Nyáry Gábor – Ambrus Éva

A koronavírus-járvány hatása a nemzetközi kiberkapcsolatokra

A koronavírus-világjárvány egyik meghökkentő fejleménye a nagyhatalmak, hatalmi csoportosulások közötti konfrontáció(k) erősödése volt. Az átlagember, a maga civil mentalitásával, azt gondolhatta: amikor egy „neutrális", azaz mindent és mindenkit fenyegető veszedelem árnyéka borul az emberiségre, akkor az egyéb ellentétek – triviális torzsalkodások és halálosan komoly érdekellentétek egyaránt – egy pillanat alatt feledésbe merülnek. Nem hirtelen támadt barátság, hanem a mindenkit fenyegető veszély okán. A valóságban mi sem állt ennél távolabb. A multipolarizálódó világ ellentétjei, rivalizálásai nemhogy gyengültek volna, de szinte a végletekig felerősödtek az elmúlt hetekben, hónapokban. A járvány okozta rendkívüli helyzetben a felek nem a veszély, hanem az esély lehetőségét látták meg.

A nemzetközi kapcsolatokat kutató szakértők azon is elmerengtek, mennyiben tekinthető ez a hirtelen erővel előbukkant járvány egyfajta „fekete hattyú"-jelenségnek, tehát olyan, előre nem jelezhető, ugyanakkor súlyos következményekkel járó eseménynek, amely azonban utólag logikus fejleményként értelmezhető.[1] Az igazság azonban az, hogy a koronavírus-járvány „eljövetelére" bőségesen utaltak jelek: az elmúlt másfél évtizedben egymás után bukkantak fel olyan járványcsírák[2] (több esetben szintén koronavírusokhoz köthetők), amelyek potenciálisan egy globális pandémia lehetőségét hordozták magukban. Talán különösebb cinizmus nélkül állítható a múltbeli események ismeretében az is, hogy a válsághelyzetek, a normális életfolyamatok megszakadása és felforgatása gyakorta jelent erős kísértést a háttérben lappangó konfliktusok gyors „rendezésére". A Covid-19-időszak egyértelmű tapasztalata is az, hogy a meglévő, formálódó folyamatok kaptak új erőt és lendületet. Az elmúlt évek döntő mozzanata a globális erőtér átrendeződése volt, a hatalmi status quo megőrzéséért küzdők (nagyok és közepesek) és a hatalmi pozíciók újraosztásáért ringbe szálló feltörekvők (nagyok és közepesek) versengése és különösen a kibertér hangsúlyos küzdelmi mezővé válása. A geopolitikai erőtér – és ezen belül különösen a kibertér – átrendeződésének felgyorsulása, tehát a már korábban bontakozó hatalmi-politikai trendek dinamikus kibontakozása az, ami meghatározza a „járványos világ" összképét.

Fogalmi keretek

A kibertér nemzetközi viszonyainak leírásával kapcsolatban mély és sokrétű a „fogalmi sokszínűség". Még a szakmai társadalom sem egységes a legfontosabb, leg-

[1] A fogalmat Nassim Nicholas Taleb, a jeles libanoni–amerikai közgazdász vezette be és tette világszerte ismertté *Fekete hattyú – avagy a legváratlanabb hatás* című, 2007-ben megjelent könyvében.
[2] Például a SARS-vírus 2004-ben, majd a H1N1-vírus 2009-ben, és végül az ebolavírus 2015-ben.

https://doi.org/10.36250/00925_30

alapvetőbb kategóriák elnevezésében (ugyanakkor központivá váló jellegénél fogva ez a témakör egyre gyakrabban jelenik meg a médiában és a politikusi közbeszédben – tovább fokozva a fogalmi zűrzavart). Szisztematikus fogalmi háló megalkotására itt nem vállalkozhatunk, azonban a jelenségek megértéséhez elengedhetetlennek tartjuk legalább néhány kulcselem definíciószerű bemutatását.

Kibertér: a geopolitikai küzdelmek alapdimenziója

A földrajzi tér alapvető kiterjedései ősidőktől az államok közötti érdekérvényesítési küzdelmek állandó színterei. Melléjük a 20. század első harmadától felzárkózott a levegő, majd a hidegháború korszakában az űr dimenziója is. A 21. század újdonságaként bővült ki ez a sokrétű geopolitikai világ egy újabb versengési területtel. A formálódó kibertér lett a geopolitikai szembenállás, érdekérvényesítés ötödik dimenziója.[3] Az informatika, a számítógépes hálózatok, a 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. Összegezve egyfajta fogalmi keretként úgy tekinthetünk a kibertérre, mint az internet, a számítástechnikai eszközök, a rajtuk futó szoftverek, sőt az őket használó, mind inkább hálózatokba szerveződő alkalmazók összességére. Alapvető jellegzetessége, hogy kezdetben egy 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, mint a szárazföldek, a tengerek, a levegő vagy az űr. Sőt, ma már abban is egyre nagyobb a konszenzus, hogy a kibertér a nemzetek közötti érdekellentéteknek és érdekérvényesítésnek nem csupán az egyik dimenziója, hanem „a" meghatározó színtere.[4]

A kiberdiplomáciától a digitális diplomáciáig

Amennyire fontos leszögezni, hogy a kibertér messze nem azonos csupán számítógépes hálózatokkal, esetleg az azokat összekapcsoló világhálóval, éppen

[3] A kibertér geopolitikai jellegének egyik első megfogalmazását Szilágyi István kiváló munkája adja. Lásd Szilágyi István: *A geopolitika elmélete.* Budapest, Pallas Athéné, 2018.

[4] Alix Desforges: Representations of cyberspace: A Geopolitical tool. *Hérodote,* 152–153. (2014), 1–2. 67–81. A kibertér, a földrajz és a hatalmi politika modern kapcsolódási rendszereire az egyik vitathatatlanul legérdekesebb mostanában napvilágot látott munka Blount kötete. P. J. Blount: *Reprogramming the world. Cyberspace and the geography of global order.* Bristol, E-International Relations Publishing, 2019.

annyira fontos tisztázni azokat az operációs fogalmakat is, amelyekkel a kibertérben mozgó állami (és egyéb) szereplők érdekérvényesítési tevékenységei leírhatók. A kibertér viszonyaival kapcsolatban a leggyakrabban előbukkanó kifejezés a „kiberhadviselés", a „kiberbiztonság", és ez persze nem véletlen. Az államok ugyanis ebben a speciális dimenzióban, az úgynevezett kibertérben is gyakran alkalmazzák az érdekeik érvényesítésére rendelkezésre álló *egyik* eszközkészletet: az erőszakot. A hangsúly itt most azon van, hogy ez az *egyik* lehetséges eszközrendszer. A paletta másik végén egy *másik,* szintén jól ismert eszközt találunk: ez a diplomácia, amely sajátos funkciókkal és egyedi eljárásokkal rendelkező tevékenység. A hadviseléstől jócskán elütő eszközkészletét jellemzően a tárgyalás és a megegyezés alkotja. A kibertér, mint geopolitikai struktúra, vonatkozásában pedig sajátos válfaja, a kiberdiplomácia kap egyre inkább teret. 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. Ha ennek a speciális tevékenységnek a tartalmát tekintjük, akkor úgy fogalmazhatunk: ezek valójában a kibertérre, az online jelenségekre, a nagy globális technológiai cégekre vonatkozó nemzetközi szabályozó és irányító cselekvésekkel kapcsolatos, államok közötti (diplomáciai) tevékenységek.

