült a multilaterális kifejezés – kiváltva ezzel a nyugati világ ellenérzését.[22]

A kínai kiberdiplomácia a belügyekbe való be nem avatkozás alapelvének és az egyenlő részvétel elvének elismerésében, a kapacitásépítés és a fejlesztési támogatás fontosságában, valamint az ENSZ és más nemzetközi intézmények támogatásában gyökerezik. Mindezek eredője pedig a kiberszuverenitás vagy internetszuverenitás kérdése, és ez a kiberdiplomácia kezdeteitől fogva központi kérdés. Kína az internet világára kétélű kardként tekint: elengedhetetlen elem a gazdasági fejlődés és a kormányzás biztosításához, ugyanakkor a belső stabilitásra és a rendszer legitimációjára nézve fenyegetés. Elsősorban az országon belüli cenzúra segítségével szándékozik megadni a válaszokat (lásd Great Firewall), de hangsúlyozza a nemzetközi együttműködés fontosságát is.

A kínai kiberdiplomáciai erőfeszítések között évek óta kiemelt helyen szerepel az internetforrások egyenlőtlen elosztása elleni fellépés, és ezzel összefüggésben az IANA[23] feletti erős amerikai ellenőrzés és az ICANN[24] megreformálásának kívánalma. Ugyanis a világ 13 gyökérszerveréből 10 az Egyesült Államokban található, és az IANA is az ICANN és az amerikai Kereskedelmi Minisztérium között köttetett szerződés eredményeként jött létre.[25] Ezért sem meglepő, hogy az amerikai dominancia letörése érdekében Kína a multilaterális internetkormányzás megvalósítását támogatja.

A kiberkérdések egyre fontosabb helyet kapnak Kína kétoldalú és regionális kapcsolataiban is. Peking a kiberbiztonságot egyrészt a regionális pozíciója erősítésére, másrészt a regionális és fejlődő országok körében vezető pozíciójának biztosítására használja fel. Kiemelt kétoldalú kapcsolatokat ápol az Egyesült Államokkal, azonban a kiberkérdéseket illetően meglehetősen változékonyan alakult a két nagyhatalom kapcsolata. A kétoldalú kapcsolatok erősítését kezdetben az Egyesült Államok forszírozta, a párbeszéd azonban leginkább gazdasági kérdésekre korlátozódott – részben annak köszönhetően, hogy a kínai diplomaták a külügyminisztérium állományából érkeztek, és nem rendelkeztek kiberszakértelemmel. Az Egyesült Államok egyre keményebb hangot ütött

[22] 70/125. sz. ENSZ közgyűlési határozat: Outcome Document of the High-Level Meeting of the Genereal Assembly on the Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society. 2015. december 16.

[23] Internet Assigned Numbers Authority.

[24] International Corporation for Assigned Names and Numbers.

[25] Michael D. Swaine: Chinese View on Cybersecurity in Foreign Relations. *China Leadership Monitor,* (2013), 42. 5.

meg, és 2013 júniusában, amikor a két ország vezetői Kaliforniában találkoztak, Obama arra figyelmeztette a kínai elnököt, hogy a kiberkémkedés súlyosan árt a kétoldalú kapcsolataiknak. Nem sokkal ezután robbant ki a Snowden-ügy, az Egyesült Államok pedig öt kínai hekker ellen emelt vádat – mire Kína válasza a kétoldalú tárgyalások befagyasztása volt. Ebben az időszakban mindkét fél részéről két nagy kutatóintézet készített éves jelentéseket a kiberbiztonság aktuális helyzetéről (az amerikai CSIS és a kínai CICIR).[26] A kapcsolatok konszolidálására csak azt követően került sor, hogy a kínai hekkerek elleni vádakat ejtették. 2015 szeptemberében Hszi elnök hivatalos látogatásra érkezett Washingtonba, ahol a kétnapos tárgyalás eredményeként a két nagyhatalom korszakos jelentőségű bilaterális egyezményt írt alá, amely külön rendelkezik a kiberbiztonság kérdéseiről is. Az egyezmény aláírása azért is volt fontos lépés, mert a kiberkapcsolatok alakításának is mintájaként szolgált az Egyesült Királyság, Németország és más nyugati államok esetében.

A 2015. szeptember 25-én aláírt kétoldalú megállapodás rögzíti,[27] hogy időben választ kell adni információ- vagy segítségkérésre vonatkozó megkeresésekre, ha az rosszindulatú kibertevékenységekkel kapcsolatos. A felek kötelesek együttműködni a kiberbűncselekmények felderítésében és elektronikus bizonyítékok gyűjtésében, valamint naprakész adatokat szolgáltatnak a nyomozás állásáról és eredményéről. Kötelezettséget vállalnak arra is, hogy egyik kormány sem folytat vagy támogat a szellemi tulajdon eltulajdonlására irányuló kibertérbeli tevékenységet. Mindkét fél támogatja az államok kibertérre vonatkozó magatartási szabályainak lefektetését, és ezt a kérdéskört egy később felállítandó szakértői csoport fogja tüzetesebben megvizsgálni. Végezetül a kiberbűnözéssel kapcsolatos kérdések megvitatására egy külön együttműködési mechanizmust is létrehoznak. A „magas szintű közös párbeszéd" elnevezésű csoport évente kétszer ül össze tanácskozási céllal.[28]

Az egyezmény utáni időszakban a két ország egymás ellen folytatott kiberkémkedési tevékenysége alacsonyabb szintre váltott, azonban nem kizárt az újbóli növekedés – s ez az amerikai–kínai kétoldalú kapcsolatok prioritásává

[26] CSIS – Center for Strategic and International Studies; CICIR – China Institute of Contemporary International Relations.

[27] *Fact Sheet: President Xi Jinping's State Visit to the United States.* The White House, Office of the Press Secretary, 2015. szeptember 25.

[28] Thomas Renard: *US-China Cybersecurity Agreement: A Good Case of Cyber Diplomacy.* 2015. október 1.

emelheti a kiberbiztonságot. Ennek valószínűsége azonban csekély, ugyanakkor vannak olyan alapvető kérdések, amelyekben gyökeresen eltér a két nagyhatalom álláspontja. Ilyen a kibertér militarizációjának, a nemzetközi jog kiberhadviselésre való alkalmazhatóságának kérdése, valamint a kiberkémkedés legitim mértékének és céljának megítélése. Márpedig ez a feszültség óhatatlanul magában rejti egy esetleges súlyosabb konfliktus kialakulásának veszélyét is. Egy ilyen konfliktus megelőzésére a kibertérbeli viszonyokra is alkalmazni lehetne a fegyverzetkorlátozás logikáját és célrendszerét – annak ellenére, hogy a fegyverzetkorlátozási mechanizmusok a hidegháború időszakában a nukleáris arzenálra vonatkoztak, és alapvetően különböznek[29] a kibertérbeli viszonyoktól.[30] Ha azonban a Trump-adminisztráció vagy Amerikai jövőbeli vezetésének egyirányú és egyoldalú diplomáciai lépései a jövőben is folytatódnak, további feszültségek várhatók a két ország viszonyában.[31]

A kétoldalú kapcsolatok közt mindenképpen ki kell térni a kínai–orosz kapcsolatokra is. A két ország 2015 májusában 32 kétoldalú megállapodást írt alá – köztük egy együttműködési megállapodást a nemzetközi információs biztonságról.[32] Ebben kötelezettséget vállalnak arra, hogy egymás ellen nem indítanak hekkertámadásokat, és elítélik a belpolitika destabilizálására irányuló, interneten keresztül tett kísérleteket. Ez utóbbi megállapodás újnak tekinthető a Sanghaji Együttműködési Szervezet égisze alatt már megkötött egyezményekhez képest. További előrelépés a konkrét intézkedések nevesítése, mint a kontaktpontok felállítása vagy közös tudományos kiberprojektek futtatása.

A kétoldalú kapcsolatok között említést kell tenni az Európai Unióval 2012-ben kialakított partneri viszonyról is. A minden évben megrendezett EU–Kína-csúcs keretében rendszeresen ülésezik az EU–Kína-kibercsoport is, ez lényegében az unió kínai kiberbiztonsági politikával kapcsolatos aggodalmai

[29] A kiberképességek kettős felhasználásúak és leginkább láthatatlanok, a kibertér legfőbb szereplői a magánszektor entitásai (szemben a nukleáris hatalmakkal mint államokkal), a kibertérbeli kötelezettségvállalások ellenőrzése lényegében lehetetlen, valamint a kiberfegyverek kiválóan alkalmasak lokalizált és múló hatás elérésére.

[30] Ariel (Eli) Levite – Lyu Jinghua: *Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation.* 2019. január 24.

[31] Erről részletesebben lásd David Dollar – Ryan Hass – Jeffrey A. Bader: *Assessing U.S.-China Relations 2 Years into the Trump Presidency.* 2019. január 15.

[32] Andrew Roth: Russia and China Sign Cooperation Pacts. *The New York Times,* 2015. május 8.

kifejezésének és az internetkormányzásról szóló megbeszélések fóruma lett.[33] A munkacsoport 2020. január 13-án tartotta hetedik ülését Kínában, ahol jelentős eredményként értékelték a gyakorlati együttműködés kiterjesztését és a kétoldalú átfogó stratégiai partnerség elmélyítését.[34] Kína az európai államok közül az Egyesült Királysággal is évente tárgyal kiberkérdésekről a kétoldalú partnerség keretében, megvitatva főként a kiberbűnözési kérdéseket.

Kína diplomáciai agendájának centrumában minden bizonnyal továbbra is a kiberszuverenitás kérdése fog állni, és kibertérbeli pozícióját a gazdasági eszközök segítségével fogja javítani. A kínai kiberdiplomáciának már most is az egyik speciális, ugyanakkor igen fejlett területe a kereskedelmi és befektetéspolitika, amelyeket gazdasági és indirekt politikai eszközökként használ. Azáltal, hogy új piacokat nyit szerte a világban, új támogatókat szerez a kínai külpolitikának, egyúttal a kínai kiberpolitikának, valamint a kibernormák elfogadtatásának. A befektetés azonban nem mindig konvertálható közvetlenül politikai befolyássá, az gyakran indirekt formában jelenik meg. A közvetlen befolyásra példa lehet a Huawei afrikai piacra lépése. 2005-ben Nigéria fővárosában a Huawei iskolát nyitott, öt évvel később pedig már ötven afrikai országban működött, ellátva 300 millió afrikai felhasználót. Másik jó példa a One Belt, One Road (OBOR) kezdeményezés. Ez két elemből áll: az egyik a Kínát a Perzsa-öböllel, a mediterrán térséggel és az Indiai-óceán térségével összekötő Selyemút gazdasági öve, míg a másik a 21. századi tengeri Selyemút, amely a régió vízi útjait köti össze. Ehhez kapcsolódóan tervezik egy „információs Selyemút" kiépítését is, amely eredendően határokat átszelő optikai kábelek lefektetését és más kommunikációs hálózatok létrehozását jelentette.[35] A tervezett, Kínát 48 afrikai országgal összekötő optikai kábel 200 000 km hosszú, a kiépítés várható költsége pedig 173 milliárd dollár.[36] A terv azonban 2019 novemberében kiegészült, és már nemcsak a kábelrengeteget kívánják lefektetni, hanem hálózati eszközökkel és szoftverekkel is bővítik, valamint okosportokat is kiépítenek a jövő menedzsmentstruktúráinak támogatására.[37]

[33] Patryk Pawlak: *Cyber Diplomacy: EU Dialogue with Third Countries.* European Parliament Think Tank, 2015. június 29.

[34] *The 7th China-EU Cyber Taskforce was Held in Beijing* (2020. január 13.).

[35] A terv sarokpontjait 2016-ban rögzítették, és megvalósítását 2018-ra tervezték, de a tényleges kiépülés még várat magára.

[36] Chinese Firm Hopes to Wire Continent with Same Strategy that Boosted Internet Access Across China. *Global Times,* 2017. március 13.

[37] *China's Digital Silk Road (DSR): The New Frontier in the Digital Arms Race* (2020. február 19.).

A kínai kiberpolitika és -diplomácia alakulását a következő időszakban két külső tényező fogja meghatározni. Az egyik az Egyesült Államokban zajló folyamatok. Ha az ország elsősorban a belső problémáira fog koncentrálni, az lehetőséget jelent Kína számára, hogy nagyobb szerepet játsszon a kibertérbeli szabályok megalkotásában. A másik a kiberbiztonsági környezet alakulása, amely a jelenlegi tendenciák alapján egyre veszélyesebbé válik, és félő, hogy bekövetkezik a „kibertér militarizációja".[38] A fontolva haladás ősi kínai elvét azonban aligha fogja Kína feladni, és átgondolt politikai-gazdasági lépéseinek legfőbb terepe továbbra is a diplomácia marad a kibertérben is.

Oroszország és a kiberdiplomácia

Az orosz kiberpotenciál az egyik legnagyobb és technológiailag legfejlettebb a világon, az amerikai és a kínai mellett. Az elmúlt években azonban az ország e képességeit többször is támadó szándékkal használta fel – ahogyan az történt Észtország vagy Georgia esetében, de még az Egyesült Államokkal szemben is. Oroszország a kiberkonfliktusokat kényszerítő eszközként használja a Nagy Stratégia részeként az ellenséggel szemben, hogy vágyott céljait elérje. Ezek az akciók azonban a posztszovjet régió határait csak a legritkább esetben lépik át – a kérdés, hogy miért? A válasz abban rejlik, hogy Oroszország nemzeti érdekei és céljai is elsősorban a posztszovjet térségre fókuszálnak, a globális színpad ehhez képest csak másodlagos – s nincs ez másképp a kibertér vonatkozásában sem.

A kiberinterakciókat vizsgálva[39] szembetűnő, hogy Oroszország messze az utolsó helyen áll, míg az Egyesült Államok és Kína toronymagasan vezet. Ebből az következik, hogy a kiberdiplomácia jelentőségét Oroszország alulértékeli, és nem a diplomácia eszközrendszere segítségével kívánja a kibertérbeli konfliktusokat rendezni, hanem sokkal inkább a kiber(támadó) képességei használatával.[40] Ennek okát a „végrehajtói körnél" kell keresni. Míg nyugaton a civil társadalom számos intézménye a *soft power* letéteményese, addig Oroszország

[38] DSR 2020, 2.

[39] Brandon Valeriano – Ryan C. Maness: The Dynamics of Cyber Conflict between Rival Antagonists, 2001–2011. *Journal of Peace Research,* 51. (2014), 3. 347–360.

[40] Ezzel szemben áll az Egyesült Államok, amelynek lehetősége lett volna a fejlett kiberképességei bevetésére az iraki, az afganisztáni vagy akár a líbiai konfliktus során, azt mégsem tette.

esetében az az állami kontroll alatt lévő média által támogatott állami szervek kizárólagos joga. Ezért nem meglepő, hogy az orosz külpolitikai eszközök között a kiberdiplomáciai eszközök nem az első helyen szerepelnek.[41]

Ez azonban nem volt mindig így. A 2000-es évek elején Oroszország még aktívan részt vett a multilaterális és regionális kibertanácskozásokon, azonban mivel az erőfeszítései nem hozták meg a kívánt eredményt, a diplomáciai lépések helyét egyre inkább a támadó jellegű kiberfellépések vették át. Ugyanis Oroszország a kiberhatalmára mint a Nagy Stratégia szerves részére tekint, és azt politikai céljai elérése érdekében kívánja használni – összhangban a clausewitzi gondolattal: a háború a politika folytatása más eszközökkel.[42]

Ami a kezdeti időszakot illeti, Oroszország diplomáciai lépéseinek célja a konfliktusok és az államok közötti kiberfegyverkezési verseny megelőzése volt. Ennek jele volt az 1999-ban orosz kezdeményezésre elfogadott 53/70. sz. ENSZ közgyűlési határozat *Fejlődés az információ és a távközlés területén a nemzetközi biztonsággal összefüggésben*[43] címmel. Igor Ivanov orosz külügyminiszter már ekkor felhívta az államok figyelmét a kibertér militarizációjának veszélyére, hangsúlyozva a kiberfegyverek esetleges ártó hatásait is.[44] Mindez azonban még nem talált teljes megértésre az államok részéről (részben azért, mert akkor még alacsony, 250 000 fő körüli volt az internetet használók száma). Az orosz diplomáciai erőfeszítések azonban folytatódtak, és *A kiberbiztonság globális kultúrájának megteremtése és a kritikus információs infrastruktúrák védelmére tett nemzeti erőfeszítések áttekintése* című, 2009-ben elfogadott ENSZ közgyűlési határozatban nyertek formát.[45] Mivel azonban a határozat nem volt kötelező érvényű, az abban foglaltak gyakorlati megvalósítása elmaradt.

Oroszország továbbra is az ENSZ-rendszer keretein belül kereste a diplomáciai megoldásokat, és üdvözölte az ENSZ Kormányzati Szakértői Csoport

[41] David E. McNabb: Vladimir Putin and Russia's Imperial Revival. *CRC Press,* 2016. 65.

[42] James J. Wirtz: Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. In Kenneth Geers: *Cyber War in Perspective: Russian Aggression Against Ukraine*. Tallinn, NATO CCD COE Publications, 2015. 32.

[43] *UN General Assembly, Resolution A/RES/53/70:* Developments in the Field of Information and Telecommunications in the Context of International Security. 1999. január 4.

[44] Kenneth W. Dam – William Owens: *Technology, Policy, Law and Ethics Regarding U.S. Acquizition and Use of Cyberattack Capabilities*. Committee on Offensive Information Warfare, National Research Council, 2009. 328.

[45] UN General Assembly, A/RES/64/211: Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures. 2009. december 11.

(UN Group of Governmental Experts – GGE) 2004-ben történt megalakítását. Ekkorra azonban már az orosz kiberdiplomácia célja megváltozott, és a megelőzés helyett a szabályozás vált elsődlegessé. Ennek oka, hogy eddigre már számos ország (köztük Oroszország is) aktívan fejlesztette kiberképességeit. Az első eredményekig azonban egészen 2014-ig kellett várni, amikor a Szakértői Csoport jelentésében rögzítette, hogy a nemzetközi jog – s különösen az ENSZ Alapokmánya – alkalmazandó a kibertérben is.[46] A kormányzati munka ezt követően folytatódott, és a csoport 2015. évi jelentése már egy kormányzati kibermagatartási kódex megalkotásának alapjait is letette, azonban a folyamatok ezt követően elakadtak.

Ezzel párhuzamosan Oroszország a regionális kapcsolatain keresztül is forszírozta a kódex megalkotásának szükségességét. 2011-ben a Sanghaji Együttműködési Szervezet nevében három országgal együtt nyújtott be erre vonatkozó javaslatot az ENSZ-nek, majd szintén 2011-ben megalkotta a Nemzetközi Információbiztonsági Konvenció tervezetét.[47] Mindkét dokumentum hangsúlyozza az állami szuverenitás és területi integritás elvét a kibertér vonatkozásában. Az orosz akaratot ezenkívül sikerült érvényesíteni a Kollektív Biztonsági Szerződés Szervezetében és a BRICS államok között is, elfogadva határozatokat és felállítva munkacsoportokat.

