

Nyáry Gábor

Kiberdiplomácia: hatalom, politika és technológia a geopolitika ötödik dimenziójában

Bevezetés¹

Kiberháború, kiberbűnözés, kiberelrettetés: 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 közkedvelté és agyonhasználttá vált, mint a „kibertér” a technikai, informatikai szakbeszédben. Ez a „geopolitika”. Képlékeny, de valahogy mindenki által „érezett” 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.

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 kiberdiplomataé. Mert az egyik legfontosabb mondandónk az lenne, hogy a világháló szövevényes útjait, dróttjait, 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 hegemonia 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 sakktabla*. 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 (benn a népesség nagysága és demográfiai mozgásai).⁷ Érdeemes 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 diszkrétan 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 esztendő, 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 alapon – 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”-ról¹⁰ meglepetést (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 multilaterális elveire építő európai közösség vezető tisztviselőjétől (ráadásul éppen egy német politikus szájából¹²) egyenesen istenkáromlásnak hathatott. A politikus (aki egészen pontosan „geopolitikus Európai Bizottságot” ígért beiktatásakor) láthatóan új, dinamikusabb szerepet szánt a sokak által nehezen mozgó, erőltetett 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 vesztésként 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 legkiméletlenebb 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 mellékük 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 népszerűsége 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 Vassily 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 összefüggérendszerében, 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, képlekeny 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 lehamozni. 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 rögzülteitől, 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 hegemonként 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 eszközkápa 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) köteté.

²⁰ Alapos, rendszeres áttekintését adja a hatalmpolitikai átrendeződés folyamatának és következményeinek az Európai Parlament kutatószolgálatá 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 jellemeznék, 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) eszközeit. 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 Power 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 kibernyomozgatás.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 háttérében, 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 „hadszínternek” 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 valószínűsége („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 fejezettrészben 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 eszközkála) 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 kavarnak 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 divaticlusok 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 legelismeretebb szakértője, az Oxfordban tanító román tudós, Corneliu Bjola írásai megkerülhetetlenek a technicizáló 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-eszközrendszer mozgósítja 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 legtöbbit 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.: Cornelius 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 kutatóegységisége, 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 tájékoztódás),
- 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 köznap 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 diplomacy*-nak 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. Eppen 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 Practitioner'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 Twitterről 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 östípusát 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 kiberbiztonság kérdése is.

Szeretnénk hangsúlyozni: a „kiberdiplomácia” nem valami metafora csupán, hanem valóságos külkapcsolati terület és államközi interakciós terep. A kiberdiplomáciát valóságos diplomatak 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* (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 Berzsényi Dániel – Krasznay Csaba: *Nemzetközi kapcsolatok a kibertérben*. Budapest, Nemzeti Közszerológiai 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 kevésbé 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 dimenzióknak” 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 előrebecsátani a korábban már megismert, de fontos alapelveket: a kiberdomén valóságos globális „tér”. Olyan, ami egyszerre összeköti a nemzeteket, ugyanakkor természetesen a közöttük való sűrűlódásoknak is gyakori terepe. A kibertér 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 diplomataik 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 jellegükénél 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 csataterekkel összevetve – kevésbé vonzó alternatívát kínálnak 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 Csoportjainak⁵⁴ ülései 2010-től kezdve, amelyek azt tűzték ki célul, hogy a nemzetközi közösség összefogásával a kibertámadások fenyegetéseinek csökkentésére vonatkozó, illetve általános-ságban véve a felelősségteljes állami magatartás önkéntes normáit kidolgozzák a kibertér vonatkozásában. A csoport, aminek felállításáról egy jóval korábban Oroszország által beterjesztett javaslat⁵⁵ 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 siker-telenségéből (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 Endowment, 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 bekeverültek 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 kyberszereplővé 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 pilléreként.

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 rivális nagyhatalom 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 léptékkal 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 kereszttülszelő hatalmi hálókat. A hálómétafora 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, létrejötté 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 világhálóiig. 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 koncentrálnó 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 kiberdiplomataék. Ezeken a vidékeken, amelyek korábban az informatikusok, számítástechnikai mérnökök, hálózattudósok felségterületének számítottak, ma már egyre inkább a külkapcsolat-építés hivatásosai mozognak otthonosan. Szakdiplomataék – 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](http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)646148).
- Berzsenyi Dániel – Krasznay Csaba: *Nemzetközi kapcsolatok a kibertérben.* Budapest, Nemzeti Közszerológiai 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 sakktabla*. 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](http://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 Practitioner'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.

Kiberdiplomácia: hatalom, politika és technológia a geopolitika ötödik dimenziójában

„*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.