Gyakorta bukkan fel ugyanakkor a digitális diplomácia fogalma is. Beszélnünk kell róla, mert nem intézhető el egyszerűen azzal, hogy csupán (egy sokszor pontatlanul, sőt pongyolán) használt szinonimával állunk szemben. A kifejezés használata indokolt, de látni kell a kifejezések közötti jelentésbeli különbségeket. A digitális diplomácia nem más, mint a diplomácia hagyományos folyamatainak gyökeres („transzformatív") átalakítása az IKT-technológiák következtében. Tulajdonképpen tehát „az érem másik oldala".[5] Leggyakrabban a korszerű infokommunikációs technológiákat (elsősorban a közösségi média platformokat) intenzíven használatba állító „kétoldalú diplomáciai párbeszéd" képében jelenik meg. Ugyanakkor a digitális diplomácia területén különösen jellemző az aktorok és a tevékenységgel lefedett területek körének rohamos bővülése: míg a nemzetközi kapcsolatok hagyományos alanyaiként és cselekvőiként politikai entitásokat (elsősorban szuverén államokat, nemzetközi államközi szervezeteket) szokás tekinteni, a digitális nyilvános diplomácia működtetőinek a köre jóval szélesebb, társadalmiasabb.

A globális járványidőszak nemzetközi kiberkapcsolatainak rendszerében – mint látni fogjuk – kirobbanó aktivitás jellemzi mindkét tevékenységet: a kiberdiplomáciát és a digitális diplomáciát egyaránt.

[5] A kiberdipolmácia esetében tehát a „kiber" a diplomaták működésének tárgya. A digitális diplomácia esetében viszont a „kiber" a diplomáciai működés megváltozott (digitalizálódó) eszközrendszere.

A vihar előszele

A téma általános bevezetőjében már igyekeztük hangsúlyozni: a koronavírus-világjárvány által előidézett helyzet – a nemzetközi kapcsolatok, következésképpen a nemzetközi kiberkapcsolatok terén – a pandémia diszruptív jellege ellenére nem generált merőben új folyamatokat. Ami ugyanakkor szembeötlő, az a korábbi időszakban kibontakozó geopolitikai mozgások jelentős, sok tekintetben drámai felgyorsulása.

Geopolitikai mozgások a kibertérben – az USA és Kína

A 2010-es évtized egyértelmű fejleménye a rendszerváltásokat követő Amerika-központú, unilaterális világrend felbomlása. A tudósok és politikai szakértők egyre gyakrabban említik az így kialakulóban lévő szisztémát egyfajta multipoláris világrendként.[6] 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.[7] 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 „megvalósításieszköz-skála mentén" több különálló, de egységes rendszerbe kapcsolódó és egyre gyakrabban formálisan is jórészt összemosódó eszközt használ a valós (vagy annak vélt) nemzeti érdekek külvilágbéli érvényesítésére. A lehetőségek tárházából még ma is gyakorta veszik elő az államok a háború (pontosabban 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

[6] Alapos, rendszeres áttekintését adja a hatalompolitikai átrendeződés folyamatának és következményeinek az Európai Parlament kutatószolgálata által kiadott mű: European Parliament: *Global Trends to 2035. Geo-politics and international power.* (2017. 09. 20.) Hasonlóan jó összefoglalót ad Megan Dee is. Megan Dee: *The European Union in a multipolar world. World trade, global governance and the case of the WTO*. London, Palgrave MacMillan, 2015.

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

érdekérvényesítés helyébe az erőszak új – fegyvertelen, de semmiképpen sem „békés" – eszközei lépnek.[8] 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 és rendszerek kifejlesztése, telepítése és alkalmazása mellett.[9] 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,[10] később mindkét hatalom támadó eszközökkel is felszerelt kiberarzenállal operál a nemzetközi kibertérben.[11] 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 stratégiakülönbségek a kapacitások kiépítésében is éreztették a hatásukat: míg Kína kezdettől egységes 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.[12] A kibertérben zajló katonai akciókról – azok jellegénél fogva – kevés megbízható információ lelhető fel a szabadon hozzáférhető (nyílt) irodalomban. Érdekességként megemlíthetjük, hogy a kibertérben való hadviselési műveletek jóval régebbiek, mint azt gondolhatnánk: az első (nyilvánosságra került) ilyen akció a hidegháború időszakába vezet vissza,

[8] A téma, a nemzetközi kapcsolatok, illetve a külpolitika és a kibertér erősödő összefonódásának különösen jó áttekintését adja: Nazil Choucri: *Cyberpolitics in international relations.* Cambridge (US-MA), MIT Press, 2012.

[9] 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 Kiber Stratégiával) lásd US DoD: *Department of Defense Cyber Strategy 2018*.

[10] Francis C. Domingo: Conquering a new domain: Explaining great power competition in cyberspace. *Comparative Strategy,* 35. (2016), 2. 154–168.

[11] Az amerikai kiberstratégiában is (annak radikális átszabása nyomán) megjelent az infrastruktúravédelem prioritása mellett a kibertérben biztosítandó katonai erőfölény megszerzésének célja.

[12] 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, az US Cyber Command (USCYBERCOM) felállításával érte el a kínaiakéhoz hasonló integrált vezetési és irányítási szervezetet.

a szovjet transzszibériai gázvezeték vezérlő rendszerei elleni kiberműveletig.[13] 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 a sérülékenységeit. Erre utaltak a 2010-es évtizedben sűrűsödő kínai támadások amerikai kormányzati rendszerek ellen, amikor a cél többnyire érzékeny információk megszerzése volt.[14]

Az államok közötti kiberkonfliktusok (incidensek) egyébként 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. Végül a kibertámadások célja lehet az ellenfél információs környezetének megzavarása, manipulálása.[15]

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 a 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.[16]

[13] Az akcióra 1982-ben került sor, és állítólag a CIA állt a hadművelet hátterében, amely egy digitális kártevővel fertőzött szoftver révén tette tönkre a rendszer vezérlését. A beavatkozás egyébként kinetikus hatásokkal járt, kolosszális méretű gázrobbanást idézve elő. Christopher Whyte – Brian Mazanec: *Understanding cyber warfare: Politics, policy and strategy*. New York, Routledge, 2019.

[14] 2003 és 2012 között legalább hat jelentősebb – amerikai kormányzati célpontok elleni – támadást írnak a Kínai Népköztársaság számlájára, amelyből 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 a titkos információk megszerzése volt. Domingo (2016): i. m. 162.

[15] Whyte–Mazanec (2019): i. m. 100.

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

Trendek és elmozdulások – Európa a kibertérben

Az átrendeződő világ két nagy hegemónja/potenciális hegemónja mellett korai volna még leírni a sok szempontból perifériára szorult EU-t. Az elmúlt években a közösség jól látható erőfeszítéseket tett az EU kiberdiplomáciai eszköztárának kialakítása érdekében.