Végezetül az orosz diplomácia a kétoldalú partneri kapcsolatok segítségével is igyekezett a kibertér szabályozását elérni. A világ első kétoldalú kiberegyezménye Oroszország és az Egyesült Államok között köttetett meg 2013-ban. A siker azonban nem egyértelmű, mert az egyezmény csak az együttműködés technikai kérdéseire szorítkozott. Rögzítette a nemzeti CERT-ek közötti információcsere és egy kiberforródrót létrehozásának szükségességét. Az oroszokban élt a remény, hogy sor kerülhet egy szélesebb körű orosz–amerikai egyezmény aláírására is, de az ukrán konfliktus miatt a tárgyalási folyamat megakadt, majd 2017-ben, amikor Oroszország ismételten próbálkozott egy, a veszélyes katonai tevékenységekről szóló egyezmény megalkotásával, attól az amerikai fél az aláírás előtti napon elállt – vélhetően a 2016-os elnökválasztásba történt

[46] UN General Assembly, A/68/98: Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 2013. június 24.

[47] A dokumentumok megalkotásában szerepet játszhatott az, hogy az internet ereje minden állam számára nyilvánvalóvá vált az arab tavasz eseményei tükrében, és Oroszország szerette volna elkerülni az orosz politikai rendszer kívülről történő manipulálását.

orosz beavatkozásról kiderült fejlemények miatt.[48] Az első kiberegyezményen túl Oroszország már több országgal is kötött hasonló megállapodást, így például Kínával, Indiával, Dél-Afrikával, Fehéroroszországgal vagy Kubával, és további egyezmények megkötését tervezi Franciaországgal, Németországgal, Izraellel, Japánnal és Dél-Koreával.

Oroszország már húsz évvel ezelőtt rögzítette kiberstratégiájában a kibertér nemzetközi szabályozásának szükségességét, és – Kínával, valamint a CSTO többi tagállamával együtt – a mai napig kitart a kibertérre vonatkozó magatartási szabályok, valamint a szuverenitás és a belügyekbe való be nem avatkozás kibertérben alkalmazandósága mellett. Ellentétben a Nyugattal – élén az Egyesült Államokkal –, amely korábban mindezt ellenezte, az utóbbi időben azonban egyre nagyobb hajlandóságot mutat a szabályok szükségességének elismerésére. A két tábor közötti szakadék igen negatívan hat az orosz–amerikai, illetve az orosz–európai kapcsolatokra is, amely következményeként egyre kisebb az esély a globális egyetértésre – még ha maga az ENSZ főtitkára a szabályrendszer megalkotásának szükségessége mellett foglal is állást.[49]

Összegzés

Az egyes államok kiberbiztonsági helyzetének összehasonlítására több mutató is létezik. Ezek közül az ENSZ Nemzetközi Távközlési Egyesülete által jegyzett, az államokat öt mutató mentén összehasonlító Globális Kiberbiztonsági Indexet emelem ki. Az ötödik mutató az együttműködés, ennél többek között a két- és többoldalú együttműködési keretek, valamint a nemzetközi szervezetekben betöltött tagság számít. Az index összesített értékelése alapján az Egyesült Államok a 2., Oroszország a 26., Kína pedig a 27. helyen szerepel a világranglistán.[50] Látható, hogy a három vizsgált ország közül egyértelműen kitűnik az Egyesült Államok, amely valóban kiberdiplomáciai nagyhatalomnak számít. Kína esetében a mutató által tükrözött relatív lemaradás annak köszönhető, hogy az ország csak az utóbbi években kezdett aktív kiberdiplomáciába, és a kezdeti

[48] Nicu Popescu – Stanislav Secrieru (szerk.): Hacks, Leaks and Disruptions. Russian Cyber Strategy. *Chaillot Papers,* 148. (2018). European Union Institute for Security Studies.

[49] US Chief Calls for Regulatory Scheme for Cyberwarfare. *Radio Free Europe/Radio Liberty*, 2018. február 19.

[50] *Global Cybersecurity Index 2018*. Geneva, UN ITU, 2019.

lépések hatásai még nem köszönnek vissza az index számaiban. Oroszország esetében nem meglepő az eredmény, mivel az oroszok a szerteágazó kapcsolatrendszerüket nem feltétlenül a kiberbiztonság területén kívánják használni. Ugyanakkor valamennyi ország esetén elmondható, hogy az együttműködési mutató alacsonynak mondható, ezért várható, hogy a kiberdiplomácia területe a jövőben jelentős fejlődést fog mutatni.

Felhasznált irodalom

53/70. sz. ENSZ közgyűlési határozat: Developments in the Field of Information and Telecommunications in the Context of International Security. *1999.* január 4. Online: https://undocs.org/A/RES/53/70

64/211. sz. ENSZ közgyűlési határozat: Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures. 2009. december 11. Online: www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211

68/98. sz. ENSZ közgyűlési határozat: Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 2013. június 24. Online: www.un.org/ga/search/view_doc.asp?symbol=A/68/98

70/125. sz. ENSZ közgyűlési határozat: Outcome Document of the High-Level Meeting of the Genereal Assembly on the Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society. 2015. december 16. Online: https://publicadministration.un.org/wsis10/

Bandurski, David: *China's Cyber-Diplomacy.* 2015. december 21. Online: http://chinamediaproject.org/2015/12/21/chinas-cyber-diplomacy/

Bley, Bonnie: *The New Geography of Global Diplomacy. China Advances as the United States Retreats.* 2019. november 27. Online: www.foreignaffairs.com/articles/china/2019-11-27/new-geography-global-diplomacy

Brandon, Valeriano – Ryan C. Maness: The Dynamics of Cyber Conflict between Rival Antagonists, 2001–2011. *Journal of Peace Research,* 51. (2014), 3. 347–360. Online: www.researchgate.net/publication/256046745_The_Dynamics_of_Cyber_Conflict_between_Rival_Antagonists_2001-2011

Chapman, Justin: *Threats and Opportunities of Cyber Diplomacy at PolicyWest.* 2019. december 24. Online: www.pacificcouncil.org/newsroom/threats-and-opportunities-cyber-diplomacy-policywest

China's Digital Silk Road (DSR): The New Frontier in the Digital Arms Race. 2020. február 19. Online: www.silkroadbriefing.com/news/2020/02/19/chinas-digital-silk-road-dsr-new-frontier-digital-arms-race/

Chinese Firm Hopes to Wire Continent with Same Strategy that Boosted Internet Access Across China. *Global Times*, 2017. március 13. Online: www.globaltimes.cn/content/1037500.shtml

Cyber Security: Confidence and Security-Building Measures (CSBMs). Federal Foreign Office website. Online: www.auswaertiges-amt.de/EN/Aussenpolitik/Friedenspolitik/Abruestung_/KonvRueKontrolle/VN-Konventionelle-Abruestung-Ruestungskontrolle_node.html.

Dam, Kenneth W. – William Owens: *Technology, Policy, Law and Ethics Regarding U.S. Acquizition and Use of Cyberattack Capabilities*. Committee on Offensive Information Warfare, National Research Council, 2009. Online: https://lawfare.s3-us-west-2.amazonaws.com/staging/s3fs-public/uploads/2013/01/NRC-Report.pdf

Dollar, David – Ryan Hass – Jeffrey A. Bader: *Assessing U.S.-China Relations 2 Years into the Trump Presidency.* 2019. január 15. Online: www.brookings.edu/blog/order-from-chaos/2019/01/15/assessing-u-s-china-relations-2-years-into-the-trump-presidency/

Eilstrup-Sangiovanni, Mette: Why the World Needs an International Cyberwar Convention. *Philosophy&Technology* 31. (2018), 3. 379–407.

Fact Sheet: President Xi Jinping's State Visit to the United States. The White House, Office of the Press Secretary, 2015. szeptember 25. Online: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

Fedosov, Sergey: *Statement by the Russian Participant at the UNIDIR Cyber Security Conference 'What Does a Stable Cyber Environment Look Like? Geneva,* UNIDIR, 2012. november 8–9. Online: www.unidir.ch/files/conferences/pdfs/pdf-conf1922.pdf

Global Cybersecurity Index 2018. Geneva, UN ITU, 2019. Online: www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. United States, 2011. május. Online: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

International Strategy of Cooperation on Cyberspace. A Kínai Népköztársaság Külügyminisztériuma, 2017. március 1. Online: www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml

Levite, Ariel (Eli) – Lyu Jinghua: *Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation.* 2019. január 24. Online: https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213

McNabb, David E.: *Vladimir Putin and Russia's Imperial Revival.* London, CRC Press, 2016.

Nabeel, Farad: International Cyber Regime: A Comparative Analysis of the US-China-Russia Approaches. *Strategem,* 1. (2018), 2. 8–27. Online: www.academia.edu/38296708/International_Cyber_Regime_A_Comparative_Analysis_of_the_US-China-Russia_Approaches

Nyáry Gábor: A digitális állam a külpolitikai térben. A Twittertől az adattudományig. *Új Magyar Közigazgatás,* 12. (2019), 2. 75–82. Online: www.kozszov.org.hu/dokumentumok/UMK_2019/2/08_Ekozig_Digitalis_allam.pdf

Painter, Christopher: The Rise of the Internet and Cyber Technologies Constitutes One of the Central Foriegn Policy Issues of the 21st Century. *The Foreign Service Journal,* 2018. június. Online: www.afsa.org/diplomacy-cyberspace

Pawlak, Patryk: Cyber Diplomacy: EU Dialogue with Third Countries. *European Parliament Think Tank,* 2015. június 29. Online: www.europarl.europa.eu/RegData/etudes/BRIE/2015/564374/EPRS_BRI(2015)564374_EN.pdf

Popescu, Nicu – Stanislav Secrieru (szerk.): Hacks, Leaks and Disruptions. Russian Cyber Strategy. *Chaillot Papers,* 148. (2018). European Union Institute for Security Studies. Online: www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 2017. május 11. Online: www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

Renard, Thomas: *US–China Cybersecurity Agreement: A Good Case of Cyber Diplomacy.* 2015. október 1. Online: www.egmontinstitute.be/us-china-cybersecurity-agreement-a-good-case-of-cyber-diplomacy/

Roth, Andrew: Russia and China Sign Cooperation Pacts. *The New York Times,* 2015. május 8. Online: www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=0

Segal, Adam (2017): Chinese Cyber Diplomacy in a New Era of Uncertainty. A Hoover Institute Essay. *Aegis Paper Series,* No. 1703. Online: www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf

Segal, Adam: *Year in Review: Chinese Cyber Sovereignity in Action.* 2018. január 8. Online: www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action

Swaine, Michael D.: Chinese View on Cybersecurity in Foreign Relations. *China Leadership Monitor,* 42. (2013). Online: https://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf

The 7th China-EU Cyber Taskforce was Held in Beijing. 2020. január 13. Online: www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/jkxw_665234/t1731937.shtml

The White House: *Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building* (17 June 2013) Online: www.whitehouse.gov/the-pressoffice/2013/06/17/joint-statement-on-a-new-field-of-cooperation-in-confidence-building

UK and 50 Nations Sign Cyber Security Pact (2018. november 13.). Online: www.itpro-portal.com/news/uk-and-50-nations-sign-cyber-security-pact/

US Chief Calls for Regulatory Scheme for Cyberwarfare. *Radio Free Europe/Radio Liberty*. 2018. február 19. Online: www.rferl.org/a/un-guterres-calls-for-cyberwarfare-rules/29049069.html

Wirtz, James J.: Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. In Kenneth Geers: *Cyber War in Perspective: Russian Aggression Against Ukraine*. Tallinn, NATO CCD COE Publications. Online: https://ccdcoe.org/uploads/2018/10/Ch03_CyberWarinPerspective_Wirtz.pdf

Xi Jinping Gives Speech at Cybersecurity and Informatization World Conference (2016. április 19.). Online: https://chinacopyrightandmedia.wordpress.com/2016/04/19/xi-jinping-gives-speech-at-cybersecurity-and-informatization-work-conference/

Ziolkowski, Katharina (szerk.): *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy.* Tallinn, NATO CCDCOE Publication, 2013.

Molnár Dóra

Európai kiberdiplomáciai helyzetkép – Franciaország, az Egyesült Királyság és Németország

Az előző fejezet folytatásaként e fejezet a három vezető európai állam, Franciaország, az Egyesült Királyság és Németország kiberdiplomáciájának alapvető elméleti és gyakorlati kérdéseit mutatja be.

Franciaország mint kiberdiplomáciai nagyhatalom

Talán nem túlzás azt állítani, hogy Franciaország évszázadok óta a diplomácia fellegvára, és a franciák a *soft* eszközök alkalmazásának nagymesterei a politikában. Az ország erejét globális szerepvállalása adja, amelyhez a kiterjedt diplomáciai hálózata szolgál alapul: páratlanul széles körű tagsággal rendelkezik multilaterális és nemzetközi szervezetekben, külföldi kulturális misszióinak száma a legmagasabb, és az 5. legnagyobb segélyező állam.[1] Ezért nem meglepő, hogy a francia politika előszeretettel és hatékonyan használja a diplomácia eszköztárát a kibertérben is – olyannyira, hogy európai szinten első e téren. Ez indokolja, hogy az európai országok vizsgálatát Franciaországgal kezdem, még ha kiberhatalmi potenciál terén van más európai állam, amely megelőzi az országot.

Már az első, 2011-ben kiadott, *Az információs rendszerek védelme és biztonsága: Franciaország stratégiája* című kiberstratégiában megjelenik a kibertérbeli nemzetközi együttműködés szükségessége mint a szükséges cselekvési területek egyike.[2] Ezt a 2012-ben elfogadott 681. számú szenátusi információs jelentés konkretizálja azzal, hogy a tíz prioritás egyikeként hangsúlyozza a bilaterális kapcsolatok fontosságát, közös akciókat sürget az Észak-atlanti Együttműködés

[1] *La diplomatie française à l'ère numérique*. Consulat Général de France á Ekaterinbourg. 2019. május 29.

[2] *Défense et sécurité des systèmes d'information: Stratégie de la France*. 2011.

https://doi.org/10.36250/01008_05

Szervezetével (a továbbiakban: NATO) és az Európai Unióval (a továbbiakban: EU), párbeszédet Kínával és Oroszországgal, valamint támogatja a nemzetközi bizalomépítő intézkedések elfogadását.[3] A 2013-ban kiadott Fehér Könyv kiemeli, hogy a kibertámadások kivédése érdekében „globális kormányzati megközelítést" kell alkalmazni, és ennek részeként Franciaország diplomáciai, jogi és politikai eszközeire épít.[4]

Az ország kiberstratégiáját 2015-ben adták ki, *A digitális biztonság nemzeti stratégiája* címmel.[5] A stratégia öt fő célkitűzést rögzít, amelyek közül az ötödik az *Európa, digitális stratégiai autonómia, a kibertér stabilitása* címet viseli. Franciaország Európa digitális transzformációjában szövetségesi kapcsolatain keresztül kíván részt venni, három főbb módon: az európai stratégia megalkotására vonatkozó menetrend megfogalmazásával közösen más uniós, önkéntesen részt vevő államok, a nemzetközi kibermegbeszéléseken való francia jelenlét és befolyás erősítésével, valamint a kiberkapacitások építésében más államok támogatásával, hozzájárulva ezzel a kibertér globális stabilitásához. A stratégia értelmében a befolyásnövelés fő színterei a nemzetközi szervezetek közül az Egyesült Nemzetek Szervezete (a továbbiakban: ENSZ) és az Európai Biztonsági és Együttműködési Szervezet (a továbbiakban: EBESZ), a bilaterális kapcsolatok miniszteri szintű diplomáciai párbeszéd keretében, valamint a politikai döntéshozók és a tudományos élet szereplői részvételével megrendezett informális nemzetközi fórumokon való aktív jelenlét. A stratégiában foglaltak végrehajtására centralizálták a kiberdiplomácia területét, és 2015-ben a Külügyminisztériumban felállították a kiberdiplomácia és digitális gazdaság nagyköveti pozícióját.[6]

A 2015-ös stratégia elfogadása óta a nemzetközi környezet jelentősen megváltozott. Elég, ha a Charlie Hebdo elleni terrortámadást követő vagy a TV5 televíziócsatorna elleni kibertámadás-sorozatokra gondolunk. Az események új megvilágításba helyezték a kiberbiztonság kérdéskörét Franciaországban is, és az országot aktívabb és erőteljesebb nemzeti és nemzetközi fellépésre sarkallták.

[3] *Rapport d'Information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense*. Par le Sénateur M. Jean-Marie Bockel. Sénat Session extraordinaire de 2011–2012. Enregistré á la Présidence du Sénat le 18 juillet 2012.

[4] *Livre Blanc. Défense et sécurité nationale.* Paris, 2013.

[5] *La stratégie nationale pour la sécurité de la numérique* (2015).

[6] A tisztséget, amelyet 2017. november 22-e óta digitális nagykövetnek neveznek, David Martinon töltötte be.

Az új megközelítést tükrözi a *Támadó kiberműveletek doktrínája,* amelyet 2018. január 18-án publikáltak, mintegy három héttel megelőzve a *Kibervédelmi stratégiai áttekintés* kiadását. A dokumentumban Franciaország nyíltan ír arról, hogy katonai tevékenységének részét képezik a kiberkapacitások, amelyeket szükség esetén kész bevetni. Ez mindenképpen fordulópontot jelez a francia kiberpolitikában, amelyet ez idáig a diszkrét diplomáciai lépések megtétele jellemzett: még olyan nyilvánvaló kiberkonfliktusok esetén, mint az oroszok által szponzorált, a haditengerészet olajutánpótlási csatornáinak kiderítését célzó kibertámadás kapcsán sem lépett fel Franciaország támadó retorikával, hanem a párbeszéd eszközéhez nyúlva igyekezett a feszültséget csillapítani.[7]

2018. február 8-án *Kibervédelmi stratégiai áttekintés* címmel adták ki a legújabb kiberdokumentumot, az ország kibervédelmi ambícióit összefoglaló hivatalos anyagot.[8] A kibervédelem fehér könyvének is nevezett dokumentum több fejezetben is kitér az egyes kiberdiplomáciai lépések szükségességére, és rögzíti Franciaország adott kérdéssel kapcsolatos álláspontját. Önálló fejezet szól a kibertér szabályozásáról szóló nemzetközi tárgyalásokról, kiemelve az ENSZ és a Kormányzati Szakértők Csoport (Group of Governmental Experts, a továbbiakban: GGE) szerepét és elért eredményeit 2013-tól kezdődően. Franciaország a 2016–2017-es ülésszakon önálló javaslattal állt elő a visszatámadás tilalmának mélyebb szabályozását illetően, és ezt a javaslatot bár támogatták a részt vevő államok, de a tárgyalások megakadtak a nemzetközi jog alkalmazásának módjával kapcsolatos eltérő nézetek miatt. Egy másik fejezet azt mutatja be, hogy az ország hogyan lép fel nemzetközi szinten a kibertérben. A kiberkonfliktusok megelőzése érdekében támogatja a párbeszédet és az együttműködést a szövetségeseivel, a kibertér szabályozását sürgeti, és célja, hogy az európai biztonság és autonómia a kibertérben is biztosítva legyen. A bilaterális kapcsolatai közül kiemeli az Egyesült Államokkal,[9] Kínával, Indiával,[10] Brazíliával és Japánnal

[7] Arthur P. B. Laudrain: *France's New Offensive Cyber Doctrine*. 2019. február 26.