Az EU nemzetközi kiberelkötelezettségét, ideértve a rosszindulatú tevékenységekre adott válaszát, az EU közös kül- és biztonságpolitikája (KKBP), valamint a közös biztonság- és védelempolitika (KBVP) keretében hajtják végre. Az EU 2015. évi, a kiberdiplomáciáról szóló tanácsi következtetéseiben leírja, hogy „koherens nemzetközi kibertér-politikára van szükség, amely előmozdítja az EU politikai, gazdasági és stratégiai érdekeit".[17] Összességében a következtetések egy értékalapú uniós megközelítést vázolnak fel – az emberi jogok védelmétől és a nemek közötti egyenlőségtől a véleménynyilvánítás szabadságáig. A következtetések rávilágítanak azokra a nehézségekre is, amelyeket részben az egymással nem koordináló nemzetközi fórumok okoznak a témában.

2017 októberében az EU tagállamai kiberdiplomácia eszköztárat[18] fogadtak el, amelynek a legfontosabb célja az iránymutatások kidolgozása minden szinten:

1. megelőző intézkedések – például bizalom- és kapacitásépítés;
2. együttműködési intézkedések – például politikai és tematikus párbeszédek;
3. stabilitási intézkedések – az EU hivatalos nyilatkozatai, a Tanács következtetései, diplomáciai kötelezettségvállalások a nemzetközi fórumokon;
4. korlátozó intézkedések (szankciók) – utazási tilalmak, embargók, vagyoni eszközök befagyasztása;
5. a tagállamok jogszerű válaszaihoz nyújtott uniós támogatás, ideértve az EU kölcsönös segítségnyújtási záradékának, az EUSZ 42. cikk (7) bekezdésének és a szolidaritási záradéknak az EUMSZ 222. cikkét.

A hatékony nyilvános üzenetküldés azt is jelenti, hogy komolyan kell venni a támadások attribúcióját, ahogyan az Európai Bizottság nemrégiben tette a Covid-19-cel kapcsolatos kínai dezinformáció kapcsán, ezzel nyomást gyakorolva Kínára.[19]

A dokumentum utal továbbá a „megosztott helyzettudatosság" szükségességére, amely lehetővé teszi a számítógépes fenyegetésekkel kapcsolatos állandó információcserét és az összes érintett EU- és nemzeti testület közötti koordinációt. A „megosztott helyzettudatosság" kialakítása kulcsfontosságú, a kiberműveletek szempontjából egyik legérzékenyebb aspektusa a hozzárendelés (attribúció) kérdése. Noha az EU eszköztára természetesen hangsúlyozza, hogy minden

[17] European Council: *Council Conclusions on Cyber Diplomacy (6122/15).* (2015. február 11.), 2.

[18] European Council: *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities (13007/17).* (2017. október 9.), 5.

[19] Lauren Speranza: China is NATO's new problem. *Foreignpolicy.com,* 2020. július 8.

tagállam szabadon hozhat szuverén politikai döntést a támadó számítógépes tevékenységekkel kapcsolatban, ugyanakkor megjegyzi, hogy a közös uniós válasz hatékonyságához kollektív értékelésre és fellépésre van szükség. Egyes elemzők[20] az EU kiberdiplomáciáját úgy értelmezték, hogy „a béke erejeként" pozicionálja magát.

Az EU kiberdiplomáciai céljainak közvetlen hozzájárulója az EU CyberDirect-projekt.[21] A projekt célja a párbeszéd elősegítése az EU stratégiai partnereivel. Arra is törekszik, hogy olyan platformmá váljon, ahol a kormányzati és nem kormányzati szereplők megvitatják a kibernormákat, a felelős kibermagatartást és a bizalomépítő intézkedéseket. Az EU kiberdiplomáciai tevékenysége globális is: a CyberEast[22] és az EU4Digital[23] a keleti partnerség országaival – Ukrajnával, Moldovával, Fehéroroszországgal, Georgiával, Örményországgal és Azerbajdzsánnal – folytatott konkrét együttműködés példái. Nyugat-Afrikában az OCWAR-C-projekt[24] célja a regionális kiberbiztonság fokozása, Délkelet-Ázsiában pedig a YAKSHA-projekt[25] célja a kiberpartnerség kialakítása. Végül az EU számos multilaterális internetes kezdeményezésben és fórumban vesz részt. Az EU saját álláspontját az ENSZ keretében kidolgozott alapelvek vezetik, összhangban a nemzetközi joggal. A kiberdiplomáciai eszköztár következtetései figyelembe veszik az ENSZ kormányzati szakértői csoportjainak (GGE) iránymutatásait. Az EU tehát elkötelezi magát amellett, hogy aktívan támogatja „az állami felelősségteljes magatartás önkéntes, nem kötelező érvényű normáinak kidolgozását a kibertérben és a regionális bizalomépítő intézkedéseket", amelyekben az EBESZ vezeti a munkát.

Az aktív kibervédelemre való felkészülés terén is jól kitapinthatók az EU intézményépítési erőfeszítései. A 2018-os globális kiberbiztonsági index[26] szerint regionálisan Európa leginkább a kibertudatosság-növelő kampányok, a kutatás és fejlesztés, valamint az oktatási programokban jeleskedik. Európa több kétoldalú és többoldalú megállapodást kötött, ennek ellenére az Európát célzó támadások nem csökkennek. Csak 2018-ban[27] több támadás történt Kínából, Iránból, Pakisztánból vagy Oroszországból, az elkövetők pedig továbbra sem ismertek.

[20] Annegret Bendiek: The EU as a force for peace in international cyber diplomacy. *SWP Comment,* 19. (2018. április 19.)

[21] *EU Cyber Direct* (2020).

[22] Council of Europe: *CyberEast.*

[23] *EU4Digital.*

[24] EEAS: *West African response on cybersecurity and fight against cybercrime (OCWAR – C).* (2019. január 7.)

[25] Yaksha: *Cybersecurity Awareness and Knowledge Systemic High-level Application* (2020).

[26] ITU: *Global Cybersecurity Index (GCI) 2018.* Geneva, ITU Publications, 2018. 17–18.

[27] Daniel Fiott: *EUISS Yearbook of European Security 2019.* Paris, EUISS, 2019. 11.

Noha az EU legutóbbi kiberbiztonsági stratégiája 2013-ra nyúlik vissza,[28] a 2017. évi kiberbiztonsági csomagban[29] felülvizsgálták, és számos útmutató dokumentumot (többek között az EUGS) adtak ki. Felismerve a kiberfenyegetések állandó jelenlétét, valamennyi EU-tagállam kiberstratégiákat[30] dolgozott ki. Javaslat készült arra nézve is, hogy nevezzék ki az EU nemzetközi kibertér-politikáért felelős különleges képviselőjét,[31] aki képviselné az EU álláspontját a nemzetközi színtéren.

Az EU-szintű együttműködés példái az ENISA szoros együttműködése az Európai Védelmi Ügynökséggel (EDA), az EU számítógépes vészhelyzet-elhárítási csoportjaival (CERT-EU) és az Europol Európai Kiberbűnözői Központjával (EC3). A főbb EU-szintű szervezetek a következők:

- ENISA (Európai Uniós Kiberbiztonsági Ügynökség),
- Europol (EC3, Kiberbűnözői Központ),
- EU hírszerzési és helyzetelemző központ,
- EU katonai hírszerzési igazgatósága,
- CERT-EU,
- vészhelyzeti koordinációs központ,
- a tagállamok számítógépes biztonsági eseményekre reagáló csoportjai,
- EiT horizontális munkacsoportja a számítógépes kérdésekkel kapcsolatban,
- EEAS kiberszemélyzete,
- EDA kiberszemélyzete,
- PESCO-kiberprojektek,
- Európai Védelmi Alap (kiberprojektek finanszírozása),
- eu-LISA,
- EU Cyber Direct,
- a hibrid fenyegetések elleni küzdelem európai kiválósági központja.

A nemzetközi jog elsőbbsége a kibertérben és általában a nemzetközi kapcsolatok terén európai alapelv.[32] A fenti operatív testületek mellett az EU első számítógépes jogszabálya – a 2016. évi hálózati és információs rendszerek biztonságáról szóló irányelv – is elősegítette a kiberbiztonsági előírások harmonizációját az EU-ban. Az Európai Bizottság jelenleg a NIS-irányelv felülvizsgálatát tervezi,[33] hogy „tovább erősítse az Unió általános kiberbiztonságát".

[28] European Commission: *EU Cyber Security strategy: An open, safe and secure Cyberspace* (2013. február 7.).

[29] European Commission: *Cybersecurity package 'resilience, deterrence and defence: Building strong cybersecurity for the EU'* (2017. szeptember 19.).

[30] ENISA: *National Cyber Security Strategies – Interactive Map* (2020).

[31] Patryk Pawlak: Rebooting the EU's cyber diplomac. *Eucyberdirect.eu,* 2019. november.

[32] Eneken Tikk: International law in cyberspace: Mind the gap. *EU Cyber Direct,* 2020. március 4.

[33] European Commission: *Commission Work Programme 2020. A Union that strives for more COM/2020/37 final* (2020. január 29.).

2017-ben a Bizottság elfogadta a kiberbiztonsági törvényt,[34] átalakítva és támogatva az ENISA-t. A törvényt tartalmazó csomag tartalmaz egy tervet is, amelynek célja, hogy az EU tagjai és az EU intézményei meglévő válságkezelési mechanizmusok segítségével[35] reagáljanak a számítógépes eseményekre. További elem következett 2018-ban a Bizottság javaslataival[36] a kiberbiztonsági kompetencia-központok hálózatának és az európai kiberbiztonsági ipari, technológiai és kutatási kompetencia-központ létrehozásáról, amelynek célja az EU kiberképességének megerősítése. 2010 óta az EU kétévente páneurópai számítógépes gyakorlatokat (CyberEurope) szervez,[37] 2020-ban az egészségügyi szektor elleni számítógépes támadás forgatókönyvére összpontosít. Az EU-nak 10 stratégiai partnersége van,[38] amelyek többsége kiberdimenzióval rendelkezik;[39] ezek révén is az EU a szélesebb körű stratégiai célkitűzései összekapcsolásán dolgozik, ideértve a kiberdiplomáciát is. Ezenkívül az EU kiberkapcsolatokban áll az Afrikai Unióval – a 2020. februári közös közlemény[40] említi a kiber-együttműködést – és a Délkelet-ázsiai Nemzetek Szövetségével (ASEAN), amelynek 2019 augusztusának közös nyilatkozata[41] rámutat arra, hogy szándékukban áll megerősíteni az „együttműködést a kiberügyekben".

Járvány: a felgyorsuló konfrontáció frontvonalai

Többször említettük, mert hangsúlyos jelenség: a Covid-19-járvány szinte követhetetlen sebességre korbácsolta fel a nemzetközi hatalmi terek, benne az egyre meghatározóbb kibertér átrendeződési folyamatait. Ennek megfelelően fontos fejleményeket dokumentálhatunk a nemzetközi kapcsolatok három alapvető működési mezőjében: a tárgyalásos mechanizmusokra épülő (és többnyire nyílt) diplomáciában, az érdekérvényesítés erőszakos (katonai és szankciós) módozataiban, valamint a közöttük húzódó szürke zónát kitöltő hírszerzés világában egyaránt. Utalni fogunk arra is, hogy ezek az elemek szorosan összekapcsolódnak, egymásra épülnek a valódi világban.

[34] European Parliament: *ENISA and a new cybersecurity act* (2019. július 5.).
[35] Uo.
[36] European Commission: *Proposal for a European Cybersecurity Competence Network and Centre* (2018).
[37] ENISA: *Cyber Europe 2020.*
[38] EPRS: *EU strategic partnerships with third countries* (2012. október 2.).
[39] Thomas Renard: EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society,* 19. (2018), 3. 1–17.
[40] European Commission: *10th African Union Commission – European Commission Meeting – Joint Communique* (2020. február 29.).
[41] ASEAN: *ASEAN-EU statement on cybersecurity cooperation* (2019).

A nagypolitikai összecsapások fő terepe: kiberdiplomácia

Ami kereskedelmi háborúskodásnak indult, az a koronavírus-járvány felbukkanásának időpontjára egyértelműen ádáz technológiai összecsapássá változott. Ha pontosabban akarunk fogalmazni: kezdettől geopolitikai jellegű volt ez az Egyesült Államok és Kína között kibontakozó konfliktus, amely eleinte a kereskedelmi viták és egyezkedések formáját öltötte magára. Amikor a Covid-19-járvány lecsapott a világra, akkor már egyértelműen a technológia alkotta a két nagyhatalom közötti összecsapás meghatározó frontvonalát. Az események fókuszában álló Huawei-ügy is jól mutatja: az időszak meghatározó fejleményei valójában jó ideje robognak a végkifejlet felé, a járvány csupán felgyorsította ezt a tempót.[42]