[8] *La Revue Stratégique de Cyberdéfense*. SGDSN, 2018. február 12.

[9] A francia–amerikai kiberdialógus harmadik állomását 2020. január 22-én, Párizsban rendezték meg. A találkozó központi témája a nemzetközi jog kibertérre történő alkalmazhatósága volt. Lásd *Troisième dialogue stratégique France-États-Unis en matière de cybersécurité (Paris, 22 janvier 2020).*

[10] Az indiai–francia bilaterális kiberdialógust 2019. június 20-án harmadik alkalommal rendezték meg, megvitatva elsősorban a kibernormákkal kapcsolatos kérdéseket. Jól jelzi a kétoldalú kiberkapcsolatok fontosságát, hogy India meghívást kapott a 2019-es G7-csúcsra az elnöki tisztet 2019-ben betöltő Franciaországtól. Lásd *Indo-French Bilateral Cyber Dialogue (Paris, 20 June 2019).*

fennálló kiberkapcsolatait, hozzátéve, hogy a nyugati szövetségeseivel továbbra is mély kapcsolatokat fog ápolni, de egyre nagyobb hangsúlyt helyez a szubszaharai térségre, ahol kapcsolatok kiépítését sürgeti a frankofón államokkal. Az európai kiberkapcsolatokat három kérdéskör mentén kell rendezni: a technikai, a szabályozási és a kapacitási kérdésekben szükséges a közös alapok megfogalmazása és azok elfogadása. Mind a bilaterális, mind az európai kapcsolatok szempontjából kiemelt helyet foglal el a francia–német kapcsolatrendszer. A két ország közötti együttműködés igen intenzív és kiterjedt, ezt az eddig kiadott két közös jelentés is alátámasztja.[11] Végezetül pedig a dokumentumban foglaltak értelmében szükséges egy cselekvési doktrína elfogadása, amely olyan alapvető kérdéseket rögzít, mint a kibertámadások osztályozásának rendszere és a kiberincidensekre adandó válaszlehetőségek köre. A kibertér szabályozásának globális rendszerét csak olyan alapelvek mentén lehet megvalósítani, mint a megelőzés, az együttműködés és a stabilitás.

A „támadóbb" szellemű hozzáállás ellenére a francia politikában minden bizonnyal a jövőben is meghatározó szerepet fognak játszani a diplomáciai lépések. Nem véletlen, hogy a különböző nemzetközi szervezetekben Franciaország az egyik legaktívabb tagállam, amikor kiberbiztonsággal kapcsolatos kérdések merülnek fel. Nemcsak az ENSZ-ben – ahogyan a GGE kapcsán arról már szó esett –, hanem a NATO-ban, a G7-ben és az EBESZ-ben is.[12] Ez utóbbi szervezetnél Franciaország igen jelentős szerepet játszott a kiberbiztonsággal kapcsolatos bizalomerősítő intézkedés két csomagjának elfogadásában. A G7-ben való francia részvétellel kapcsolatban kiemelem a 2019. április 5–6-án Dinard francia kisvárosban megrendezett találkozót, ahol elfogadták az úgynevezett Dinard-deklarációt a kiberszabályok kezdeményezéséről.[13] Ebben üdvözölték az ENSZ közgyűlésének támogató hozzáállását a nemzetközi jog kibertérben alkalmazhatóságáról, és megerősítették szándékukat egy nyitott, biztonságos, stabil, hozzáférhető és békés kibertér támogatása iránt. Egyúttal megerősítették szándékukat a kiberszabályozási kezdeményezés (Cyber Norm Initiative – CNI) megfogalmazására, amelyet 2019. augusztus 26-án öntöttek formába tíz, a kiber-

[11] *ANSSI/BSI Common situational picture*. 1. – 2018. július. *Second Edition of the Franco-German Common Situational Picture*. 2019. május 21.

[12] *La France et la cybersécurité*.

[13] *Dinard Declaration on the Cyber Norm Initiative*. 2019. április 6.

térben alkalmazandó alapvető szabály megalkotásával.[14] Mindez jól illeszkedik a francia soft politika sikertörténetébe, bár hozzá kell tenni, hogy nem volt előzmények nélküli egy ilyen kezdeményezés elfogadása. 2018. november 12. és 14. között ugyanis az UNESCO párizsi székháza adott otthont az Internetkormányzási Fórum (Internet Governance Forum) tizenharmadik éves ülésének, ahol Emmanuel Macron francia elnök maga jelentette be a *Párizsi felhívás*t a bizalom és biztonság kibertérben való megteremtésére.[15] A felhívásban foglaltak széles körű elfogadását jól jelzi, hogy azt azonnal több mint 500 entitás (állam, szervezet és vállalat) támogatta.[16] A kép teljességéhez azonban az is hozzátartozik, hogy a három „nagy" kiberállam mindegyike visszautasította a kezdeményezést, megtorpedózva ezzel annak globális elfogadhatóságát. A felhívással és számos hasonló kezdeményezéssel Franciaország célja, hogy kibernagyhatalomként tartsák számon világszerte. Talán ez a cél vezérelte az országot 2019. szeptember 9-én is, amikor a francia Védelmi Minisztérium hivatalos dokumentumban rögzítette véleményét arról, hogy a nemzetközi jog Franciaország szerint miként alkalmazható a kibertérben[17] – ezzel is úttörő kiberdiplomáciai szerepet vállalva.

Németország

Bár Németország 2004-től aktívan részt vett az ENSZ kiberbiztonsági tanácskozásain és más két- és többoldalú fórumokon, az együttműködés technikai kérdésekre korlátozódott. Az első, 2011. évi német kiberbiztonsági stratégia megemlítette ugyan a kiberbiztonság nemzetközi és diplomáciai dimenzióit, egészen a Snowden-ügyig azonban Németország nem játszott különösebb szerepet a kiberporondon. Csak ezt követően kezdeményezte Angela Merkel német kancellár érintettsége okán Németország – Brazíliával karöltve – az ENSZ-ben a magánélethez való jog védelméről és sérthetetlenségéről szóló határozat elfogadását a digitális kor vonatkozásában, amelynek eredményeképp 2013. december 18-án megszületett a 68/167. sz. közgyűlési határozat. Ez Németország jelentős

[14] *Inititative pour des normes dans le cyberespace. Synthese des enseignements tirés et des bonnes pratiques*. 2019. augusztus 26.

[15] *Appel de Paris pour la confiance et la sécurité dans le cyberespace*. 2018. november 12.

[16] *Cybersécurité: Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans la cyberespace*. Liste des soutiens à l'appel de Paris (actualisé le 14 novembre 2018.).

[17] Przemyslaw Rogusky: *France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I*. 2019. szeptember 24.

kiberdiplomáciai sikere volt, különösen úgy, hogy a dél-amerikai támogatással globális szintre sikerült emelnie e kérdéskört. Innentől kezdve Németország a kiberdiplomácia aktív támogatójává vált. 2016-ban az EBESZ német elnöksége alatt fogadták el a kibertérbeli bizalomerősítő intézkedések második csomagját, majd 2016–2017-ben Németország diplomáciai képviselői elnököltek a UN GGE-n is.

Az egyre aktívabb német fellépés alapjai az ország kiberbiztonsági stratégiájában keresendők, 2016-ban adták ki az ország második kiberstratégiáját.[18] A dokumentum már kiemelten kezeli az együttműködés fontosságát, amely azonban nem korlátozódhat nemzeti keretek közé, hanem összeurópai, sőt világszintű együttműködési csatornákat kell kialakítani. A stratégia négy cselekvési területet nevesít, amelyek közül az egyik Németország megfelelő pozicionálása az európai és a nemzetközi kiberbiztonsági politikai megbeszéléseken. Ez egyértelműen mutatja, hogy a kiberdiplomácia kiemelt területté nőtte ki magát, és az ország biztonságát befolyásoló alapvető tényezővé vált. Ennek részeként Németország hangsúlyozza a kétoldalú partneri kapcsolatok fontosságát is, főként olyan területeken, mint az információmegosztás és a határon átnyúló szolgáltatásokkal kapcsolatos biztonsági kérdések összehangolása, valamint a kapacitások megosztása, másrészt a fejlesztési együttműködés terén, ahol elsősorban a biztonság- és bizalomerősítő intézkedések segítségével érhetők el sikerek.

Németország a stratégiában foglaltakat a gyakorlatba is fokozatosan átülteti, ahol fokozott szerepet szán a kétoldalú kapcsolatoknak. Kiemelt stratégiai partnere az Egyesült Államok, ezért nem véletlen, hogy a kiberpárbeszédük is hosszú és tartalmas múltra tekint vissza. 2012 óta évente megrendezik a kétoldalú kibertalálkozót, hol Washingtonban, hol Berlinben. A találkozások alkalmával olyan kérdéseket vitatnak meg, mint 2016-ban például a nemzetközi jog kibertérben való alkalmazhatóságának kérdése vagy az emberi jogok online érvényesülése, de jól kirajzolódik közös gondolkodásmódjuk a kibertér többszereplős *(multi-stakeholder)* kormányzati modelljében is.[19]

Kínával 2016 novemberében születetett megegyezés arról, hogy a két állam a kiberkérdések vonatkozásában egy speciális mechanizmus segítségével folytatja a párbeszédet, de kétoldalú szerződés aláírására a mai napig nem került sor.[20] Legutóbb 2020 januárjában folytatott Merkel kancellár tárgyalásokat Kiná-

[18] *Cyber Security Strategy for Germany 2016.* Federal Ministry of the Interior, 2016.
[19] *Joint Statement on U.S.-Germany Cyber Bilateral Meeting*. 2016. március 24.
[20] Christopher Burgess: Dissectiong China's Global Bilateral Cybersecurity Strategy. 2016. október 9.

ban egy, az amerikai–kínai egyezményhez hasonló német–kínai kiberegyezmény megalkotásáról, annak előfeltétele azonban a *no spy* klauzula beiktatása az amerikai Huawei-botránynak köszönhetően. Amikor azonban a kancellárt az egyezményről kérdezték, ő diplomatikusan mindössze annyit mondott, hogy Németország és Kína több szinten is folyamatosan tárgyal egymással számos kétoldalú és nemzetközi kérdésről.[21]

A német bilaterális paletta ugyanakkor nem szűkül le a nagy partnerállamokra, hanem rendkívül színes képet mutat. Németország például jó kétoldalú kiberkapcsolatokat ápol Szingapúrral. A szingapúri miniszterelnök 2017-ben látogatást tett Németországban, amely alkalommal a két fél közös szándéknyilatkozatot írt alá a kiberbiztonsági együttműködésről olyan területeken, mint az információmegosztás vagy a közös kutatások. A látogatást 2018 júniusában Merkel kancellár viszonozta, s ennek keretében a két ország vezetője védelmi szerződést is kötött, külön kiberklauzulával.[22]

Németország számos nemzetközi intézményben aktívan lép fel a kiberbiztonsági kérdések tárgyalásakor, de talán mindezen fellépések közül kiemelkedik az EBESZ-ben játszott szerepe. Predesztinálva is volt arra, hogy élére álljon az EBESZ-beli kezdeményezéseknek. Egyrészt azért, mert történelmileg politikai és gazdasági szálak kötik mind a Kelethez, mind a Nyugathoz, az EBESZ pedig összeköti e térségek vezető hatalmait is. Másrészt azért, mert Németország vezető állam e területen – elég, ha az adatvédelem területén felállított technikai sztenderdekre és szabályozásra gondolunk. Harmadrészt pedig azért, mert Németország hatékonyan vesz részt olyan, a kibertérbeli normák és szabályok megalkotásával foglalkozó szervezetekben, mint a GGE, ráadásul az itt szerzett tapasztalatait kamatoztatni is tudja.[23]

Az EBESZ 2013-ban megalkotta a kibertérbeli bizalomerősítő intézkedések első csomagját, amely megfelelő alapul szolgált a továbblépéshez. A 2016-os német EBESZ-elnökség alatt mindhárom kosárban külön tárgyalták a bizalom- és biztonságerősítő intézkedések lehetséges körét. Az első kosár vonatkozásában 2013-ban még csak önkéntes megállapodások sorát rögzítették a tagállamok

[21] Guy Chazan: German Cyber Security Chief Backs 5G 'No Spy' Deal over Huawei. *Financial Times,* 2020. február 28.

[22] Prashanth Parameswaran: *Singapore-Germany Cyber Cooperation in Focus with Introductory Visit*. 2018. augusztus 14.

[23] *Three Priorities for Cyber Diplomacy under the German OSCE Chairmanship 2016*. Berlin, German Institute for International and Security Affairs. 2015. november 11.

közötti katonai együttműködésről. Megegyezés született, hogy az EBESZ-t platformként használják a kibertámadásokról szóló információcserére és a nemzeti kapacitások kiterjesztésének kölcsönös támogatására. A német elnökség kifejezett célja volt, hogy a mérnököket (elsősorban az informatikusokat) is bevonják a kiberdiplomáciába (nem csak az első kosarat érintően), amelytől olyan, a diplomáciai feszültségeket csökkentő hatást várnak, mint az 1950-es évek óta megrendezett Pugwash-konferenciák[24] fejleményei. A második, gazdasági kosárba tartozó lépésekhez referenciapontként szolgált a 2015-ben elfogadott német információbiztonsági törvény, amely a kritikus infrastruktúra védelmével kapcsolatban magasabb biztonsági követelményeket írt elő. A német törvényben foglaltak hivatkozási alapul szolgáltak a NIS-irányelv megalkotásakor is. A központi német kiberszerv, a Szövetségi Információbiztonsági Hivatal (BSI)[25] pedig számos EBESZ-partner számára a műszaki szakértelem modelljeként szolgált. Mindezek a fejlemények új horizontot nyitnak az EBESZ gazdasági együttműködés kontextusában. A harmadik kosár esetében az emberi jogok, azon belül is az interneten megvalósuló szólásszabadság kérdése a problematikus. A német elnökségnek mindenekelőtt a cenzúrával, a hálózati megfigyeléssel és a szerzői jogi kérdésekkel kapcsolatos dilemmára kellett választ találnia.

Németország kiemelt külpolitikai prioritásként kezeli a kibertér szabályozásának kérdéseit. Határozottan kiáll amellett, hogy a globális kérdéseket csak közös szabályozás mentén lehet megoldani – s e körbe tartozik a kiberbiztonság kérdése is. A probléma nem kezelhető csak nemzeti szinten, szükséges az államok, nemzetközi szervezetek, civil szervezetek és a tudományos szféra közti szoros együttműködés. Deklarálja a nemzetközi jog kibertérben való alkalmazhatóságát és alkalmazandóságát, valamint támogatja a multilaterális megközelítést.[26] Mindenképp diplomáciai sikernek tekintendő, hogy 2019 novemberében Németország adhatott otthont az ENSZ Internetkormányzás Fórumának.

[24] A béke és a leszerelés kérdéseivel foglalkozó, évente megrendezett konferenciák, amelyeken a nemzetközi tudományos élet jeles képviselői vesznek részt 1957 óta.

[25] Bundesamt für Sicherheit in der Informationstechnik – Federal Office for Information Security (BSI).

[26] *Cyber Policy: Multilateral Solutions for the Future*. Federal Foreign Office, 2019. szeptember 25.

A vezető (európai) kiberhatalom: az Egyesült Királyság

Az Egyesült Királyság – hasonlóan a nagyhatalmakhoz – idejekorán felismerte a kiberbiztonság és a kiberdiplomácia fontosságát, amelyet a stratégiai dokumentumaiban is megjelenít, és a gyakorlatban is sikeresen alkalmaz. Az első kiberbiztonsági stratégiát még 2009-ben adták ki, azt azonban hamar, 2011-ben felváltotta egy új stratégia, amely ötéves távlatban vázolta fel a fő irányvonalakat, célkitűzéseket és a megvalósításhoz szükséges feltételrendszert. A stratégia címe: *Megvédeni és segíteni az Egyesült Királyságot egy digitális világban (Protecting and Promoting the UK in a Digital World).*[27] A dokumentum négy célkitűzést fogalmaz meg, amelyek közül a második célkitűzés kapcsán van szerepe a kiberdiplomáciának. Az ország megfogalmazott célja, hogy rugalmasan tudjon reagálni a kibertérbeli fenyegetésekre és támadásokra, valamint hatékonyabban tudja érdekeit megvédeni és érvényesíteni a kibertérben. Ez proaktív magatartást és aktív részvételt feltételez a kibertér alakításának folyamatában, amelynek elsődleges eszközei mind békés eszközök: részben diplomáciai, részben pedig gazdasági jellegűek, ugyanis a brit kormány igen nagy súllyal csatornázza be a brit vállalatok kereskedelmi érdekeinek támogatását az egyre növekvő nemzetközi kiberbiztonsági piacra. Érdemi előrelépést jelent a harmadik kiberstratégia,[28] amelyet a brit kormány 2016. november 1-jén adott ki, ismét deklaráltan öt évre. A dokumentum három stratégiai célt fogalmaz meg, ezért nevezhetjük a 2016-os kiberstratégiát a „3D stratégiájának" is: megvédeni *(defend),* elrettenteni *(deter),* fejleszteni *(develop),* amelyek megvalósulásához elengedhetetlennek tartja a nemzetközi fellépést. A célkitűzések közül a második kapcsán kiemelt szerep jut a kiberdiplomáciának. Az elrettentést ugyanis nemcsak *hard* eszközökkel képzelik el (mint a támadó kiberképességek fejlesztése), hanem az együttműködési csatornák további szélesítésével és mélyítésével is – ahogyan a stratégia fogalmaz: a britek tovább folytatják a már megkezdett globális kiberszövetség kiépítését, és továbbra is támogatják a nemzetközi jog kibertérben történő alkalmazását. A három stratégiai cél megvalósítása csak megfelelő nemzetközi keretek között képzelhető el. Az Egyesült Királyság továbbra is élharcosa a szabad, nyitott, békés és biztonságos kibertér megteremtésének,

[27] *The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World.* 2011. november.

[28] *National Cyber Security Strategy 2016–2021*. United Kingdom, HM Government, 2016. november 1.

ahol a nemzetközi jog alkalmazandó, és az alapvető emberi jogok érvényesülése biztosított online és offline egyaránt. Ebben az Egyesült Királyság számít nemcsak a hagyományos szövetségeseire, hanem új partnereire is, és igyekszik kihasználni az olyan multilaterális fórumok adta befolyásolási lehetőségeit, mint az ENSZ, a G20, az Európai Unió, a NATO, az EBESZ, az Európa Tanács vagy a Brit Nemzetközösség.[29]

A globális kiberszövetség kiépítése célkitűzésének megvalósításában kiemelt szerep jut a kétoldalú kiberkapcsolatoknak. A britek hagyományos szövetségesei közül kétségkívül az Egyesült Államok áll az első helyen, amellyel a „különleges kapcsolat" *(special relationship)* – vagy ahogyan az utóbbi időben hívják, „a legfontosabb kétoldalú kapcsolat" *(the most important bilateral partnership)* – keretében igen szoros kapcsolatokat ápol a szigetország a kiberkérdések vonatkozásában is már közel egy évtizede. Már 2011-ben rögzítették a magánszektor és az üzleti élet szereplői bevonásának, a kutatás-fejlesztés, valamint a joguralom alapintézményei kibertérben való alkalmazásának szükségességét.[30] 2015-ben Washingtonban Obama elnök és Cameron miniszterelnök egyeztetett az együttműködés részletkérdéseiről,[31] amelyet végül 2016. szeptember 7-én intézményesített a két védelmi miniszter által aláírt kiberegyezmény.[32]

Bár a szigetország még nem írt alá bilaterális egyezményt Kínával, azonban 2015. október 22-én a kínai elnök angliai látogatásán a két ország közös nyilatkozatot adott ki a globális, átfogó stratégiai partnerségük kiépítéséről, útjára indítva ezzel a bilaterális kapcsolat „aranykorát".[33] Ennek részeként rögzítették, hogy egymás ellen nem folytatnak, illetve nem támogatnak a szellemi tulajdon, üzleti titkok vagy bizalmas üzleti információk jogosulatlan eltulajdonítására irányuló kiberakciókat, amelyek célja a versenyelőnyhöz jutás.[34]

Az Egyesült Államokkal fennálló speciális partneri viszony nyomán nem meglepő, hogy az Egyesült Királyság 2012-ben Japánnal is kétoldalú kiberkapcsolatokat létesített. A kétévenkénti találkozók ötödik állomását Tokióban

[29] Molnár Dóra: Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia. *Hadmérnök,* 12. (2017), II. különszám „KÖFOP". 136–148. 144.

[30] *US-UK Cyber Communiqué*. 2011. május 25.

[31] *Fact Sheet: U.S.-United Kingdom Cybersecurity Cooperation*. The White House, Office of the Press Secretary. 2015. január 16.

[32] *U.S. – U.K. Cyber Agreement Opens Doors for Both Nations*. DoD News, 2016. szeptember 18.

[33] A brit politika egyes elemeiről részletesebben lásd *The Making of UK Strategy towards China*. 2019. április 4.

[34] *UK-China Joint Statement 2015*. Foreign and Commonwealth Office, 2015. október 22.

tartották 2020. január 31-én.[35] A megbeszélés alkalmával a kapacitásépítés és a nemzetközi porondon történő együttműködés lehetőségeiről tárgyaltak. Ez összhangban van a 2018-ban megrendezett negyedik találkozó során meghatározott fő együttműködési területekkel, amelyek között szerepel még a szabályalapú nemzetközi kiberrendszer támogatása és az IoT eszközök biztonságos használatával kapcsolatos nemzeti megoldások megosztása is.[36]

Az ázsiai bilaterális kapcsolatok közül végül Indiát emelem ki, amely a britek számára is hatalmas gazdasági potenciált rejt magában. Elég, ha arra gondolunk, hogy már ma is 600 millió internetfelhasználó és 650 millió mobilhasználó él az országban. Az indiai–brit biztonsági együttműködés egyik fontos aspektusát jelentik a kiberkérdések, és a 2012 óta folytatott indiai–brit kiberdialógus keretében olyan témák vannak napirenden, mint a kiberkockázatok csökkentése, a kiberbűnözés kezelése és az internetkormányzás globális, multilaterális, transzparens és demokratikus rendszerének kiépítése. 2018 áprilisában Londonban a két ország ötéves, 14 területre kiterjedő együttműködésről szóló keretmegállapodást írt alá. India ilyen széles körű kiberegyüttműködési megállapodást az Egyesült Királyságon kívül ez idáig csak az Egyesült Államokkal kötött.[37]

Az Egyesült Királyság számos európai országgal is létesített már kétoldalú kiberkapcsolatot. Közülük a lengyel–brit kiberegyüttműködési megállapodást emelem ki, nem elsősorban a benne foglaltak miatt (amely lényegi újdonsággal nem szolgál), hanem regionális jelentősége okán: a britek e kapcsolaton keresztül kívánják a kelet-európai és a nyugat-balkáni kiberkapacitás-építési programokat támogatni.[38]

Végezetül az Egyesült Királysággal kapcsolatban nem szabad megfeledkezni a Brit Nemzetközösségről, amely már önmagában is régóta fennálló diplomáciai fórum a részt vevő államok számára, de az utóbbi években már önálló napirendi kérdésként szerepel a kiberbiztonság kérdésköre is. A részt vevő államok együttműködésüket 2018. április 20-án intézményesítették a kiberdeklaráció aláírásával.[39] A nyilatkozat rögzíti a kölcsönös segítségnyújtási kötelezettséget a kiberkapacitások építésében és a kibertérrel kapcsolatos egységes vízió

[35] *The 5th Japan–UK Bilateral Consultations on Cyberspace*. 2020. január 31.

[36] *The 4th Japan–UK Bilateral Consultations on Cyberspace.* Japan-UK Joint Press Release, 2018. március 16.

[37] Rahul Roy-Chaudhury: *India-UK Cybersecurity Cooperation: The Way Forward*. 2019. november 22.

[38] *UK–Poland Cyber Cooperation Commitment*. 2017. december 21.

[39] *Commonwealth Cyber Declaration*. 2018. április 20.

megfogalmazásának igényét, amelyet az Egyesült Királyság anyagilag is támogat, 15 millió fonttal hozzájárulva a rögzített célok megvalósításához.[40]

Zárógondolatok

Az előző fejezetben már hivatkoztam az egyes államok kiberpotenciálját rangsoroló Globális Kiberbiztonsági Indexre. Az index alapján a világ vezető kiberhatalma az Egyesült Királyság, a harmadik helyen pedig Franciaország található. A harmadik vizsgált állam, Németország a 26. helyet szerezte meg.[41] Igen érdekes ugyanakkor, hogy az ötödik vizsgált terület, az együttműködés vonatkozásában az angolok igen jó pontot értek el, míg a diplomáciai nagyhatalomnak számító Franciaország jelentős lemaradásban van. Az európai kiberbiztonság vizsgálata azonban nem ér véget a három nagy állam bemutatásával. Számos üdítő példa létezik arra, hogy kis országok milyen nagy sikereket tudnak elérni a kiberbiztonság területén. Az index ezt is visszatükrözi, ugyanis a 4. helyen Litvánia, az 5. helyen pedig Észtország áll az összesített világrangsorban. Mindez természetesen nem véletlen: elég, ha arra gondolunk, hogy ezeket az államokat érte elsőként olyan horderejű kibertámadás a 2000-es évek vége felé, amely a kiberkérdéseket az államok biztonsági agendájának élvonalába emelte. Mindkét állam magasabb részpontszámot ért el az együttműködés területén, mint a három vezető nagy állam. Ez az eredmény jól jelzi, hogy a kis államok milyen nagy hangsúlyt helyeznek a kiberdiplomácia fontosságára, és a békés diplomáciai eszközök használatát előrébb valónak tartják a hard kapacitásoknál. Az európai térség pedig valamennyi részkérdés tekintetében magasan a világ előtt jár, így az együttműködés vonatkozásában is, amely talán alapul szolgálhat egy békés kibertér alapjainak lerakásához.

Felhasznált irodalom

Analysis: Untangling the Web of Multi-Level Cyber Diplomacy. 2018. Online: www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/may/nalysis-untangling-the-web-of-multi-level-cyber-diplomacy/.

[40] *Analysis: Untangling the Web of Multi-Level Cyber Diplomacy*.
[41] *Global Cybersecurity Index*. 2018.

ANSSI/BSI Common Situational Picture. 1. 2018. 1. –2018. július. www.ssi.gouv.fr/uploads/2018/07/bilateral-french-german-it-security-situation-report.pdf.

Appel de Paris pour la confiance et la sécurité dans le cyberespace. 2018. november 12. Online: www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf.

Burgess, Christopher: *Dissectiong China's Global Bilateral Cybersecurity Strategy.* 2016. Online: https://securityboulevard.com/2017/10/dissecting-chinas-global-bilateral-cybersecurity-strategy/.

Chazan, Guy: German Cyber Security Chief Backs 5G 'No Spy' Deal over Huawei. *Financial Times,* 2020. február 28. Online: www.ft.com/content/5a0fe826-3b34-11e9-b856-5404d3811663.

Commonwealth Cyber Declaration. 2018. április 20. Online: https://thecommonwealth.org/sites/default/files/inline/CommonwealthCyberDeclaration_1.pdf.

Cyber Policy: Multilateral Solutions for the Future. Federal Foreign Office, 2019. szeptember 25. Online: www.auswaertiges-amt.de/en/aussenpolitik/themen/multilateralism-cyber/2250332.

Cybersécurité: Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans la cyberespace. Liste des soutiens à l'appel de Paris (actualisé le 14 novembre 2018). Online: www.diplomatie.gouv.fr/IMG/pdf/soutien_appel_paris_cle8e5e31.pdf.

Cyber Security Strategy for Germany 2016. Federal Ministry of the Interior. Online: www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf.

Défense et sécurité des systèmes d'information: Stratégie de la France. 2011. Online: www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf.

Dinard Declaration on the Cyber Norm Initiative. 2019. április 6. Online: www.diplomatie.gouv.fr/IMG/pdf/g7_dinard_declaration_on_cyber_initiative_cle4e553d.pdf.

Fact Sheet: U.S. – United Kingdom Cybersecurity Cooperation. The White House, Office of the Press Secretary. 2015. január 16. Oline: https://obamawhitehouse.archives.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation.

Global Cybersecurity Index. UN ITU, 2019. Online: www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Inititative pour des normes dans le cyberespace. Synthese des enseignements tirés et des bonnes pratiques. 2019. augusztus 26. Online: www.diplomatie.gouv.fr/IMG/pdf/_fr_synthesis_cyber_norm_initiative_cle025b33.pdf.

Joint Statement on U.S.–Germany Cyber Bilateral Meeting. 2016. március 24. Online: https://2009-2017.state.gov/r/pa/prs/ps/2016/03/255082.htm.

La diplomatie française à l'ère numérique. Consulat Général de France á Ekaterinbourg. 2019. május 29. Online: https://ru.ambafrance.org/La-diplomatie-francaise-a-l-ere-numerique.

La France et la cybersécurité (é. n.). Online: www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-france-et-la-cybersecurite/.

La Revue Stratégique de Cyberdéfense. SGDSN, 2018. február 12. Online: www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

La stratégie nationale pour la sécurité de la numérique 2015. Online: www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf.

Laudrain, Arthur P. B.: *France's New Offensive Cyber Doctrine*. 2019. február 26. Online: www.lawfareblog.com/frances-new-offensive-cyber-doctrine.

Livre Blanc. Défense et sécurité nationale 2013. Online: www.defense.gouv.fr/content/download/206186/2286591/file/Livre-blanc-sur-la-Defense-et-la-Securite-nationale%202013.pdf.

Molnár Dóra: Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia. *Hadmérnök,* 12. (2017), II. különszám „KÖFOP". 136–148. Online: http://hadmernok.hu/170kofop_09_molnar.pdf.

National Cyber Security Strategy 2016–2021. United Kingdom, HM Government, 2016. november 1. Online: www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Parameswaran, Prashanth: *Singapore–Germany Cyber Cooperation in Focus with Introductory Visit*. 2018. augusztus 14. Online: https://thediplomat.com/2018/08/singapore-germany-cyber-cooperation-in-focus-with-introductory-visit/.

Rapport d'Information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense. Par le Sénateur M. Jean-Marie Bockel. Sénat Session extraordinaire de 2011–2012. Enregistré á la Présidence du Sénat le 18 juillet 2012. Online: www.senat.fr/rap/r11-681/r11-6811.pdf.

Rogusky, Przemyslaw: *France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I.* 2019. szeptember 24. Online: http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/.

Roy-Chaudhury, Rahul: *India–UK Cybersecurity Cooperation: The Way Forward*. 2019. november 22. Online: www.iiss.org/blogs/analysis/2019/11/sasia-india-uk-cyber-security-cooperation.

Second Edition of the Franco–German Common Situational Picture. 2019. május 21. Online: www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/D-F_Reports/Common_Situational_Picture_2019.pdf?__blob=publicationFile&v=2.

Troisième dialogue stratégique France-États-Unis en matière de cybersécurité (Paris, 22 janvier 2020). 2020. Online: www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/lutter-contre-la-criminalite-organisee/la-france-et-la-cybersecurite/actualites-et-evenements-lies-a-la-cybersecurite/article/troisieme-dialogue-strategique-france-etats-unis-en-matiere-de-cybersecurite-22.

The 4th Japan–UK Bilateral Consultations on Cyberspace. Japan–UK Joint Press Release, 2018. március 16. Online: www.mofa.go.jp/press/release/press4e_001960.html.

The 5th Japan–UK Bilateral Consultations on Cyberspace. 2020. január 31. Online: www.mofa.go.jp/press/release/press4e_002766.html.

The Making of UK Strategy towards China. 2019. április 4. Online: https://publications.parliament.uk/pa/cm201719/cmselect/cmfaff/612/61210.htm.

The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World. 2011. november. Online: www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

Three Priorities for Cyber Diplomacy under the German OSCE Chairmanship 2016. Berlin, German Institute for International and Security Affairs, Berlin, 2015. november 11. Online: www.swp-berlin.org/en/point-of-view/three-priorities-for-cyber-diplomacy-under-the-german-osce-chairmanship-2016/.

UK–China Joint Statement 2015. Foreign and Commonwealth Office, 2015. október 22. Online: www.gov.uk/government/news/uk-china-joint-statement-2015.

UK–Poland Cyber Cooperation Commitment. 2017. december 21. Online: www.gov.uk/government/publications/uk-poland-cyber-co-operation-commitment-joint-statement/uk-poland-cyber-co-operation-commitment.

U.S.–U.K. Cyber Agreement Opens Doors for Both Nations. DoD News, 2016. szeptember 18. Online: www.defense.gov/Explore/News/Article/Article/937878/us-uk-cyber-agreement-opens-doors-for-both-nations/.

US–UK Cyber Communiqué. 2011. május 25. Online: www.gov.uk/government/publications/us-uk-cyber-communique és https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62647/CyberCommunique-Final.pdf.

[Vákát oldal]

Nyáry Gábor

Kiberbiztonság és külgazdasági kapcsolatok: a digitális gazdaság dilemmái

Bevezetés

2020 májusában, amikor az új koronavírus-világjárvány első hulláma kicsit engedett szorításából, szűkszavú hír jelent meg.[1] A korábbi hónapok drámai bejelentéseihez képest ártatlannak tűnő szövegre azonban okkal figyeltek fel a szakemberek. Az amerikai Szövetségi Nyomozó Iroda, az FBI és a Kiberbiztonsági és Infrastruktúra Védelmi Hatóság a Kínai Népköztársasághoz köthető kiberszereplők fokozott aktivitására figyelmeztettek. Az állami és a magánszférába tartozó „érdeklődők" a Covid–19-járványhoz kapcsolódó kutatási adatokat és szellemi tulajdont igyekeztek illegálisan megszerezni. Amerikai egészségügyi intézmények, gyógyszergyárak, kutatólaboratóriumok hálózatait támadva azonosították, gyűjtötték a koronavírus-vakcinákkal, -gyógyszerekkel kapcsolatos létfontosságú információkat.[2] Más szóval nemzetbiztonsági adatokat. Ám ezek az adatok, joggal mondhatjuk, ugyanakkor roppant üzleti értéket képviselő, gazdasági információk is. A 21. századi kibervalóság fontos mozzanata éppen ez: a kibertér egyszerre országok közötti politikum és nemzeteken átívelő gazdasági terep. Amikor „kiberbiztonságról" beszélünk, szinte mindig gazdasági vetületeket is érintünk alatta. És viszont: az egyre inkább digitalizálódó, globális „kibergazdaság" mindig egyfajta biztonsági téma is. Biztonság és gazdaság – a kibertér két oldala. A kiberdomén mint gazdasági mező, üzleti érdekek és ambíciók egyszerre virtuális és nagyon is valóságos térsége ma még kialakulóban van:

[1] *FBI–CSISA PSA PRC Targeting of COVID-19 Research Organisations.* 2020.

[2] A kiberdiplomácia elismert kutatóbázisa, a genfi DiploFoundation havi jelentése egyenesen úgy fogalmazott: „A világban a kiberbűnözés is visszatért a szokványos kerékvágásba." A kutatócsoport is egyértelműen jelezte: a kibertérben megszaporodott támadások többsége kórházak, kutatóintézetek ellen irányul, alapvetően a gazdasági kiberhírszerzés és kibertolvajlás eseteit szaporítva. A primer „nemzetbiztonsági" vagy politikai jellegű kiberakciók mintha háttérbe szorultak volna, noha az akciókban részt vevők között szép számmal akadnak állami aktorok is. *Digital Watch Newsletter.* 2020.

https://doi.org/10.36250/01008_06

evolúcióját, fejlődési irányait, szabályozási kereteit ma még kérdések, élénk nemzetközi viták kísérik. Minden jel arra mutat: a kibertér mint gazdasági szféra dilemmái a kiberdiplomácia napirendjének fő tételei maradnak még egy időre.

Digitális geoökonómia

Kötetünk bevezető tanulmányában a kibertér geopolitikai értelmű koncepcióját igyekeztünk bemutatni. Elsőnek említettük, hogy úgy tekinthetünk a kibertérre, mint az internet, a számítástechnikai eszközök, a rajtuk futó szoftverek, sőt az őket használó, mindinkább hálózatokba szerveződő alkalmazók összességére. Ehhez hozzátettük a korszak (ismét divatba jövő) hatalmi-politikai koncepcióját, a geopolitika fogalmát, amely lényegét tekintve azt hangsúlyozza: a nemzetek egymás közötti viszonyát, érdekérvényesítési mozgásait nagymértékben befolyásolják bizonyos hosszú távon állandó struktúrák. Elsősorban persze maga a környezet, a fizikai tér: az ország elhelyezkedése, domborzati viszonyai, vízrajza, népesedésföldrajza.[3] Most, a kibertér gazdasági aspektusait szemügyre véve, elérkezettnek látjuk az időt arra, hogy ezzel az újabb vetülettel bővítsük koncepciónkat. Azzal a területtel, amelyet talán a digitális geoökonómia fogalma írhat le a legjobban.[4]

Keretek és fogalmak

Ha korábban (e kötet bevezető fejezetében) siettünk hangsúlyozni, hogy a „geopolitika" kifejezés távolról sem rendelkezik valamilyen egységes, mindenki által elfogadott jelentéstartalommal vagy akár használattal, akkor még erőteljesebben érdemes most figyelmeztetni rá: az általunk bevezetett újabb szóösszetétel, a „geoökonómia" sincsen jobb helyzetben. Sőt! Sokan, sokféle jelentésárnyalattal

[3] Nyáry Gábor: Kiber geopolitika. Mesterséges intelligencia alkalmazások az államigazgatás külpolitikai alrendszereiben. *Új Magyar Közigazgatás,* 13. (2020), 1. 32–39.