Az USA 2017-ben érezte úgy, hogy a minden téren rohamosan erősödő Kínai Népköztársaság technológiai óriáscégei, a Huawei, a ZTE, a DJI, a Tencent, az Alibaba immár komoly kihívást jelentenek az amerikai műszaki-technológiai fölény számára. A kereskedelmi, pénzügyi, technológiai területen kirobbant viták akkor a ZTE-re kirótt több mint egymillió dolláros amerikai büntetésben csúcsosodtak ki, de elemzők már akkor is úgy vélték: a figyelmeztetés valójában a Huawei-nek szólt. A kínai vállalatóriás ugyanis a kidolgozója és egyben élenjáró fejlesztője az 5G-technológiának. Márpedig – vélik egyöntetűen a szakemberek – az okoseszközök összekapcsolását, a mesterséges intelligencia széles körű alkalmazását ez az új generációs mobilhálózat teszi majd lehetővé. A jövő csúcstechnológiája szempontjából kulcsfontosságú területen ugyanakkor az USA végletesen lemaradt a kínaiak mögött.[43] A stratégiai, sőt geostratégiai jelentőségű ügyben az Egyesült Államok már 2018-ban megkezdte az „ellentámadást". Az USA kérésére pénzügyi csalás vádjával letartóztatták a Huawei alapítójának lányát, majd 2019-ben az amerikai kormány tiltólistára helyezte a kínai nagyvállalatot. Az indokolás az volt, hogy a kínai kormánnyal és hadsereggel szoros kapcsolatokat ápoló Huawei súlyos nemzetbiztonsági kockázatot jelent a berendezéseit, rendszereit használó államok számára.[44] Az alapvető gyártási-üzleti folyamataiban ezzel súlyosan megszorongatott cég ellen az idei évben erőltetett tempójú és immár globális kiterjedésű diplomáciai támadásba kezdett az amerikai külügy. Az eredményesnek látszó akciósorozat nyomán a kiemelt szövetséges Nagy-Britannia bejelentette a Huawei kizárását épülő 5G-hálózataiból, illetve a cég által gyártott egyéb berendezések kötelező cseréjét. Hasonló módon lépett az USA több más

[42] A Huawei-ügy pontos és kimerítő bemutatását adja: Shoo Zen – Sarah Dai: How did Huawei fall foul of the US government and find itself at the epicentre of a new tech war? *South China Morning Post,* 2020. április 6.

[43] Szemben a Huawei-jel vagy a szintén kínai ZTE-vel, illetve a mögöttük járó finn Nokiával vagy a svéd Ericsonnal szemben az USA nem rendelkezik ilyen méretű piacvezető telekommunikációs céggel a Lucent Technologies felvásárlása óta.

[44] További vádként szerepelt az is, hogy a cég technológiájával figyelik meg Kínában a muszlim ujgur kisebbség tagjait is.

szövetségese, közöttük Olaszország, Franciaország, illetve az amerikai kontinensen befolyásos Brazília is.

Különösen érdekes fejlemény volt az ügyben India lépése. A Kínával szomszédos (és rivális) ország maga is regionális hatalmi státuszra tart igényt, és ebben kapóra jön számára az angolszászok vezetésével az Indo-Pacifikum térségében kovácsolódó új tömörülés („Quad", a „Négyes fogat") tagsága.[45] Az indiai kormány 2020 nyarán betiltotta 59 kínai fejlesztésű és tulajdonú kisalkalmazás használatát az ország területén. Az érintett appok között olyan ismert márkaneveket találunk, mint a TikTok, a Hello vagy a WeChat, tehát a világ legnépszerűbb (és legtöbb felhasználóval büszkélkedő) közösségimédia-platformjainak némelyikét. A lépést nem sokkal később újabb „digitális csapás" követte: India ezúttal további 47 kínai mobilalkalmazást tiltott ki az ország területéről; a vád itt is az indiai felhasználók személyiségi jogainak a megsértése volt.[46]

S ezzel tulajdonképpen ő adta meg a jelet a kínai technológiai nagyvállalatok elleni amerikai támadás második menetének. A rövidvideó-megosztóként üzemelő TikTok bizonyos értelemben nagyobb szálka Amerika szemében, mint a Huawei. A kínai fejlesztésű és tulajdonú közösségimédia-alkalmazás minden képzeletet felülmúló népszerűségre tett szert eddigi rövid pályafutása alatt. A mai világban, ahol a közösségi média roppant közvéleményformáló ereje az elmúlt fél évtized során meglehetősen nyilvánvalóvá vált, egy ilyen eszköz óhatatlanul geopolitikai jelentőséget is kap. Különösen, ha figyelembe vesszük, hogy a TikTok az amerikai tizenévesek körében is kirobbanó népszerűségnek örvend. Az amerikai kormányzat most eltökélte, hogy kitiltja a „Kínai Kommunista Pártnak közvetlenül adatokat szivárogtató" mobilalkalmazást. Érdekes fordulat – és egyben lehetséges törésvonalak sejtetője – ugyanakkor, hogy Emmanuel Macron francia elnök éppen most nyitott saját fiókot a TikTokon.

Szakmai és politikai körökben ugyanakkor megindult a gondolkodás arról, hogy a járvány időszakában érezhetően lobbanékonyabbá vált kiber-ökoszisztémában hogyan szilárdíthatná meg (vagy legalább őrizhetné) a pozícióit Európa. Az elmúlt időszak eseményeire (a kínaiak EU-beli kritikusinfrastruktúra-akvizíciói és az általuk vívott hibrid hadviselés) válaszul több javaslatot is megfogalmaztak szakmai körökben a NATO szemszögéből. Ezek közé tartozik a további kritikus infrastruktúrák, stratégiailag fontos vállalatok felvásárlása elleni közös fellépés. A járvány ideje alatt egyes tagországok (például Spanyolország) olyan döntést hoztak, hogy megvédik e gazdaságilag nehéz időszakban a stratégiailag fontos vállalataikat, azonban közös egyetértés, fellépés nincsen ez irányban. Izgalmas felvetés a kínai hibrid hadviselés elleni offenzív fellépés erősítése a szövetségen belül, illetve a NATO és az EU együttműködésének erősítése. Ahol a NATO-nak nincs mandátuma és megfelelő eszköze, ott az EU és a multinacionális vállalkozások a kínai hibrid fenyegetések leküzdéséhez szükséges

[45] A „Quad" az USA mellett Ausztráliát, Japánt és Indiát kapcsolná stratégiai együttműködésbe.

[46] A technológiai támadássorozathoz a Himalája magashegységeiben kirobbant, emberéleteket is követelő kínai–indiai határincidens szolgált apropóul.

jogszabályok és pénzügyi ösztönzők kidolgozásában és érvényesítésében játszhatnak kritikus szerepet, míg a másik oldalról a NATO és szövetségesei az információk megosztására, a kibertér védelmére, az új technológiák képességi céljainak kidolgozására és a gyakorlatok lebonyolítására összpontosíthatnak az elrettentés megerősítése érdekében.[47] Ennek egyik megvalósulási terepe lehetne a hibrid fenyegetések elleni küzdelem európai kiválósági központja.

A narratívák harcmezején: digitális diplomaták

A 2019-es év szembeötlő újdonsága az volt, ahogyan a kínai államigazgatás – minisztériumok, állami tisztviselők, diplomaták sokasága – rohamos gyorsasággal elkezdte „belakni" a közösségi média tereit, elsősorban a Twitter hírfolyamát. A hivatalos minőségben folytatott posztolás – az új csatornához igazodva – hangnemében is változást hozott a kínai nemzetközi kapcsolattartásban. Élesebb, nyíltabb, „asszertívabb" lett. A Kínai Népköztársaság jól láthatóan erősíti közvetlen kapcsolódását a nemzetközi közvéleményekhez, új kommunikációs csatornákat keresve és használatba véve arra, hogy Kína „narratíváját" immár globális léptékben is terjessze.[48] Az ügy érdekessége, hogy a Digitális Tűzfal mögé húzódó Kína – miközben kitűnő és igen népszerű hazai közösségimédia-platformokat biztosít polgárainak – blokkolja a jelentős nyugati (értsd: amerikai tulajdonú vagy fejlesztésű) platformokat, egyebek mellett a Facebookot és a Twittert is. Ugyanakkor láthatóan arra ösztönzi tisztségviselőit, hogy aktív közéleti-kommunikációs szerepet vigyenek ezekbe a „nyugati" közösségi médiaterekbe.