[4] A koncepciónak nincs túlságosan kiterjedt szakirodalma (összevetve legalábbis a geopolitika fogalomkörével). A probléma egyik legkitűnőbb exponálására vállalkozik Sami Moisio: Re-Thinking Geoeconomics: Towards a Political Geography of Economic Geographies. *Geography Compass,* 13. (2019), 10. 1–13. Ugyanakkor magyar nyelven ad kiváló betekintést és általános hátteret Pintér István (szerk.): *Műhelymunkák. A virtuális tér geopolitikája. 2016/1.* Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016.

alkalmazzák: vannak, akik létjogosultságát is vitatják, de az mindenesetre jól látható, hogy még a szakmai közbeszédben sem tudott annyira gyökeret verni, mint rokona, a „geopolitika".[5] Pedig a „geoökonómia" – noha a szóösszetétel valóban kicsit félrevezető lehet – rendkívül pontos és fontos meglátást takar. Érdemes ehhez felidézni azt a szerzőt, aki a világpolitika tektonikus átalakulásainak időszakában, az 1990-es évek legelején (ismét) divatba hozta az elképzelést. Edward Luttwak, a stratégiaelmélet és stratégiatörténet egyik sokat kritizált, de kétséget kizáróan legeredetibb gondolkodója nyers őszinteséggel fogalmazta meg a kor egyre szembeötlőbb jelenségét: a gazdaság, és különösen a nemzetközi gazdaság – valójában harc, háború. Ennek a háborús jellegnek az érzékeltetésére vezette be a geoökonómia fogalmát.[6] Ugyanakkor ez az időszak volt az a történelmi pillanat, a hidegháború vége, amikor sokan gondolták úgy, hogy az államok közötti konfliktusok katonai megoldása örökre a múlté lett.[7] Luttwak geoökonómia-kifejezése azt hangsúlyozza: immár a katonai erő helyett a gazdaság, a nemzetközi kereskedelem eszköztárával vívják majd küzdelmeiket a rivális világhatalmak. Akár úgy is fogalmazhatunk: a geoökonómia szűkebb jelentéstartalmú, mint a fegyveres erőszakot is magába foglaló geopolitika, ám a puszta külgazdasági kapcsolatrendszernél szélesebb.[8] Az elképzelés jogosságát, használhatóságát és időtálló jellegét jól bizonyítja a világ globális nagyhatalma, az USA 2017-es Nemzetbiztonsági stratégiája, amely precíz erővel mondja ki: a gazdaság biztonsága – nemzetbiztonsági kérdés.[9] Ha most egy pillanatra felidézzük a jelen fejezet bevezető gondolatai között említett mostani példát, ahol állami szereplők igyekeznek nemzetbiztonsági horderejű üzleti titkokat megszerezni és eltulajdonítani a kibertérben, akkor kezdjük látni, hogyan kapcsolódnak egymásba ezek a körök.

[5] Mihael Wigell et al. (szerk.): *Geo-economics and Power Politics in the 21st Century* (London, Routledge, 2019) a terminológiai kérdések áttekintése mellett a koncepció jól alkalmazható leírását adja.

[6] Edward Luttwak (From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce. *The National Interest,* [1990], 20. 17–23.) későbbi követői tovább is léptek a történelmi parafrázisgyártás terepén, és egyenesen a 19. századi nagy porosz katonai gondolkodó, Clausewitz híres mondatát fogalmazták át így: „A gazdaság a háború folytatása más eszközökkel."

[7] Nem véletlenül éppen ez az a pillanat, amikor például megszületik – az amerikai politikatudós Joseph Nye tollából – a nemzetközi kapcsolatok elméletének egyik leghíresebb koncepciója, az államok békés érdekérvényesítését hangsúlyozó *soft power* fogalma.

[8] Franz-Stefan Gady: *Interview: Robert Ward and Yuka Koshino on Geo-Economics in East Asia*. 2020.

[9] Gady (2020): i. m.

A kibervilág mint a politikum színtere – ezt a felfogást igyekszik megragadni a „kibergeopolitika" koncepciója (erről szóltunk részletesen e könyv bevezető fejezetében). Létezik azonban egy másik dimenzió, ahol a kibertér mint gazdasági-üzleti folyamatok színtere jelenik meg. Ez a „kiber-geoökonómia" (vagy digitális geoökonómia) területe. Alapvetően ez határozza meg a digitális gazdaság jellegét, működési módjait, folyamatait.

Digitális gazdaság

Digitális gazdaságot mondtunk, és okkal: ma már a szakmai nyelv bevett kifejezésévé vált ez a szókapcsolat. A 2000-es évek elejétől ugyanis érezhetően gyorsuló tempójú jelenség formálja a világ szinte valamennyi társadalmát: a digitalizáció. Sommás megfogalmazással úgy jellemezhető ez a folyamat, mint amelyben az adatok és a hálózatok körbefonják, átitatják a termelési folyamatokat, a kormányzati és személyes fogyasztást, a határokon átívelő kereskedelmi forgalmat és természetesen a gazdaságot mozgató pénzügyeket is.[10] Némi óvatosság azonban nem árt! A „digitális gazdaság" kifejezés, nyilvánvaló jelentéstartalma ellenére, tudományos értelemben nem egységes koncepció, nem elfogadott definíció. A globális gazdaságstatisztikákban megkerülhetetlen Nemzetközi Valutaalap a digitális gazdaság teljesítményéről szólva leszögezi: még abban sincs teljes egyetértés, hogy mit értsünk a gazdaság „digitális szektorán", vagy miket soroljunk a „digitális termékek" körébe. Noha a szakmai beszédben mára teljességgel polgárjogot nyert, és így mi is használjuk a „digitális gazdaság" fogalmát, ne veszítsük szem elől, hogy ez még egy alakuló, formálódó koncepció, folyamatosan bővülő jelentéstartalmakkal.[11]

[10] *Measuring the Digital Economy.* 2018. 6. A téma friss áttekintését adja Vladimir M. Filippov et al. (*The Cyber Economy. Opportunities and Challenges for Artificial Intelligence in the Digital Workplace.* Cham, Springer Nature, 2019), aki rávilágít arra, hogy a meglehetősen következetlen fogalomhasználat csak tovább bővül azzal, hogy a korábbi „internetgazdaság" kifejezés helyébe mind gyakrabban lép az „ipar 4.0" fogalom is, tehát a dolgok internete (Internet of Things – IoT) által forradalmasított és átalakított gazdaság.

[11] *Measuring the Digital Economy.* 2018. A pontosság kedvéért érdemes megjegyezni, hogy a nemzetközi statisztikák, egyebek mellett az ENSZ gazdaságstatisztikai rendszere, „információs és kommunikáció technológiai (IKT-) szektorról" beszél, valamint egy „tartalom- és médiaipari szektorról". A kicsit szabadabban vett szakmai közbeszéd nagyjából e két kategóriához sorolható fogalomkészleteket érti a „digitális gazdaság" alatt.

A definíció feljebb ismertetett nehézsége miatt a számadatokkal is óvatosan érdemes ugyan bánni, de a digitális gazdaság teljesítménye, fejlődési üteme így is figyelemre méltó. Mértékadó számítások szerint a digitális gazdaság aránya a világgazdaság összteljesítményén belül eléri a 22,5%-ot.[12] A digitalizáció terén hagyományosan az élen szereplő Egyesült Államok 5,9 billió dolláros digitális gazdasága az ország GDP-jének mintegy 33%-ára rúg. A szakemberek különösen fontos szerepet, gazdaságnövekedési motort látnak a digitális befektetésekben: ez az USA-ban, 2020-ra számítva, további 2,2%-os GDP-növekedést eredményez.[13] A digitalizáció terjedésének, a digitális gazdaság növekvő potenciáljának kihasználásához elengedhetetlen az IKT-technológiák széles körű társadalmi befogadása és abszorpciója is. A digitális gazdaságban rejlő lehetőségek kiaknázására való képességet mutatja a Világgazdasági Fórum Hálózatos Készenléti Indexe (NRI), ahol az Egyesült Államok már csak az 5. helyen áll, előtte Szingapúrral, Finnországgal, Norvégiával és Svédországgal.[14]

Kiberbiztonság és nemzetközi kereskedelem

Az üzlet, a gazdaság ma már ezer szálon kapcsolódik az internethez, az IKT-technológiákhoz. Az országhatárokon átnyúló, nemzeteket összekötő külkereskedelem esetében pedig ma már nem mozdulhat áru vagy szolgáltatás a kibertér (valamilyen formában történő) érintése nélkül. A kibertér szabályozási, kormányzási-igazgatási kérdéseivel foglalkozó kiberdiplomácia fókuszában éppen ezért egyre előkelőbb helyre kerülnek a kereskedelem, sőt általában véve a digitális

[12] Chooi Shi Teoh – Ahmad Kamil Mahmood: National Cyber Security Strategies for Digital Economy. *Journal of Theoretical and Applied Information Technology,* 95. (2017), 23. 6510–6522. 6511. A számítások természetesen eltérő eredményeket hoznak. A Foreign Policy folyóirat adatkormányzásról, nemzetközi kiberdiplomáciai és szabályozási törekvésekről szóló friss összefoglalója például a globálisan előállított GDP 15,5%-ára teszi a digitális gazdaság teljesítményét. Jellemző adat azonban ezen belül is: a nagy internetes platformok (mint a Google, Facebook, WeChat stb.) együttes értéke teszi ki a világ GDP-jének csaknem 10%-át. *Data Governance. Part I. Emerging Data Governance Practices.* 2020.

[13] Teoh–Mahmood (2017): i. m. 6511.

[14] Teoh–Mahmood (2017): i. m. 6511.

gazdaság és a kibertér kapcsolódási területein felbukkanó kockázatok, problémák.[15]

Közhely már lassan, de érdemes sokadszorra is hangsúlyozni: a modern gazdaságokban egyre nagyobb szerepet kap az adat; sőt hovatovább meghatározóvá válik a szerepe. Nem véletlenül élnek gyakorta az új fordulattal: az adat a 21. századi gazdaságok „olaja". Az adat pedig, nem mondunk ezzel meglepőt, a kibertérben él, ott sokasodik, ott mozog. Ahogy bővül (méghozzá exponenciális sebességgel) a világban felhalmozódó adattömeg, ahogy terjeszkedik, bővül a digitális gazdaság – egyre növekszik a kiberbiztonsági kockázatok abszolút és relatív mértéke.[16] A digitális gazdaság, és különösen az élenjáró technológiák, az adatok tömegének határokon átnyúló globális áramlásától függenek ma már: az adat élteti az innovációt, adatokon alapul a termelőeszközök beszerzése, és adatok teszik lehetővé a késztermékek és szolgáltatások kiszállítását is. A mesterséges intelligencia (a továbbiakban: MI), az elkövetkező évtizedek nagy ígérete adatok, méghozzá hatalmas adattömegek nélkül semmire sem menne. Az MI-technológiák egyik legfontosabb területét jelentő gépi tanuló rendszerek például hatalmas adattömegeken „tréníroznak". Ezeknek az adatoknak egy része ma már a globális digitális hálózatokon át jut felhasználási helyére.

De ott van az e-kereskedelem, amelynek révén nem csupán a gazdasági élet mamutjai, de kis- vagy akár mikrovállalkozások is szerves kapcsolatba léphetnek a kibertérrel. Az elektronikus kereskedelemben is az adat az éltető elem, és ez az esetek jó részében itt is globális forgalmat jelent. Az Egyesült Államokban például a közismert eBayre felcsatlakozott kisvállalatok 97%-a exportál is, azaz aktívan kapcsolódik be a nemzetközi kereskedelmi forgalomba.[17] De ma már az internetes hozzáférés és a határokon átívelő adatáramlás jellemzi a szolgáltató szektor jelentős szeletét is. A szolgáltatások egyre nagyobb hányadát adják és veszik online hálózatokon át.

[15] Pascal Brangetto et al. (*Economic Aspects of National Cyber Security Strategies. Project Report.* Tallin, CCDCOE, 2015) egyik fő erőssége, hogy az egyes nemzeti kiberbiztonsági stratégiák explicit gazdasági vetületeit veszi számba, amire viszonylag kevés példa akad a szakirodalomban.

[16] Joshua Meltzer: *Cybersecurity, Digital Trade, and Data Flows. Re-Thinking a Role for International Trade Rules.* 2019. 7. Ugyanakkor a téma átfogó áttekintéséhez, az elsődlegesen biztonsági fókuszú kiberbiztonsági koncepciók egyre erőteljesebben jelentkező gazdasági összefüggéseihez itt találunk rendkívül hasznos adalékokat: Brangetto (2015): i. m.

[17] Meltzer (2019): i. m. 5.

A digitális gazdaságot és a globális adatáramlást fenyegető kiberfenyegetések öt nagyobb területet ölelnek fel.[18] Az első terület maga a nemzetbiztonság térrendszere: a fegyveres erők, a nemzetbiztonsági szervezetek. A második nagyobb terület, ahol a kibertér fenyegetései ma már több mint kézzelfoghatóak egyes esetekben, a kritikus infrastruktúra területe. A harmadik nagyobb fenyegetési terület az üzleti-kereskedelmi titkok területe. A negyedik olyan terület, ahol a kibervalóság fenyegető árnya tornyosul, az egyéb online információk hatalmas gyűjtőterülete. És van még egy ötödik tér, ahol a kiberfenyegetésekkel szembeni sérülékenység gyors tempóval növekszik: a nemzetközi befektetésekre vonatkozó (kulcsfontosságú) információk szintén hatalmas tere. Ebben az összefüggésben érthető, hogy az államokra egyre nagyobb mértékben nehezedik a magángazdaságba tartozó szereplők kiberbiztonságának védelme, garantálása, amiből a kiberdiplomácia struktúrái is kiveszik a részüket.

Érdemes egy pillanatra kitekinteni: a kiberincidensekkel, kibervédelemmel kapcsolatos híradásokban – érthető módon – a nemzetbiztonsági, politikai jellegű akciók és események kapnak különös hangsúlyt.[19] Ugyanakkor, ha a bevezetőben említett, gyógyszeripai információszerző kiberakciókon elgondolkodunk, és szemügyre vesszük az (ismertté vált) ilyen incidensek folyamatosan bővülő listáját, akkor jól látható tendencia bontakozik ki a szemünk előtt.[20] Érzékelhetően növekszik a gazdasági jellegű kiberakciók mennyisége és az ilyen támadások intenzitása. A jelenség nagyobb időtávban szemlélve is ehhez hasonló képet mutat: gyors pillantást vetve például a CSIS vezető agytröszt fontosabb kiberakciókat rögzítő listájára, viszonylag nagy számban sorjáznak rajta a gazdasági jellegű beavatkozások.[21] A témával kapcsolatban van olyan kutató, aki egyenesen a gazdasági kiberkémkedés aranykorát jósolja, illetve egyfajta aranylázhoz hasonlítja a virtuális terekben felerősödő, ipari-, pénzügyi-, gazdasági-, technológiaiinformáció-szerző aktivitást.[22] A kiberkémkedéssel foglalkozó szakirodalom ezt a felfelé ívelő trendet egészen a hidegháború végéig vezeti vissza. Többről van szó véletlen egybeesésnél, hogy a geoökonómia, tehát a nemzetközi gazdasági kapcsolatok fegyverként való használatának koncepciója éppen akkor

[18] Meltzer (2019): i. m. 8.

[19] Joyce Hakmeh: *Cybercrime and the Digital Economy in the GCC Countries.* London, Chatham House, 2017.

[20] *Covid-19 Cybercrime Weekly Update.* 2020.

[21] *Significant Cyber Incidents.* 2020.

[22] Danilo D' Elia: La Guerre économique á l'Ére du Cyberspace. *Hérodote,* 152–153. (2014), 1–2. 240–260. 243.

vert gyökeret, amikor a gazdasági előnyöket szem előtt tartó kibertevékenységek is sokasodni kezdtek.[23] Figyelemre méltó jelenség továbbá az is, hogy amíg korábban döntően állami szereplőkhöz kapcsolták a gazdasági jellegű kiber(kémkedési) akciók többségét,[24] addig az utóbbi évtizedekben stabilan erősödik a nem állami szereplőkhöz kapcsolható, gazdasági előnyszerzésért indított kiberhadműveletek aránya.

A fentiek fényében nem meglepő, hogy a kibertér vonatkozásában a „biztonság" és a „gazdaság" szféráinak egyre jobban kitapintható átlapolódásáról, összeolvadásáról beszélnek.[25] Összességében kijelenthető, hogy a kibertér egyre meghatározóbb szerepet játszik a nemzetközi kereskedelemben.[26] A kiberbiztonsággal kapcsolatos aggodalmak, beleértve a nemzeti és nemzetközi ellátási láncok épségével kapcsolatos kiberbiztonsági félelmeket is, arra sarkallják az államokat és a magánszféra szereplőit egyaránt, hogy hatékony lépéseket tegyenek a kibertér biztonságának megóvásáért. Egymást követően jelennek meg az újabb irányelvek és szabályozási keretrendszerek, amelyek gyors tempóban alakítják át a nemzetközi kereskedelmet. Újabb mechanizmusok és megállapodások formálódnak, amelyek a kibertér konfliktushelyzeteinek a feloldását célozzák, és hozzájárulnak a potenciális kiberbiztonsági fenyegetések csökkentéséhez. Érdemes itt kiemelni egy sajátos szegmenst, már csak azért is, mert a 2020-as év elejének globális egészségügyi krízise különösen ráirányította a témára a világközvélemény figyelmét. A globális pandémia, a koronavírus-járvány különös élességgel mutatta meg a globalizálódott gazdaság egyik legfontosabb tényezője, a globális ellátási láncolatok nagyfokú sérülékenységét. A kiberbiztonság és a kereskedelem összefüggéseit kutató szakemberek most különösen határozottan mutatnak rá a globális (és nemzeti) ellátási láncolatok kiberbiztonsági kérdéseinek fontosságára. Egyértelműnek látszik a konszenzus abban, hogy – ha az elkövetkező időszakban nem történik számottevő elmozdulás a kibertérben

[23] Russell Buchan: *Cyber Espionage and International Law.* Oxford, Hart, 2019. 23.

[24] A teljességhez hozzátartozik az is: az 1990-es évektől felerősödő, állami szereplők által folytatott gazdasági célú kiberakciók egy jelentős részében is a magánszektor gazdasági szereplői lettek a megszerzett információk „kedvezményezettjei".

[25] A nemzetközi kereskedelem erőteljes „felköltözése" a kibertérbe a korszak egyik igazán jellemző vonásaként értékelhető. Nem véletlen, hogy az államok közötti kiberkonfliktusok egy nem jelentéktelen része már most is a globális kereskedelmi ügyletekhez és csatornákhoz kapcsolódik. *International Trade Regulation and Cybersecurity* (é. n.).

[26] Keman Huang et al.: *Interactions between Cybersecurity and International Trade: A Systematic Framework.* Cambridge, MIT Sloan, 2018. 45.

való viselkedés normarendszereinek kialakításában – az ennek nyomán sokasodó kiberkonfliktusok és kiberincidensek rendkívül károsan érintik majd a nemzetközi kereskedelem egészét.[27] A kiberdiplomatákon tehát ezen a rendkívüli fontosságú gazdasági területen is nagyon sok múlik majd.