Az új keletű „asszertivitás", magyarul ez a határozott, sokszor éles fellépés nem szorítkozik az információk megosztására. A kínai diplomácia közösségimédia-tevékenységének fontos része az országáról terjesztett – és a hivatalosság által hamisnak tekintett – „álhírek" megcáfolása. A digitálismédia-terekben aktivizálódó kínai diplomácia a jelek szerint felismerte, hogy micsoda erő rejlik az információ hitelesítésében – vagy éppen hiteltelenítésében. A koronavírus-járvány ezen a téren is roppant kihívásokat és hasonlóan nagy lehetőségeket teremtett.

Amikor 2020 márciusában, tehát a járvány korai időszakában az Oroszországi Föderáció egészségügyi felszereléseket, orvoscsoportokat küldött a legnagyobb bajban levő európai uniós (és várományos) államok segítségére, az bombaként robbant az információs terekben is. A NATO-tagállam Olaszország országútján, orosz zászló alatt robogó katonai konvoj látványa szinte sokkolta az euroatlanti világ erőcsoportjait. Elsőként Oroszország ellen indult koncentrált támadás a médiaterekben. Az igazi figyelem azonban szinte kezdettől Kínára összpontosult. A nyugati média-

[47] Speranza (2020): i. m.

[48] Feng Zhaoyin: China and Twitter. The year China got louder on social media. *BBC,* 2019. december 29.

ökoszisztéma minden fontosabb orgánuma bekapcsolódott az egymást követően kidolgozott, újabb és újabb offenzív narratívák terjesztésébe. Az első ilyen fegyverként használt „elbeszélés" ez volt: „A járvány – a kínai vírus vagy vuhani vírus, mert hiszen már a jól megválasztott szóhasználat is fegyverként használható – Kína bűnös, megfontolt gondatlansága miatt szabadult rá a világra". Ezt követte – párhuzamosan azzal, ahogy a kínai védekezési intézkedések egyre eredményesebbnek bizonyultak – egy újabb támadó narratíva: „Kína a járvány elleni küzdelem ürügyén az állampolgárok minden lépését figyelni képes digitális lehallgató-megfigyelő államot építi ki." Majd a kínai egészségügyi felszerelések (segélyek és árucikkek) külföldre áramlásával párhuzamosan megjelent egy újabb információs hadviselési tartalom: „Kína – pontosabban: a kínai állam – csupa használhatatlan ócskaságot szállít még pénzért is a bajban levő országoknak." Ezt követően épült fel (elsősorban egyes USA-beli szövetségi tagállami kezdeményezések és politikai nyilatkozatok nyomán) egy újabb narratíva: „Kínát rá kell kényszeríteni, hogy úgymond független nemzetközi vizsgálatot folytathassanak más államok a területén a járvány keletkezésének kiderítésére." Ehhez kapcsolódva szinte azonnal megjelent az is: „Kínát, mint a világjárvány okozóját, törvényszék előtt kell ezért felelősségre vonni, és kártérítés fizetésére kell őt kötelezni." Ez utóbbi két információs hadviselési narratíva mögé immár közös diplomáciai akcióban sorakozott fel a (nyugati világ új szövetségi csoportosulásaként alakuló) angolszász országcsoport, a Five Eyes[49] is.

Az egyes narratívák valóságtartalmát, „igazságát" itt most nem vizsgáltuk; önmagában sokatmondó a kommunikációs kampányok lépcsőzetes struktúrája, az újabb és újabb központi sztorik köré felhúzható narratívaépítés. S egy különösen fontos mozzanatra kell felfigyelnünk: az itt felvázolt információs hadjárat félideje környékén hirtelen megváltozott a kínai kommunikáció tartalma, és különösen stílusa, attitűdje. A korábban jellemző magyarázó, tárgyszerűségre törekvő, higgadtan fogalmazó, tehát markánsan védekező jellegű kínai kommunikációt felváltotta egy fogalmazásában nem kertelő, élesen visszavágó mondandó. Azaz a kínaiak az addigi defenzív kommunikációt egy offenzív ellennarratívára cserélték. Elsősorban a diplomáciai közlési csatornákon (ahol ráadásul markáns képviselőket kapott az új attitűd és stílus egy tehetséges, fiatal szóvivői csapat képében), de villámgyorsan tovagyűrűzött a közösségi média tereibe is, az úgynevezett „népi diplomácia" közegébe. Ez az ellennarratíva, illetve maga a harcias hozzáállás szimbolikus nevet is kapott a kínai moziipar néhány évvel ezelőtti *Wolf Warrior* című sikerfilmjéről: az igaztalannak tartott, manipulatív szándékúnak elkönyvelt

[49] Ami eredetileg a második világháború utáni világban kialakuló és döntően a hírszerzés területére szorítkozó „különleges kapcsolatrendszert" jelentett az angolszász „ötök", az USA, Nagy-Britannia, Kanada, Ausztrália és Új-Zéland között. A szoros együttműködés, amely nyers, feldolgozatlan hírszerzői értesülések kölcsönös cseréjét (tehát egy a nemzetbiztonság világában szokatlanul intim együttműködést) jelentette, a hidegháború utáni világban is folytatódott. Az utóbbi évek fejleményei (Brexit, USA és EU közötti viszony hűvösebbre fordulása) nyomán erősödnek a törekvések az együttműködés új tartalmakkal való kiszélesítésére a globális geopolitika és főleg a nemzetközi kiberkapcsolatok területén.

nyugati narratívákkal bátran szembeszálló és a kínai érdekeket a történetmesélés nemzetközi hadszínterein is védelmező diplomatákat keresztelték el „farkasharcosoknak".[50]

Az elszánt és kemény fellépéseken megütköző amerikai külpolitikai establishment (majd a mögé rövid fáziskéséssel felzárkózó nyugati médiaelit) ekkor újabb támadó narratíva köré szervezte megszólalásait: „A kínai diplomácia durva és agresszív hangnemre váltott, és ez csak ártani fog az országnak." A hajdan halk szavú, simulékony, jelentéktelen kínai diplomácia „farkasharcosok" falkájává változott – vette át a formulát, koncentrikus körökben, egyre több nyugati médiatermék. Amerikai kommunikációs kutatók szerint az új stílussal, új nyelvezettel, új attitűddel a kínai diplomácia csak veszít. A „világ közvéleményét" ugyanis, mondják, ez a „farkasharcos diplomácia" csak még jobban maga ellen hangolja.[51] A megalapozott válaszhoz azonban még további idő szükséges.