A digitális gazdaság dilemmái

A kibervilág, különösen annak gazdasági dimenziója, ma még képlékeny és formálódó terület. Olyan térsége a nemzetközi kapcsolatoknak, ahol több fontos kérdésben ellentétes felfogások és érdekek feszülnek egymásnak. És a tét óriási. Sokszor ezek a viták elvi jelentőségűnek tűnnek, pedig a valóságban jól tapinthatóan ott húzódnak a pőre gazdasági célok és érdekek. Ezért is gondoljuk azt, hogy ezeket a témákat itt, a kibertér gazdasági viszonyainak ismertetésekor indokolt körbejárni. Két különböző probléma, két egymással ellentétes attitűd, magatartás, szabályozási törekvés érdemel ebben az összefüggésben említést, de közös bennük: a digitális gazdaság mindkét nagy kérdéscsoportja valójában az „adat" körül forog, az adatról szól.[28] Az ok végül is könnyen érthető: ebben a modern gazdaságban már nem a fizikailag létező javak, termékek előállítása, forgalmazása, szállítása, vásárlása és fogyasztása a meghatározó. A számítástechnikai rendszerek terjedésével óriási tömegű információ generálása, feldolgozása, tárolása, változatos célú továbbhasznosítása, a hálózatokon (elsősorban az interneten) keresztüli továbbítása az, ami a gazdasági értékteremtő folyamatok központi mozzanatává válik. Az adat tehát az új erőforrás, ténylegesen egyfajta nyersanyag, ezért megszerzése, birtoklása, használata, feldolgozása hasonló kérdéseket vet fel, mint az ipari gazdaságok „hagyományos" nyersanyagainak esete. Az „adat" fogalmán itt általában különlegesen nagy adattömegeket értünk, ezek megjelölésére szolgál az úgynevezett *big data* fogalom.[29] Az adat különleges tulajdonságát, megváltozott gazdasági szerepét mutatja az is, hogy az illetéktelen

[27] Huang (2018): i. m. Az MI-technológiák alapvetően stratégiai jellegű orosz megítélésére és jelentőségére lásd még David Meyer: Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World. *Fortune,* 2017. szeptember 4.

[28] Barbara Roseb Jacobson – Katharina E. Höhne – Jovan Kurbalija: *Data Diplomacy.* Genf, DiploFoundation, 2018 kiváló, tömör áttekintését adja az adatok digitális gazdaságon belüli szerepének és a felmerülő szabályozási kérdéseknek.

[29] Az IBM informatikai óriáscég becslése szerint világunkban naponta mintegy 2,5 exabit adat keletkezik, amit egy szám után álló 18 nullával lehet kifejezni. Ennek az óriási mennyiségű adatnak

eltulajdonítás (magyarul adatlopás) a kiberbűncselekmények egyik jellemző válfajává kezd válni.[30] Az adat tehát érték, és a roppant sok adat roppant nagy gazdasági értéket képvisel.

Az internet szabadsága és a kiberszuverenitás mint gazdasági szempont[31]

Az egyik legjobban exponált (és kétségtelenül a legnagyobb horderejű) dilemma így hangzik: „az internet szabadsága" vagy a „kibertér szuverenitása"? Melyik volna a kívánatosabb?[32] A probléma gyökere tulajdonképpen a kibertérnek, ennek a furcsa technológiai-társadalmi-politikai struktúrának a különlegességében gyökerezik. A fogalomhoz ugyanis szinte születésétől fogva erősen kötődik annak „közlegelő" felfogása. Nagyon erős a vélekedés, hogy a kibervalóság egyfajta „digitális köztulajdon": olyan, mint az iparosodás előtti idők falusi társadalmainak közösen használt javai, az erdők, a halászó vizek, a legelők. Geopolitikai értelemben szemlélve olyasmi, mint a nyílt óceán vagy a világűr. Az internet szabadsága, vagy más megfogalmazással a netsemlegesség mellett lándzsát törők ezt a felfogást képviselik, és a kibertér nemzetközi szabályozását, szabályozottságát (tehát korlátait) igyekeznek a lehető legcsekélyebb mértékűre szorítani.[33] Ezzel ellentétben azonban létezik egy másik felfogás, egy másik vízió arról, hogyan kellene kinéznie és működnie ennek az egyszerre virtuális és nagyon is kézzelfogható világnak. A „kibertér szuverenitása" mellé állók azt az elvet tartják követendőnek, hogy a térbeliség legfontosabb ismérvei, a korlátozottság, a határok éppen olyan fontos és természetes velejárói a hálózatos világnak, mint a másiknak, a „valóságosnak". Ennek a koncepciónak a hívei

az „előállításában" persze nem kis szerepet játszik a társadalmakban élő (és egyre több IKT-eszközzel körülvett, azokat minden élethelyzetben használó) emberek sokasága.

[30] A tétek nagyságát mutatja az eddigi legnagyobb méretű adatlopás, amikor 2013-ban a Yahoo cég 3 milliárd felhasználójának személyes adatai (telefonszámoktól születési adatokon át rengeteg információ) kerültek illetéktelen adattolvajok kezébe. *Yahoo Says All 3 Billion Accounts Hacked in 2013 Data Theft.* 2017.

[31] Shaun Riordan: *Cyberdiplomacy. Managing Security and Governance Online.* Cambridge, Polity Press, 2019 az internetszabadság problematikájának legkitűnőbb bemutatását tartalmazza, miközben a kibertér diplomáciai napirendjének egyéb pontjait is példásan foglalja össze.

[32] Ayers jó összefoglalóját adja a kiberszuverenitás általános vetületeinek, hangsúlyosan a geopolitikai jellegre ügyelve. Lásd Cynthia Ayers: *Rethinking Sovereignty in the Context of Cyberspace*. Carlisle, US Army War College, 2015.

[33] Justin Sherman: *How Much Cyber Sovereignty Is Too Much Cyber Sovereignty?* 2019.

a kibertér alapos és aprólékos szabályozottságáért munkálkodnak a nemzetközi egyeztető fórumokon és formációkban is. A szakemberek úgy szoktak fogalmazni, hogy – nagy vonalakban persze – a liberális demokráciák képviselik a netsemlegesség elvét, és az autoriter rendszerű államok szorgalmazzák a szuverenitás elvének kiterjesztését a kibervalóságra is. Kétségtelen, hogy a formálódó multipoláris geopolitikai valóságban inkább a feltörekvő (erős regionális vagy globális pozícióra pályázó) országok ragaszkodnak a nemzeti szuverenitás elvének kiterjesztéséhez a digitális terekre is. Oroszország és Kína jellemzően e felfogás legfőbb szószólóinak számítanak, nem csupán elvben, de a nemzetközi kapcsolatok multilaterális fórumainak gyakorlatában is.[34] Természetesen az internet erős szabályozásában, korlátokkal történő lehatárolásában felsejlenek a nyilvánvaló hatalmi-politikai szándékok is. Érdemes azonban emlékezni rá: a kiberszuverenitás (ahogy ellentétpárja, a netsemlegesség is) legalább ennyire fontos gazdasági érdek.

A digitális gazdaság legfontosabb éltetője az adatok határokat átszelő, globális áramlása. Ennek az adatfolyamnak óriási a gazdasági, pénzügyi értéke: a McKinsey pénzügyi tanácsadó számításai szerint a digitális gazdaság értéke már jócskán meghaladja a külkereskedelmi forgalomba kerülő hagyományos javak által generált összegeket.[35] A növekedés ráadásul folytatódik, és ennélfogva a gazdaság új „olajának" tekintett adatjavak nemzetközi áramlásának szabályozása óriási gazdasági jelentőséggel bír. Az Egyesült Államok az elmúlt időszak nemzetközi kereskedelmi megállapodásai során a határokon átívelő szabad adatforgalom híveként kötelezte el magát. Amerika mind a csendes-óceáni úgynevezett TPP-egyezményben,[36] mind az USA–Mexikó–Kanada közötti kereskedelmi keretmegállapodásban, mind pedig az USA és Japán közötti digitális kereskedelmi egyezményben ragaszkodott annak garantálásához, hogy az adatok szabadon áramolhassanak a határokon át, illetve hogy a helyi adatokat ne legyen kötelező helyi szervereken tárolni.[37]

[34] Yi Shen: Cyber Sovereignty and the Governance of Global Space. *Chinese Political Science Review, (2016), 1.* 81–93.

[35] Sam DuPont: *An Open Alliance for Digital Trade*. 2020.

[36] Hivatalos nevén Transz-csendes-óceáni Partnerség, angolul Trans-Pacific Partnership.

[37] DuPont (2020): i. m. Figyelemre méltó, jelzés erejű mozzanat, hogy a nemzetközi kereskedelempolitikában a korábbi liberális felfogással sok szempontból szakító Trump-kormány alatt sem változott az USA internetszabadságra (az adatok szabad áramlására) vonatkozó prioritása. Ezt az álláspontot Amerika következetesen érvényesíti továbbra is, például a Világkereskedelmi Szervezetben (WTO) folyó multilaterális tárgyalásokon.

Ezzel a megközelítéssel élesen szemben áll az Egyesült Államokkal egyre inkább minden fronton erőteljes rivalizálásba kezdő Kína álláspontja. A WTO-ban folyó digitális kereskedelempolitikai tárgyalásokon egyértelműen azt a szempontot igyekszik érvényesíteni, hogy az egyes államok korlátozhassák a határaikon átfolyó adatáramlást, megszűrhessék az internetes forgalmat, illetve jogukban álljon egyes külföldi digitális tartalmakat blokkolni államhatáraikon belül. Ez az egyes szakemberek megfogalmazásában „kiber vesztfáliai" álláspont[38] tükröződik a (Kínán belüli internetet a külvilágról leválasztani képes) úgynevezett „Nagy Kínai Tűzfal" működtetésén, illetve a helyben keletkezett adatok helyi szervereken való tárolását előíró kínai jogszabályokban is. Hasonló pozíciót képvisel ebben a kérdésben Oroszország is: a globális internetről leválaszthatóan működő saját hálózat fejlesztése és próbaüzeme (akárcsak az egyes helyi adatok helyi tárolását előíró törvényei) világosan utalnak a kiberszuverenista álláspont melletti elkötelezettségére.[39] A nemzetközi viszonyok fokozatos átrendeződésének egyik jeleként az elmúlt évben több ország (Irán, Vietnám, Kazahsztán, Indonézia) is felzárkózott az ENSZ-ben a kínai és orosz kiberszuverenista javaslatok mögé, miközben más országok is (például a korábban a szabad adatáramlás mellett elkötelezett Japán, vagy különösen India) keresik a módját az adatfolyamok hatékony igazgatásának, kontrollálásának.[40]

[38] Chris Demchak – Peter Dombrowski: Cyber Westphalia: Asserting State Prerogatives in Cyberspace. *Georgetown Journal of International Relations,* (2013–2014). 29–38. A „Vesztfália" szó (ami néha az angolszász írásmód hatását tükröző Wesztfália formában is előfordul) gyökere a 17. század nagy európai békekonstrukciójáig nyúlik vissza. A harmincéves háborút lezáró nemzetközi szerződés teremtette meg a nemzetközi kapcsolatok modern szuverenitásfogalmát. Manapság az erős nemzetállami lét elsőségét hangsúlyozó külpolitikai-hatalmi felfogás elnevezésére használatos a vesztfáliai jelző.

[39] Sherman (2019): i. m.

[40] Sherman (2019): i. m. A téma európai uniós megközelítéséhez, és így a formálódó multipoláris rend egyik potenciális pillérének álláspontjához érdemes kézbe venni: Megan Dee: *The European Union in a Multipolar World. World Trade, Global Governance and the Case of the WTO.* London, Palgrave MacMillan, 2015. Ugyanakkor megkerülhetetlenül fontos ebben a témában is Riordan (2019): i. m. Fontos észrevételeket tartalmaz az európai erőközpontok (EU) pozíciójáról a befolyásos kutatóműhely, az European Council on Foreign Relations projektje. Stefan Scesanto: *Europe's Digital Power: From Geo-economics to Cybesrsecurity.* London, European Council on Foreign Relations, 2017.

Nyílt adatok és adatvédelem: az adatgazdaság alapjai[41]

Az új gazdaságot éltető virtuális nyersanyag, az adat egy másik (bár az előző polémiához természetesen több szálon is kapcsolódó) összefüggésben is vitákat, egymással ellentétes koncepciókat, sőt filozófiákat generál a 21. századi kibergazdaságban. Ezt a dilemmát úgy lehetne megfogalmazni: az adatok nyíltsága, transzparenciája a fontosabb, vagy inkább az adatok (különösen a személyes adatok) védelme legyen-e a digitális gazdaság vezérlőelve? A digitális gazdaságban működő cégek folyamatosan „vadásznak" az újabb és újabb adattömegekre. Különösen érvényes ez (mint később még látni fogjuk) a mesterségesintelligencia-fejlesztésekre, -alkalmazásokra épülő új iparágakban, amelyek az adattömegek nélkül gyakorlatilag nem is létezhetnek.

Nyílt adatnak azokat nevezhetjük, amelyek szabadon, megkötések nélkül és bárki számára hozzáférhetőek („elvihetők", felhasználhatók, továbbadhatók), és mint ilyenek gazdasági értékteremtés céljára (magyarul üzleti célokra) is felhasználhatók.[42] Fontos azt is látni: ahhoz, hogy az adat nyílt legyen, tehát – nemcsak elvben, de ténylegesen is – szabadon hozzáférhető és felhasználható legyen, ahhoz megfelelő formátumban és adatstruktúrában kell lennie. A nyílt adatokat (azok körét, felhasználhatóságát) általában jogszabály írja körül, és jellemző módon a közszférában keletkező (illetve a közszféra szervezetei és intézményei által birtokolt, tárolt, használt) adatokat öleli fel.[43] A nyílt adatok körébe tartoznak például az időjárási adatok, a kataszteri (ingatlanügyi) információk, műholdas felvételek, közműtérképek. Ezek használata a gazdasági élet szereplőinek döntési tevékenységét segítheti. Természetesen az adatok újrahasznosításában (továbbadásában) is jelentős gazdasági értékteremtési potenciál rejlik.[44]

[41] A rendkívül fontos kiberszabályozási témakör korszerű összefoglalóját mutatja be Dário Moura Vicente – Sofia de Vasconcelos Casimiro: *Data Protection in the Internet*. Cham, Springer Nature, 2020.

[42] Yannis Charalabidis: *The World of Open Data. Concepts, Tools and Experiences*. Cham, Springer Nature, 2018 a téma jó átfogó ismertetését adja, beleértve a nyílt közadatok kérdéskörét is. Bart Custers et al.: *EU Personal Data Protection in Policy and Practice*. Berlin, Springer, 2019 viszont az érem másik oldalát, az adatvédelem koncepcióját járja körül, különös tekintettel az EU gyakorlatára.

[43] *Open Government Data Report.* 2018.

[44] A McKinsey pénzügyi tanácsadó cég tanulmányának becslése szerint a kormányok által szabadon hozzáférhetővé tett, nyílt adatkészletek éves szinten és globálisan mintegy 3 billió dollárnyi új értéket teremthetnek a gazdaság néhány kulcsszektorában, elsősorban az oktatásban,

Az adatok szabad, korlátok nélküli felhasználásához fűződő, erős gazdasági érdekkel szemben áll ugyanakkor egy másik érdek is, amely az adatok védettségét, hozzáférhetőségének, mások által történő felhasználhatóságának erős korlátokat szabna. Ez az adatvédelem elsősorban a személyes adatok körét érinti. Az adatok védelmét szintén jogszabály rögzíti, és fontos megjegyezni, hogy ezen a téren az Európai Unió különösen élen jár (a mára közismertté váló, széles körben alkalmazott GDPR-szabályozás kidolgozásával).[45] Az adatvédelmi jogszabályok rögzítik azokat az elveket és körülményeket, feltételeket, amelyeket az adatok begyűjtőinek, tárolóinak és felhasználóinak szem előtt kell tartaniuk.[46]

Látható tendenciaként jelentkezik, hogy a mesterségesintelligencia-technológiák széles körű elterjedésével (például az arcfelismerő vagy más bionikus azonosító rendszerek tömeges alkalmazásával) az adatvédelem kérdése a korábbinál is hangsúlyosabbá válik. Üzleti, biztonsági szempontok és elvek ütköznek itt etikai, személyiségi jogi kívánalmakkal.

Államok és magánszereplők (governance-modellek)

A nemzetközi kiberbiztonsági rendszer, ahogy egyébként maga az egész digitális ökoszisztéma, a kibertér geopolitikai és geoökonómiai rendszere is képlékeny, alakulóban levő formáció. Szabályozó és működtető elveinek, normarendszerének kimunkálásánál (ahogy azt az előző két alfejezetben jól láthattuk) jelentősen eltérő szemléletek, különböző érdekek, egymásnak ellentmondó törekvések munkálkodnak. A kiberteret szabályozó és irányító elképzelésekben is két jelentős megközelítés tapintható. Az egyik a kibertér „kormányzását" alapvetően a szuverén államok hatáskörébe utalná, és döntően a nemzetközi jog már létező

a közlekedésben és az egészségügyben. *Open Data: Unlocking Innovation and Performance with Liquid Information. McKinsey Global Institute Report.* 2013.

[45] Az Általános Adatvédelmi Szabályozás (General Data Protection Regulation) 2018-ban lépett életbe az EU tagállamaiban. Normatív szerepét jól mutatja, hogy az unión kívüli gazdasági szereplők is csatlakoztak az alkalmazásához. A GDPR jelentős előrelépést jelentett az adatok védelme terén az EU korábbi, 1998-ban életbe léptetett adatvédelmi szabályzatához képest.

[46] Jellemzően például az adatok begyűjtőinek felelősnek (elszámoltathatónak) kell lennie az adatok „tulajdonosaival" szemben. Az adatok begyűjtése csakis jogszerűen történhet. A begyűjtött adatok köre nem lehet korlátlan, csak indokolt adatkörre és adatmennyiségre vonatkozhat. Az adatok tárolása is csak jogszabályban meghatározott, korlátozott időtartamig lehetséges. A begyűjtött adatok tárolása és felhasználása biztonságos körülmények között kell hogy történjék.

szabályrendszereit igazítaná az új geopolitikai, geoökonómiai térrendszer megváltozott valóságához, és alkalmazná a digitáliák világában is.[47] Illetve létezik egy másik felfogás, amelyik a magángazdaság szereplőit, elsősorban a nagy internetes cégeket, technológiai globális vállalatokat is bevonná a normatív szabályozásba, a digitális geoökonómiai komplexum igazgatásába. Az előbbi álláspont legfajsúlyosabb szószólója a nemzetközi porondon az Egyesült Államok, amely globálisan (és önkéntesen) elfogadott normarendszerrel biztosítaná a kibertér szabályozott működését, és amely a kibertérség irányításába bevonná a magángazdaság meghatározó szereplőit is. A másik elképzelést elsősorban Oroszország és Kína képviseli a vitákban, amelyek multilaterális szerződésrendszerrel, és így értelemszerűen csak szuverén szereplők (államok) által kormányozva garantálnák a kibervilág biztonságát, kiszámítható működtetését.[48]

Érdemes egy további pillantást vetnünk arra a megközelítésre, illetve törekvésre, amely a kibertér nemzetközi szabályrendszerének kimunkálásába kezdettől bevonná a magáncégek képviselőit is. Furcsának tűnhet, de ezt a gondolatot mindkét részről (nagyvállalati oldalról, illetve a szuverén állami aktorok térfeléről is) jelentős erők támogatják. Láttuk egy kicsit feljebb, hogy a technológiai cégek milyen óriási értékteremtő potenciállal rendelkeznek. A méretek összehasonlító érzékeltetésére érdemes rámutatni: a nagy internetes platformüzemeltető globális vállalatokat tömörítő cégcsoport együttes értéke mintegy 7 billió dollárra rúg, ami jelentősen meghaladja a világ bármely országának a GDP-jét, kivéve természetesen az USA-t és a Kínai Népköztársaságot.[49] A Rettegett Ötöknek is nevezett óriásvállalati kör teljesítményadatai egyenként is több, mint imponálóak: az élen természetesen a Microsoft áll az 1000 milliárd dollárt éppen meghaladó piaci kapitalizációs[50] értékkel, de nem sokkal marad el tőle az Amazon (888 milliárd dollár), az Apple (875 milliárd), a Google (741 milliárd) és a Facebook (496 milliárd dollár) piaci értéke.[51] A nemzetközi erőviszonyok további érzékeltetésére

[47] Stadnik Ilona: What Is an International Cyber Regime and How We Can Achieve It? *Masaryk University Journal of Law and Technology,* 11. (2017), 1. 129–154. 146. és Sash Jayawardane: *Cyber Governance: Challenges, Solutions and Lessons for Effective Global Governance.* The Hague, The Hague Institute for Global Justice, 2015. 5.

[48] Stadnik (2017): i. m. 134.

[49] *Data Governance. Part I. Emerging Data Governance Practices.* 2020.

[50] Egy vállalat piaci kapitalizációja olyan pillanatnyi piaci értékösszeget mutat, amelyet a piac (a befektetők) az adott időpontban a cégnek tulajdonít. Lényegében a vállalat részvényei számának és azok pillanatnyi piaci árfolyamának (ez folyamatosan változhat!) a szorzatával adható meg.

[51] Samuele Dominioni: *Digital Economic Powers and Digital Political Rulers*. 2019. október 17.

egyébként azt sem haszontalan megjegyezni: az első tíz ilyen technológiai óriásvállalat között két kínai található, a boly alsó végében.[52] Az ebben a roppant gazdasági erőben rejlő hatalmi realitás sok állam képviselői számára is azt diktálja, hogy célszerűbb ezeket a gigantikus szereplőket bevonni a játékszabályok kialakításába, a békés ügymenet fenntartásába. Ennek a felismerésnek válfajaként jelent meg a nemzetközi kiberdiplomáciai porondon egy merőben új tisztség és munkakör: a technonagykövet szerepköre. Első képviselője Casper Klynge hivatásos dán diplomata lett, aki országát szabályos nagyköveti meghatalmazással képviselte az USA-ban és Kínában is.[53] Azonban nem az említett országokhoz akkreditálva kezdte meg munkáját, hanem a világ vezető technológiai cégeihez „delegálva". Elsőként ennek megfelelően az amerikai Szilícium-völgyben épített ki képviseletet 2017-ben, majd hamarosan Pekingben is megnyitotta regionális irodáját Dánia technonagykövete.[54] Működésének deklarált célja az, hogy a (digitalizációban egyébként korántsem lebecsülendő teljesítményt mutató) skandináv ország közvetlen párbeszédet kezdhessen az internetgazdaság meghatározó szereplőivel, méghozzá éppen a nemzetközi szabályozási keretrendszer előmozdítására. Az állam–cég közvetlen együttműködés kiemelt tématerületei egyébként a kiberbiztonság, illetve a digitális gazdaság etikai kérdései is. A várakozás az, hogy ilyen új formájú „népi diplomáciai" szintek kiépítésével Dánia a technológiai fejlesztések élvonalába kerülhessen.

Mesterséges intelligencia: biztonság és gazdaság újraértelmezése a kibertérben

„Aki a mesterségesintelligencia-kutatásokban az élre kerül – az uralja majd az egész világot." Vlagyimir Putyin orosz elnök két éve elhangzott idézetét nyugodt szívvel választhattuk volna jelen tanulmány mottójának.[55] Az innovációkutatók a nagy társadalmi átalakítások motorjaként úgynevezett „általános célú technológiákat" (GPT) azonosítanak, amit persze talán pontosabb volna

[52] Dominioni (2019): i. m. A vezető technológiai nagyhatalmak között találjuk 402 milliárd dolláros piaci kapitalizációval a kínai Alibaba céget, illetve a szintén kínai Tencentet, 398 milliárd dollárral.

[53] Nurtilzah Rohaidi: *Exclusive: Meet the World's first Tech Ambassador*. 2017.

[54] *The World"s First Ambassador to the Tech Industry.* 2019.

[55] Meyer (2017): i. m.

„átfogó hatókörűnek" neveznünk. Ezek azok a technológiai újítások, amelyek (az általuk generált további részinnovációk sorával együtt) meghatározó változásokat idéznek elő a köznapi emberi életben és az üzleti-termelői világban egyaránt.[56] Ebben a körben az elmúlt kétszáz év nagy technológiai változtatásai négy egymást követő hullámban érkeztek: elsőnek a gőzgép, majd az elektromosság, illetve az informatika. A negyedik hullám hátán most érkezik éppen a mesterséges intelligencia.

Az innovációban rejlő geopolitikai és geoökonómiai[57] potenciál – amelynek érzékeltetésére a híres amerikai politikus és geopolitikai gondolkodó, Zbigniew Brzezinski sakktábla-metaforáját[58] emeltük ide – természetesen nem csupán az orosz vezető számára nyilvánvaló. Igazi technológiai versenyfutásnak lehetünk tanúi, amelyben egyébként Oroszország, szakértők véleménye szerint, a vezető helyről aligha álmodhat komolyan. A legesélyesebb versenyzőnek most többnyire Kínát tekintik: a 2015-ben bejelentett Made in China program 1,36 billió dolláros fejlesztési forrásai, amelynek zöme MI-kutatásokra és fejlesztésekre irányul majd, nagyságrenddel haladják meg a többi versenyző állam célzott fejlesztési befektetéseit. Ugyanakkor sokat számíthat a vetélkedésben az USA vállalkozás- és innovációbarátabb környezete, vagy az EU perspektivikusabb jogi szabályozó közegei. És a pénzügyi erőben tetten érhető hátrányos helyzet ellenére komoly versenyben van még az MI-forradalom kibontakoztatásában Japán, Nagy-Britannia, Franciaország, Németország, továbbá a már említett Oroszország és Kanada.

A verseny tehát éles, a tempó – ebben mindenki egyetért – exponenciálisan növekvő. Az elkövetkező évtized várhatóan döntő lesz ebben az új technológiai forradalomban. És ha igaz az, hogy a kibertér a geopolitikai érdekérvényesítés új, sőt meghatározó dimenziója, az egymással szemben nemzeti érdekeik érvényesítéséért küzdő szereplők 21. századi sakktáblája, akkor ezen a véresen komoly játékmezőn a mesterséges intelligencia lesz a legfontosabb bábu, a kibersakkjátszmák királynője.

A digitális diplomácia, a kiberdiplomácia szakértői nagyjából egyetértenek abban, hogy a mesterséges intelligencia két alapvető – és egymástól

[56] Indermit Gill: *Whoever Leads in Artificial Intelligence in 2030 Will Rule the World until 2100*. 2020.

[57] Filippov (2019): i. m. kitűnő, friss összegzése a digitális gazdaság problématerületeinek. Hangsúlyosan jelennek meg nála a mesterséges intelligencia alkalmazások nyomán támadó kibergeopolitikai és kiberbiztonsági kérdések is.

[58] Zbigniew Brzezinski: *A nagy sakktábla*. Budapest, Európa, 1999.

eltérő – módon kapcsolódhat, kapcsolódik a külügyi igazgatási struktúrák és különösen a diplomáciai szervezetek működéséhez.[59] Érdemes felidézni, hogy hasonló a helyzet az átfogóbb „digitalizáció" fogalom és a külügyek, illetve diplomácia kapcsolódási lehetőségeinél. A digitalizáció egyfelől tématerülete lehet a diplomáciának: ezt, az online terek, működések és szereplők szabályozásával kapcsolatos diplomáciai, államközi tevékenységet nevezzük mi „kiberdiplomáciának". Másfelől a digitalizáció új eszközöket biztosíthat a nemzeti külpolitikai érdekek érvényesítéséért felelős diplomáciai szervezetek hatékony és korszerű működéséhez. Ezt a technologizált eszközparkot és működést nevezzük „digitális diplomáciának". Hasonló kettősséget találunk a digitalizáció szélesebb témakörén belüli, meghatározó technológiai fejlesztések, a mesterséges intelligencia külügyi kapcsolódásainak esetében is.

Mesterséges intelligencia: fogalmi alapok

Elsőként is fontos leszögezni, hogy a „mesterséges intelligencia" nem egyetlen technológiát jelöl, hanem sokkal inkább a komputertudomány egy jellemzően interdiszciplináris kutatási területét, illetve az ezekhez kapcsolódóan fejlesztett technológiákat és alkalmazásokat. Az MI fókuszában az emberre jellemző intelligens tevékenységek (folyamatok) számítógépes rendszerek általi szimulációját értjük.[60] E tevékenységek felölelik mindenekelőtt az emberi tanulás képességét (tehát információk és az információk használatához szükséges szabályok megszerzésének képességét); felölelik továbbá az emberi érvelés képességét (tehát azt, hogy a szabályokra támaszkodva következtetéseket tud levonni); és különösen fontos képességként ölelik fel az önkorrekció képességét.

Érdemes kiemelni azt is: a mesterséges intelligencia szorosan kapcsolódik a big data fogalmához. A big data nagymennyiségű, rendkívüli változatosságú/összetettségű és gyorsan változó adattömeget takar. Ezek az adattömegek

[59] A fogalmi rendszer olyan kulcselemeinek, mint a „digitális diplomácia", illetve a „kiberdiplomácia" tisztázásához, illetve az átfogó digitális diplomáciai keretrendszer elemeivel kapcsolatos különbségtételekhez vö. Nyáry (2020): i. m.

[60] A mesterséges intelligencia áttekintéséhez jó kiindulás pontot ad a téma egyik legkiválóbb magyar kutatójának kötete: Futó Iván: *Mesterséges intelligencia*. Budapest, Aula, 1999. A mérnöki-informatikusi előképzettséggel nem rendelkező humán szakembereknek, olvasóknak különösen nagy segítséget jelenthet egy friss angol nyelvű monográfia: Tom Taulli: *Artificial Intelligence Basics. A Non-Technical Introduction*. Monrovia, Apress, 2019.

a hagyományos eszközökkel (például adatbázis-kezelőkkel) nem kezelhetők már. Feldolgozásukhoz éppen az MI-technológiák nyújtanak segítséget. Ugyanakkor elmondható az is: az MI egyik fontos technológiáját jelentő gépi tanulási eljárások nem képzelhetők el olyan (számottevő, többnyire a big data fogalomkörébe sorolható) adattömeg nélkül, amely az algoritmusok tréningezésére szolgál.

Fontos megemlíteni a mesterségesintelligencia-technológiák klasszifikációját, azaz főbb csoportjait vagy alosztályait. A diplomácia működési területén jelenleg alkalmazott okosmegoldások kapcsán szokás néha megemlíteni, hogy azok még aligha tekinthetők „igazi" mesterségesintelligencia-technológiáknak; valójában csak azokhoz hasonló, ám valójában inkább csak „pszeudó-MI"-technológiáknak nevezhetjük azokat.[61] Ez az óvatos megközelítés annak a tényleges jelenségnek egyfajta ellenhatása, amely a modern korban (különösen a nem szakmai közbeszédben), alapvetően divatmegfontolásból használ megalapozatlan fogalmakat.

Ténylegesen az MI-technológiákat szokás úgynevezett általános képességű mesterséges intelligencia, más néven „erős MI" kategóriába, illetve szűk alkalmazási képességű mesterséges intelligencia, más megnevezéssel „gyenge MI" kategóriába sorolni. A „gyenge MI" lényegében egyetlen célfeladat elvégzésére tervezett és betanított MI-technológiát takar. Jellemző példája a közönségkapcsolati rendszerekben alkalmazott beszélgetőrobot. Természetesen igaz, hogy ma még a diplomáciai feladatkörökben is többnyire ilyen MI-alkalmazásokat találunk. Akad azonban – igaz, egyelőre kísérleti jelleggel – példa az „erős MI" külügyi célú alkalmazására is: a lejjebb felvillantott esettanulmányoknál több példát is bemutatunk majd rá. Ezeknél a technológiáknál részben vagy egészben sikerül immár szimulálni az általános hatókörű emberi kognitív képességeket (tehát például egy addig ismeretlen feladat eredményes megoldásához szükséges „intelligenciát").

Az MI a diplomáciai szervezetek eszköztárában[62]

A bevezető részekben szó volt a geopolitikát várhatóan átformáló fejleményekről. Ugyanakkor a mesterségesintelligencia-technológiák nem csupán a nemzetközi kapcsolatok környezetét, az államok közötti vetélkedés geopolitikai sakktábláját

[61] Nyáry (2020): i. m.

[62] *Mapping the Challenges and Opportunities of Artificial Intelligence for the Conduct of Diplomacy.* 2019.

rajzolhatják át teljesen, de az államközi érdekérvényesítés békés intézményrendszerének tekinthető diplomácia eszköztárát is. Az adatok már ma is a diplomáciai háttérműveletek éltető alapanyagát szolgáltatják. A big datára alapozott eszközök, részben már MI-alkalmazások a digitális diplomácia eszközrendszerének gerincét képezik ma is az információgyűjtéstől és feldolgozástól kezdve a szoftverrel támogatott külügyi döntéshozatalig sok területen. És a nyersanyag, az adat szédítő tempóban növekszik tovább, a nap minden percében. Ami – ha figyelembe vesszük, hogy egyetlen év alatt mintegy 370 millióval nőtt az internethasználók száma – nem is meglepő. A mesterséges intelligencia tehát egyfelől eszközként kapcsolódik a külügyi szervezetekhez, mindenekelőtt (de, mint az esettanulmányokból látni fogjuk, nem kizárólagosan) a politika végrehajtásáért felelős diplomáciai szervezetekhez és működésekhez.[63]

A tájékozódás és tájékoztatás a diplomáciai munka alapvető funkciója volt és maradt. Jelentősége mindkét irányú információáramoltatásnak növekedett, noha természetesen – a közösségi platformokon zajló közdiplomácia népszerűségének szárnyalásával – elsősorban a tájékoztatás jut róla az eszünkbe. Az MI-projektek jó része ugyanakkor a diplomáciai információszerző, rendszerező, elemző, prezentáló munkát igyekszik új minőségi szintre emelni. Közben a tájékoztatáshoz kapcsolódóan is egyre több az MI-kezdeményezés, elsősorban az álhírprobléma kezelésére.[64]

Az adattudomány, a mesterséges intelligencia, a különféle modellezések alkalmazásának érdekes példáját adja a brit külügyi szervezet fejlesztése. Az általuk kialakított MI-alapú informatikai eszközrendszer több százezer, különböző nyelvű információs forrást képes automatikusan figyelni, angolra fordítani és valós időben megjeleníteni egy központi felhasználói felületen. Korábban a diplomatáknak rengeteg időt kellett fordítaniuk a helyi hírforrások olvasására. Most az így szerzett információkat az online források tömegéből beszerezhető értesülésekkel lehet számottevően kiegészíteni. A „gyorsreagálású" külügyi csoportok (például válságok idején) rövid határidő alatt készülhetnek fel olyan információtömegből, amelynek megszerzésére korábban egyszerűen nem volt

[63] A mesterséges intelligencia külügyi, diplomáciai alkalmazásaiban rejlő lehetőségeket és kihívásokat a digitális diplomácia egyik legfigyelemreméltóbb európai kutatóműhelye, a genfi székhelyű DiploFoundation tanulmányozza önálló programként immár két éve. *Mapping the Challenges and Opportunities of Artificial Intelligence for the Conduct of Diplomacy.* 2019.

[64] A tájékoztatási funkcióhoz kapcsolódó MI-alapú alkalmazásra példának lásd a Brit Külügyminisztérium Nyílt Forrású Osztályát (OUSU). Hasonlóan jó bepillantást enged a legújabb adatalapú külügyi fejlesztések irányába a Svéd Intézet közösségi média hírszerző funkciója.

lehetőség. Az adatok hasznosulásához azonban nélkülözhetetlen az is, hogy azokat a maguk „emberi kontextusába" helyezzék. Ezért foglalkoztatnak viselkedéstudományban járatos szakembereket is. Az ő feladatuk, hogy felfedezzék az adatokból kirajzolódó tendenciákat, rámutassanak a mögöttük megbúvó emberi viselkedésekre. A csoport egyik fontos profilja ugyanis az „extrém megnyilvánulások" figyelése.[65]

A konzuli feladatok, a külügyi szervezet par excellence igazgatási típusú feladatai zömében nem egyedi, típusproblémák kezelését igénylik, viszont sokszor rövid határidővel, és néha jelentős távolságokból is. A konzuli ügyintézés éppen ezért ideális terepet kínál az egyszerű „gyenge MI"-technológiák alkalmazására, a hatékonyság számottevő növelése érdekében. A legjellemzőbb és ma már széles körben elterjedt ilyen MI-technológiákra támaszkodó alkalmazások a konzuli tevékenységhez kapcsolódó chatbotok. A konzuli beszélgetőrobotok elsősorban utazással kapcsolatban segítik az ügyfelet, másrészt a tipikusan külföldön előforduló vészhelyzetekkel kapcsolatban biztosítanak gyors, hatékony tájékoztatást – ráadásul a nap minden szakában.[66]

A diplomáciai szervezetek működésének – ahogy a diplomata munkának is – máig egyik legfontosabb, meghatározó feladata, funkciója maradt a nemzetközi (két- vagy többoldalú) tárgyalások folytatása. E már-már művészetnek számító munkafolyamat technológiai támogatására fejlesztették ki a „Debatör" projektet, amelynek algoritmusa beszélgető interfészen keresztül vitába képes szállni emberi partnerekkel. A fejlesztés mögött álló izraeli külügyi szakemberek a diplomácia máig legfontosabb funkciója, a tárgyalások támogatásának új eszközét remélik ettől a speciális MI-fejlesztéstől.[67]

A kereskedelmi attaséi hálózatokkal, illetve a külképviseletektől sokszor elkülönülve működő, de azok általános irányítása alatt maradó kereskedelmi képviseletekkel kapcsolatos megnövekedett elvárásoknak azonban az emberi és tárgyi erőforrásokban többnyire szűkölködő szervezetek mind nehezebben képesek megfelelni. Nem véletlen, hogy a diplomáciai tevékenység e speciális szekciójában is nagy reményeket fűznek az IKT-technológiák, és specifikusan az MI-fejlesztésekben rejlő „erősokszorozó" lehetőségekhez. Erre példa

[65] Nyáry (2020): i. m. 11., továbbá *Exclusive: Meet the UK's „Data Diplomat"* (é. n.).
[66] Nyáry (2020): i. m. 9.
[67] Nyáry (2020): i. m. 12., továbbá *Inside Project Debater Speech by Crowd* (é. n.).

a Portugál Külügyminisztérium égisze alatt kifejlesztett „Portugal Exporta" portál, számos MI-vel támogatott funkcióval segítve az ország külkereskedelmét.[68]

Utoljára hagytuk az MI-technológiákra támaszkodó „diplomáciai" fejlesztések legérdekesebbikét. Merthogy nem a külpolitika végrehajtásáért felelős diplomáciához (tehát a taktikai szinthez) kapcsolódik, hanem magához a nemzeti külpolitika formálásához, a külügyi stratégiaalkotáshoz. A Kínai Tudományos Akadémia által fejlesztett, MI-alapú külpolitikai döntéstámogató rendszer korai változatát már használja is a feltörekvő ázsiai nagyhatalom külügyi apparátusa. A szoftver óriási adattömeget elemez, a diplomáciai koktélpartik pletykáitól a nemzetbiztonsági stratégiákig. Ha a külpolitika alakítói egy komplex helyzeten belüli konkrét külkapcsolati cél eléréséhez szükséges döntéseket latolgatják, akkor a szoftver villámgyorsan több, nagyon pontos döntési alternatívát rajzol fel nekik.[69]

Kiberdiplomácia az MI nemzetközi szabályozásában

A mesterséges intelligencia ugyanakkor a diplomáciai tevékenységek új tematerületeként is jelentkezik. Azaz: nemcsak a mesterségesintelligencia-technológia segíti a diplomácia működését, de a diplomácia is támogatja működésével a mesterséges intelligencia térhódítását. Láttuk, hogy ennek az új technológiának mekkora jelentőséget tulajdonítanak a modern geopolitikai kapcsolatrendszerekben. Nem meglepő, hogy a mesterséges intelligencia, annak technológiai, alkalmazási, személyes adatvédelmi, sőt etikai vonatkozásai erősen foglalkoztatják a nemzetközi közvéleményt. Ebből következően az ezeknek a – sok szempontból újszerű, analógiák és megszokott fogódzkodók nélküli – helyzeteknek a kezelésére szolgáló nemzetközi szabályozások kidolgozására növekszik az igény. Már most látható, hogy az MI-tématerület a diplomácia, és ezen belül is az úgynevezett multilaterális kapcsolatok egyik legfontosabbjaként kezd szerepelni. Ezen a területen különösen aktív az Európai Unió, de az ENSZ is fontos kezdeményezésekkel, célzott munkacsoportokkal és más nemzetközi fórumokkal törekszik e nagy hatású geopolitikai vonatkozású technológia nemzetközi szabályrendszerének kidolgozására.