A járvány azonban nem csak bilaterális viszonylatban ösztönözte a digitális diplomácia aktivitását. Az online közösségi terekben zajló kommunikáció jelentőségét a legfontosabb multilaterális szervezet is felismerte. A koronavírus-világjárvány egyik szembeötlő kísérőjelensége ugyanis a veszélyekhez, a betegség lefolyásához, a várható következményekhez kapcsolódó közgondolkodás és a társadalmi párbeszéd megszaporodása. Az emberek természetszerűen aggódnak, információkra vágynak, bizonyosságokat szeretnének. Az elektronikus kommunikációs eszközök széles körű elterjedésével, és különösen a közösségi média eszközeinek már-már központi szerepkörével, életünkben korábban nem látott tömegben és sebességgel kerültek forgalomba a „Covid-19-információk". Problémát jelent persze már maga az óriási információtömeg is, de az igazi gondot az jelenti, hogy a valóságos tényeket tartalmazó (és jó szándékkal közzétett) információk mellett hatalmas mennyiségben keringenek megalapozatlan, akár valótlan, sőt kifejezetten félrevezető (és eleve rossz szándékkal koholt és terjesztett) információk is. Az ENSZ is egyenesen „infodémiáról" beszél: a vírusjárvánnyal párhuzamosan kibontakozó és a koronavírus-járványhoz hasonlóan fenyegető információs pandémiáról.[52] A Világszervezet álláspontja szerint a koronavírus-járványhoz kapcsolódó hamis és félrevezető információk drámaian veszélyeztetik a betegség elleni védekezés eredményességét, a közegészségügyi rendszerek működését. A probléma kezelésére az ENSZ átfogó akciót hirdetett májusban. Nyílt felhívásban kezdett toborozni önkénteseket, akik a koronavírussal kapcsolatos online információforgalom elemzésével, az adatok szűrésével, valóságtartalmuk ellenőrzésével segítik az egészségügyi témájú álhírek elleni harcot. A Világszervezet mintegy 10 ezer főnyi „tényellenőrző" csapatot

[50] Zhaoyin (2020): i. m.

[51] Daniel C. Mattingly – James Sundquist: *How public diplomacy builds China's soft power.* New Haven (US-CT), Yale University Department of Political Science, 2020. Érdemes azonban felfigyelni rá: a Yale Egyetem kutatói a tanulmány alapjául szolgáló attitűdvizsgálatba kizárólag indiai megkérdezetteket választottak ki (ráadásul kizárólag angolul beszélőket). Az pedig, hogy regionális szinten jelenleg India jelenti Kína első számú geopolitikai riválisát, vélhetően erősen befolyásolja a vélemények alakulását.

[52] Amy Lieberman: UN enlists 10,000 digital volunteers to fight COVID-19 misinformation. *Devex.com,* 2020. július 2.

szeretne felállítani. Az önkéntesek e-mailen keresztül kapják meg az ellenőrizendő információkat. Ugyanakkor saját baráti, szakmai közegükben is végzik a vírussal kapcsolatos tények ellenőrzését, korrigálását. A munkába számos újságíró-szervezet munkatársai kapcsolódtak be, akik eredményesen képesek támogatni az ENSZ járványügyi globális felvilágosító munkáját.

Az ENSZ Egészségügyi Világszervezete (WHO) a globális koronavírus-járvány elleni küzdelem összetett feladatrendszerében maga is nagy jelentőséget tulajdonít a járványhoz kapcsolódóan hömpölygő infóáradatnak. A WHO-szakemberek úgy látják, hogy az információs járványt, az infodémiát nem lehet felszámolni, legfeljebb csak kezelni. Ennek érdekében a világszervezet egy többhetes konferenciasorozatot és webináriumot szervez, amely három egymásra épülő szakaszból tevődik majd össze, lehetőséget adva a világszervezet specialistái mellett a szélesebb szakmai közvélemény bevonására is. A cél az, hogy olyan eljárásokat, eszközkészleteket fejlesszenek ki, amelyek segítik az infodémia jelenségeihez való társadalmi alkalmazkodást, a kognitív boldogulást megnehezítő információs fenyegetésekkel (tömegesség, megalapozottság hiánya, félrevezető szándékosság stb.) szembeni ellenálló képességet.

Árnyékháború: hírszerzők és felforgatók a kibertérben

A nemzetközi kiberkapcsolatok „szürke zónájában" is aktív időszakot hozott a koronavírus-járvány terjedése és elhatalmasodása. A közegészségügyi, járványügyi és különösen a vírus tartós megfékezésére alkalmas vakcina előállításához szükséges orvos-biológiai kutatási információk értéke hihetetlenül megnőtt. Lényegében minden ország versenyt fut az idővel, a gyógyszerfejlesztés hosszadalmas ciklusának lerövidítése érdekében rendkívüli mértékben fokozódott az online hírszerzői tevékenység. Egy óvatos intés azonban már a téma elején kikívánkozik: a kiberhírszerzés világa, a dolog jellegénél fogva, többnyire rejtve zajlik. Általában nagyobb titkolózás övezi, mint a felderítés és elhárítás „hagyományos" akcióit. A kibertérben végzett hadműveletek esetében ugyanis már maga az „attribúció", az elkövetők észlelése, felderítése és egyértelmű azonosítása is sokszor problematikus. Az ilyen eseményekről nyilvánosságra kerülő információk esetében mindig érdemes észben tartani: éppen annyi kerül ezekből a nyilvánosság elé, amennyit az érintettek szeretnének. Ami óhatatlanul azt is jelenti, hogy a kibertérben folyó hírszerzéssel kapcsolatos információk szinte mindig összefonódnak a külvilág befolyásolását célzó információs hadviselési mozgásokkal. Nehéz ezt nem észrevenni a járványidőszakban: amikor a nagyhatalmak minden korábbinál nagyobb lendülettel vetik bele magukat a geopolitikai birkózásba, és amikor a középhatalmak is – sőt még a kis államok is – erőforrásaik összességét igyekeznek mozgósítani a vírus okozta hirtelen támadt nemzetbiztonsági fenyegetés elhárítására –, akkor csupán három olyan szereplővel találkozunk a nyilvánosságban, amelyek a válsághelyzethez kapcsolódó illegális információszerzésre vállalkoznak: Iránnal, Oroszországgal és Kínával. Magyarán az Egyesült Államok (és következésképpen a nyugati világ) „ősellenségeivel".