[68] Nyáry (2020): i. m. 37.
[69] Nyáry (2020): i. m. 37.

A mesterségesintelligencia-kutatások, fejlesztések és alkalmazások körülményeinek átfogó szabályozása minden kétséget kizárólag ma az egyik legégetőbb feladat. A technológiában rejlő elképesztő potenciálok, és így a várható fejlődés üteme és kiterjedése nélkülözhetetlenné teszi a szabályrendszerek kidolgozását. Éppen ezért az elkövetkező időszakban vélhetően ez a tématerület áll majd a kiberdiplomaták figyelmének fókuszában. Ugyanakkor a mesterséges intelligencia szabályozására, illetve a kapcsolódó szakpolitikákra vonatkozó nemzetközi jogi környezet még maga is csupán kialakulóban van.

Az MI-szabályozás részben a technikai, részben a gazdasági, részben pedig a társadalmi alkalmazási (etikai) aspektusokra fókuszál. Maga a jogi szabálykörnyezet kialakítása jelenleg az alábbi fő témákkal foglalkozik elsősorban: autonóm intelligens rendszerek, az MI-rendszerek felelőssége és számonkérhetősége, valamint a személyiségi jogi és biztonságossági kérdések.[70] A szabályozás nemzetközi kereteinek megteremtése a 2010-es évtized második felétől került a multilaterális fórumok érdeklődési körébe. 2018-ban közös kanadai–francia kezdeményezésre merült fel az elképzelés, hogy (a klímaváltozással foglalkozó nemzetközi panel példájára) a G7-es csoport égisze alatt induljon el egy Mesterséges Intelligencia Nemzetközi Panel az új technológiai fejlesztési terület lehetséges globális kihatásainak tanulmányozására. 2019 tavaszán elfogadták az OECD *Mesterséges intelligencia ajánlásait*, majd néhány hónapra rá a G20-as csoport *Mesterséges intelligencia alapelvet*. Még szintén 2019-ben a Világgazdasági Fórum is kibocsátott egy útmutatót a kormányzati MI-beszerzések támogatására.[71]

A világ vezető multilaterális tömörüléseihez hasonlóan az EU is a mesterségesintelligencia-szabályozás előmozdítása mellett kötelezte el magát az évtized utolsó éveiben. 2018 nyarán a Bizottság független Magas Szintű Szakértői Csoportot állított fel a mesterséges intelligencia kérdéseinek – elsősorban a technológia megbízhatóságának – tanulmányozására.[72] Az MI-szabályozás témájában mérföldkőnek tekinthető 2020 februárja, amikor az EU Bizottság publikálta a *Mesterséges intelligencia fehér könyvét*.[73] A dokumentum azonosította

[70] Tom Wheeler: *History's Message about Regulating AI*. 2019.

[71] *France and Canada Create New Expert International Panel on Artificial Intelligence* (2018) és *OECD Principles on AI* (2019), valamint *G20 Human-Centered AI Principles* (2019), továbbá *World Economic Forum AI Government Procurement Guidelines* (2019).

[72] Buddle Findlay: *Artificial Intelligence and the Regulatory Landscape*. 2020.

[73] *White Paper on Artificial Intelligence. A European Approach to Excellence and Trust.* 2020.

a mesterségesintelligencia-fejlesztések és -alkalmazások kapcsán felmerülő legfontosabb kockázati tényezőket: az alapvető jogok sérülhetősége, az adatokhoz fűződő személyiségi jogok sérülhetősége, a biztonsággal és a hatékony működéssel kapcsolatos problémák, valamint a felelősségrevonhatóság kérdése. A Bizottság úgy határozott, hogy a fejlesztéseknek ebben a relatíve korai fázisában nem bocsát még ki részletes szabályozást a témában, hanem csupán felvázolt egy jogi követelményrendszert, amely értelmében minden jövőbeli keretszabályozásnak garantálnia kell az MI-rendszerek megbízhatóságát, illetve azt, hogy tiszteletben tartják az Európai Unió alapvető elveit és értékeit. A követelményrendszer kitér arra is, hogy a hatályos EU-jog alkalmazandó – technikai tisztázásokat követően – az MI-kérdésekre is.

Kitekintés

A kibertér geoökonómiáját, kiberdiplomáciai témáit és kihívásait és szabályozási törekvéseit bemutatni szándékozó áttekintésünket a nemzetközi szabályozási törekvések ellentmondásaival és ellentéteivel, majd a digitális gazdaságot a várakozások szerint gyökerestül felforgatni készülő mesterséges intelligencia témáival zártuk. Nem haszontalan, ha most zárszóként egy pillanatra mondandónk első részeihez kanyarodunk vissza, oda, ahol az újra megjelenő, majd mind jobban élesedő geoökonómiai szembenállások rendszeréről szóltunk. Esetleg azért is, hogy a két végpontot most mintegy egybeöltsük. A kibertér egyre inkább a hatalom meghatározó dimenziója.[74] És, ha lettek volna illúzióink, akkor most már kristálytisztán láthatjuk: a gazdaság (a termeléssel és ellátási láncokkal, nemzetközi kereskedelemmel és technológiával) jórészt nemzetbiztonság is – hatalom. Kibertér és digitális gazdaság: egymásba fonódó hatalmi dimenziók tehát. Az egyik jeles kiberszakmai szervezet, az Internet Governance közelmúltban megjelent írása arra figyelmeztet: az Egyesült Államok és Kína között a tavalyi évben elmélyülő, majd mostanra végképp elmérgesedő kereskedelmi háború ma már egyértelműen technológiai konfrontációt takar. A tét nem egy-egy jól jövedelmező fejlesztés vagy versenyelőny, hanem a globális hegemóniában kulcsszerepet kapó kibertér, a geopolitika 5. dimenziójának uralása. Azé a közegé, ahol hamarosan a mesterséges intelligenciával támogatott

[74] André Barrinha – Thomas Renard: Power and Diplomacy in the Post-Liberal Cyberspace. *International Affairs,* 96. (2020), 3. 749–766. 756.

rendszerekre támaszkodva igyekszik majd operálni a támadó és a védekező fél egyaránt. Sokan úgy tartják: ez (is) egy olyan terület, ahol a rendet, biztonságot megőrizni akarók vannak hátrányban. A gépi tanulás ugyanis ma már olyan gyorsan képes megkerülni, lebontani a kibervédelmi rendszereket, amellyel a szokványos védelmi eszközök nem tudnak lépést tartani. A gépi tanulást persze a kibervédelemért felelős szakemberek is csatasorba állítják. Az MI segítségével a fenyegetést jelentő online viselkedési mintákat igyekeznek felderíteni. És, miközben a kiberharcosok a hálózatos térben keresik a megfelelő fegyvert, addig ugyanott keresik a rendezés lehetőségeit mások is. A ma már egyre gyakrabban csak fejlett technológiájú „új hidegháborúként" emlegetett szembenállás ugyanis ösztönzi a kibertér békés rendezésén, kollektív szabályozásán munkálkodó szakembereket, a kiberdiplomatákat is.

Felhasznált irodalom

Ayers, Cynthia: *Rethinking Sovereignty in the Context of Cyberspace*. Carlisle, US Army War College, 2015.

Barrinha, André – Thomas Renard: Power and Diplomacy in the Post-Liberal Cyberspace. *International Affairs,* 96. (2020), 3. 749–766.

Brangetto, Pascal – Mari Kert-Saint Aubyn: *Economic Aspects of National Cyber Security Strategies. Project Report.* Tallin, CCDCOE, 2015.

Brzezinski, Zbigniew: *A nagy sakktábla*. Budapest, Európa, 1999.

Buchan, Russell: *Cyber Espionage and International Law.* Oxford, Hart, 2019.

Charalabidis, Yannis: *The World of Open Data. Concepts, Tools and Experiences*. Cham, Springer Nature, 2018.

Covid-19 Cybercrime Weekly Update. 2020. Online: www.riskiq.com/blog/analyst/covid19-cybercrime-update/.

Custers, Bart et al.: *EU Personal Data Protection in Policy and Practice*. Berlin, Springer, 2019.

Data Governance. Part I. Emerging Data Governance Practices. 2020. Online: https://foreignpolicy.com/2020/05/13/data-governance-privacy-internet-regulation-localization-global-technology-power-map/?utm_source=PostU.

D' Elia, Danilo: La Guerre économique a l'Ére du Cyberspace. *Hérodote,* (152–153. (2014), 1–2. 240–260.

Dee, Megan: *The European Union in a Multipolar World. World Trade, Global Governance and the Case of the WTO*. London, Palgrave MacMillan, 2015.

Demchak, Chris – Peter Dombrowski: Cyber Westphalia: Asserting State Prerogatives in Cyberspace. *Georgetown Journal of International Relations,* (2013–2014). 29–38.

Digital Watch Newsletter. 2020. Issue 50, May 2020.

Dominioni, Samuele: *Digital Economic Powers and Digital Political Rulers*. 2019. október 17. Online: www.ispionline.it/en/pubblicazione/digital-economic-powers-and-digital-political-rulers-24187.

DuPont, Sam: *An Open Alliance for Digital Trade*. 2020. Online: www.csis.org/analysis/open-alliance-digital-trade?utm_source=Members&utm_campaign=aba-3460b2a-EMAIL_CAMPAIGN_2020_01_29_04_21_COPY_01&utm_medium=email&utm_term=0_e842221dc2-aba3460b2a-221725217.

Exclusive: Meet the UK's „Data Diplomat" (é. n.). Online: https://govinsider.asia/innovation/uk-foreign-office-open-source-unit-data-diplomat-graham-nelson/.

FBI–CSISA PSA PRC targeting of COVID-19 research organizations (2020). Online: www.cisa.gov/publication/fbi-cisa-psa-prc-targeting-covid-19-research-organizations.

Filippov, Vladimir M. – Alexander A. Chursin – Julia V. Ragulina – Elena G. Popkova: *The Cyber Economy. Opportunities and Challenges for Artificial Intelligence in the Digital Workplace.* Cham, Springer Nature, 2019.

Findlay, Buddle: *Artificial Intelligence and the Regulatory Landscape.* 2020. Online: www.lexology.com/library/detail.aspx?g=4c845762-e954-4f47-8809-f5ad0f5d3716.

France and Canada create new expert International Panel on Artificial Intelligence (2018). Online: www.gouvernement.fr/en/france-and-canada-create-new-expert-international-panel-on-artificial-intelligence.

Futó Iván: *Mesterséges intelligencia*. Budapest, Aula, 1999.

G20 Human-Centered AI Principles (2019). Online: www.mofa.go.jp/files/000486596.pdf.

Gady, Franz-Stefan: *Interview: Robert Ward and Yuka Koshino on Geo-Economics in East Asia*. 2020. Online: https://thediplomat.com/2020/04/interview-robert-ward-and-yuka-koshino-on-geo-economics-in-east-asia/.

Gill, Indermit: *Whoever Leads in Artificial Intelligence in 2030 Will Rule the World until 2100.* 2020. Online: www.brookings.edu/blog/future-development/2020/01/17/whoever-leads-in-artificial-intelligence-in-2030-will-rule-the-world-until-2100/?fbclid=IwAR3UJSDfUG4aFGXpHRDdch76HQu9ZgDIOQXGZo-2t8iVjn-0HIQPNPnD42MM.

Hakmeh, Joyce: *Cybercrime and the Digital Economy in the GCC Countries*. London, Chatham House, 2017.

Huang, Keman et al.: *Interactions between Cybersecurity and International Trade: A Systematic Framework.* Cambridge, MIT Sloan, 2018.

Inside Project Debater Speech by Crowd (2019). Online: www.linkedin.com/pulse/inside-project-debater-speech-crowd-ibms-effort-extend-rodriguez

International Trade Regulation and Cybersecurity (é. n.). Online: www.hoganlovells.com/en/publications/international-trade-regulation-and-cybersecurity.

Jacobson, Barbara Roseb – Katharina E. Höhne – Jovan Kurbalija: *Data Diplomacy.* Genf, DiploFoundation, 2018.

Jayawardane, Sash: *Cyber Governance: Challenges, Solutions and Lessons for Effective Global Governance.* The Hague, The Hague Institute for Global Justice, 2015.

Luttwak, Edward: From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce. *The National Interest,* (1990), 20. 17–23.

Mapping the Challenges and Opportunities of Artificial Intelligence for the Conduct of Diplomacy. Geneva, DiploFoundation, 2019.

Measuring the Digital Economy. Washington, International Monetary Fund, 2018.

Meltzer, Joshua: *Cybersecurity, Digital Trade, and Data Flows. Re-Thinking a Role for International Trade Rules.* 2019. Online: www.brookings.edu/research/cybersecurity-digital-trade-and-data-flows-re-thinking-role-for-international-trade-rules/.

Meyer, David: Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World. *Fortune,* 2017. szeptember 4. Online: https://fortune.com/2017/09/04/ai-artificial-intelligence-putin-rule-world./

Moisio, Sami: Re-Thinking Geoeconomics: Towards a Political Geography of Economic Geographies. *Geography Compass,* 13. (2019), 10. 1–13.

Nyáry Gábor: Kiber geopolitika. Mesterséges intelligencia alkalmazások az államigazgatás külpolitikai alrendszereiben. *Új Magyar Közigazgatás,* 13. (2020), 1. 32–39.

OECD Principles on AI (2019). Online: www.oecd.org/going-digital/ai/principles/.

Open Data: Unlocking Innovation and Performance with Liquid Information. McKinsey Global Institute Report (2013). Online: www.mckinsey.com/business-functions/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information.

Open Government Data Report. Paris, OECD, 2018.

Pintér István (szerk.): *Műhelymunkák. A virtuális tér geopolitikája. 2016/1.* Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016.

Riordan, Shaun: *Cyberdiplomacy. Managing Security and Governance Online.* Cambridge, Polity Press, 2019.

Rohaidi, Nurtilzah: *Exclusive: Meet the World's first Tech Ambassador.* 2017. Online: https://govinsider.asia/innovation/danish-tech-ambassador-casper-klynge/.

Scesanto, Stefan: *Europe's Digital Power: From Geo-Economics to Cybesrsecurity.* London, European Council on Foreign Relations, 2017.

Shen, Yi: Cyber Sovereignty and the Governance of Global Space. *Chinese Political Science Review,* (2016), 1. 81–93.

Sherman, Justin: *How Much Cyber Sovereignty Is Too Much Cyber Sovereignty?* 2017. Online: www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty.

Sherman, Justin: *To Preserve a Global and Open Internet, We Need to Invest in Cyber Diplomacy*. 2018. Online: www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/preserve-global-and-open-internet-we-need-invest-cyber-diplomacy/.

Significant Cyber Incidents (2020). Online: www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

Stadnik Ilona: What is an International Cyber Regime and How We Can Achieve It? *Masaryk University Journal of Law and Technology,* 11. (2017), 1. 129–154.

Taulli, Tom: *Artificial Intelligence Basics. A Non-Technical Introduction*. Monrovia, Apress, 2019.

Teoh, Chooi Shi – Ahmad Kamil Mahmood: National Cyber Security Strategies for Digital Economy. *Journal of Theoretical and Applied Information Technology,* 95. (2017), 23. 6510–6522.

The World's First Ambassador to the Tech Industry (2019). Online: www.nytimes.com/2019/09/03/technology/denmark-tech-ambassador.html.

Vicente, Dário Moura – Sofia de Vasconcelos Casimiro: *Data Protection in the Internet*. Cham, Springer Nature, 2020.

Wheeler, Tom: *History's Message about Regulating AI.* 2019. Online: www.brookings.edu/research/historys-message-about-regulating-ai.

White Paper on Artificial Intelligence. A European Approach to Excellence and Trust. Brussels, European Commission, 2020.

Wigell, Mihael et al. (szerk.): *Geo-economics and Power Politics in the 21st Century.* London, Routledge, 2019.

World Economic Forum AI Government Procurement Guidelines (2019). Online: www.weforum.org/whitepapers/ai-government-procurement-guidelines.

Yahoo Says All Three Billion Accounts Hacked in 2013 Data Theft (2017). Online: www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1.

Kötetünk betekintést nyújt a kiberdiplomácia alapjaiba: rávilágít az olyan alapvető, a kérdéskör megértéséhez elengedhetetlenül szükséges fogalmak közötti különbségekre, mint a kiberdiplomácia, a digitális diplomácia vagy az e-diplomácia; elemzi az Európai Unió kiberdiplomáciai lépéseinek elméleti hátterét, és felfedi az egyes uniós lépések mögötti mozgatórugókat is. Az olvasó részletesen megismerkedhet a három nagyhatalom kiberpolitikájának alapjaival, valamint a három vezető európai állam utóbbi években elért kiberdiplomáciai eredményeivel. A kötet kitér a külgazdasági kapcsolatok kiberdiplomáciai vonatkozásaira, valamint olyan új típusú problémákat is felvillant, amelyek az adatbiztonsággal vagy a mesterséges intelligenciával kapcsolatosak.

Hasznos olvasmány lehet nemcsak a területen jártas és a kiberbiztonság iránt érdeklődő szakközönség számára, hanem mindenkinek, aki a világ problémáit és a mögöttes mozgatórugókat szeretné megérteni, különösen ebben az új, ötödik geopolitikai dimenzióban.

9 789635 316496