A nyugati médiában először májusban jelent meg híradás arról, hogy amerikai és brit kiberbiztonsági szakértők figyelmeztetése szerint „három meg nem nevezett ország" hackerei igyekeznek a Covid-19-járvány megfékezését lehetővé tevő védőoltás kifejlesztéséhez kellő kutatási adatokat, információkat megszerezni. „Jól értesült sajtókörök", mint például a brit állami fenntartású BBC, tudni vélték: az orvos-biológiai és gyógyszeripari kutatóintézetek hálózatait célba vevő elektronikus hírszerzők az imént említett Irán, Oroszország és Kína speciális katonai alakulataiból kerültek ki.[53] Két héttel később aztán az iráni állam online hírszerzőinek a járványhoz köthető titkos akcióiról jelent meg híradás, azzal vádolva őket, hogy a vakcinák kifejlesztéséhez szükséges kutatási adatok illegális megszerzésére törekedtek. Az amerikai IBM biztonsági csoportja által az ITG18-csoportként azonosított katonai hackereket a különösen képzett és jól felszerelt online hírszerzők között tartják számon a szakemberek.[54]

Alig néhány nappal ezután, összehangolt formában, tette közzé a nyugati világ néhány fontos sajtóterméke (élén a liberális körökben meghatározó *The New York Times*szal) a hírt: az APT29 kódon számon tartott (és az orosz hírszerzéssel kapcsolatba hozott) orosz hackeregység illegális akcióinak a nyomára bukkantak a brit, az amerikai és a kanadai biztonsági szolgálatok.[55] A közzétett hírek szerint az orosz hírszerzők több egyetemi kutatóközpont, vállalati laboratórium, illetve állami közegészségügyi intézmény szervereit megpróbálták feltörni abból a célból, hogy az oltóanyag-előállítással kapcsolatos kísérletek eredményeit megszerezzék. A feltételezés szerint az oroszok számos kanadai és brit cég levelezőrendszerei ellen is támadást intéztek, ám a cél – hangsúlyozták a források – sehol sem a károkozás (szabotázs volt), itt belső emberek e-mail-címeinek megszerzésével akartak hozzáférést szerezni különböző rendszerekhez. A közreadott állításokban az is hangsúlyosan szerepelt, hogy a behatolási kísérletekért felelőssé tett szervezet az SZVR, az orosz külső hírszerző szolgálat alárendeltségébe tartozik.[56] A biztonsági források szerint a behatolási kísérletek már februárban elkezdődtek, ám tényleges adatlopásra nem merült fel bizonyíték. A brit GCHQ hírszerző központ korábbi vezetője szerint a célpontok között szerepelhetett az Oxfordi Egyetem orvos-biológiai kutatóintézete, valamint a nyugati vakcinafejlesztési erőfeszítések egyik központjának számító svéd–brit AstraZeneca gyógyszeripari vállalat.

[53] Gordon Corera: Coronavirus: Cyber-spies hunt COVID-19 research, US and UK warns. *BBC,* 2020. május 5.

[54] A „Bájos Kiscicák" *(Charming Kitten)* fedőnéven is ismert egységről feltételezik, hogy már a 2016-os amerikai elnökválasztás idején is igyekezett behatolni az USA számítógépes rendszereibe. Dan Goodin: Iranian state hackers caught with their pants down in intercepted videos. *Arstechnica,* 2020. július 17.

[55] Julian E. Barnes: Russia is trying to steal virus vaccine data, Western nations say. *The New York Times,* 2020. július 16. A „Kedélyes Mackók" *(Cozy Bear)* fedőnéven is ismert egységről feltételezik, hogy ők voltak felelősek a 2016-os amerikai elnökválasztás idején a Demokrata Párt számítógépes rendszereibe való illegális behatolásért és adatlopásért.

[56] Az APT29 csoportot a laikus nyugati sajtó gyakorta a GRU, az orosz katonai hírszerzés kötelékébe tartozónak véli.

Alig néhány nappal ezután, szinte menetrend szerint időzítve, újabb kiberkémkedési kísérletről számolt be a nyugati sajtó, a prímet most is a *The New York Times* vitte.[57] Az USA Igazságügyi Minisztériumának közlésére hivatkozva adta hírül a cikk, hogy két kínai hackert gyanúsítottak meg hivatalosan is azzal, hogy hazájuk állami szervezeteinek megbízásából amerikai oltóanyag-fejlesztési kutatási anyagokat igyekeztek jogtalanul eltulajdonítani amerikai számítógépes rendszerekből. A két gyanúsított (akiket szokatlan módon néven is neveztek az amerikai elhárítási és igazságügyi szervezetek) az FBI feltételezése szerint hol a Kínai Állambiztonsági Minisztérium javára, hol pedig saját hasznukra dolgozva egész sor vállalat szervereibe hatolt be, nagy értékű szellemi tulajdont eltulajdonítva. A koronavírus-járvánnyal összefüggésben már januárban akcióba léptek: előbb egy a vakcina fejlesztés-kutatási problémáin dolgozó massachusettsi biotechnológiai cég szerverein végeztek „előzetes felderítést", majd egy másik, ezúttal kaliforniai kutatócég hálózatát igyekeztek feltörni. Ismert, hogy a Moderna, az amerikai oltóanyag-fejlesztés élenjáró vállalata, is Massachusettsben található. Május közepén, szintén Kalifornia államban, egy Covid-19-teszteket előállító cég kutatási anyagait tulajdonították el. A Kínai Külügyminisztérium, természetesen, vehemensen cáfolta a vádakat.

Kiberharcosok: szervezetépítés és szárnypróbálgatás

Bár csupán szórványosan, de a katonai jellegű (támadó) akciókkal (és az ellenük való védekezéssel) kapcsolatban is akad néhány dokumentálásra érdemes fejlemény, részben közvetve, részben pedig közvetlenül kötődve a koronavírus-járványt kísérő intenzívebb nemzetközi mozgásokhoz.

A járvány által lefedett időszakban elsőként a kiberhadműveletekben erőteljes szereplőként nyilvántartott Iránhoz kapcsolódó esemény keltett figyelmet. A július elején regisztrált akcióban azonban a perzsa állam nem a kezdeményező, hanem a szenvedő fél volt. Súlyos kibercsapás érte az ország atomipara szempontjából kulcsfontosságú Natanz üzemet.[58] A kiberhadművelet mögött – amely tehát valóságos fizikai károkozó, műszóval kinetikus akció volt – amerikai források az izraeli államgépezet egységeit sejtették. Érdemes emlékeztetni rá: ez volt az első olyan létesítmény, amelyet a kibertéren át történő beavatkozás következtében fizikai károk értek. A hajdani, úgynevezett Stuxnet-vírust bevető akció mögött is az izraeli hadsereg különleges high-tech egységét gyanították.[59]

[57] Julian E. Barnes: Data for China. *The New York Times,* 2020. július 21.

[58] Itt működtek azok a nagy sebességű centrifugák, amelyek a fegyverminőségű uránium dúsítását végezték. A Stuxnet néven emlegetett féregvírus a centrifugákat vezérlő számítógépeket zavarta meg. A 2010-ben felfedezett támadás során helyreállíthatatlanul károsodott a gyártósor tetemes része.

[59] Simin Kargar: What the Natanz explosion signalled to Iran's disinformation apparatus. *Medium.com,* 2020. július 24.

Noha a fizikai károkozásra képes kibertámadás nagyon súlyos dolog, a járványidőszak legjelentősebb kibervédelmi eseménye mégsem az iráni esethez köthető. Ugyancsak július hónap végén az Európai Bizottság szokatlanul határozott lépésére figyelt fel a világ szakmai közvéleménye. Az Unió kiberhadviseléssel szembeni álláspontjának „keményedésére" már a hónap közepén történtek jelzések. A járványhoz kapcsolódóan ugyanis – a közvéleményt különösen felháborító módon – kibertámadások célpontjaivá váltak a súlyos esetekkel túlterhelt kórházak is. Hamarosan kiemelt fontosságúvá vált az egészségügyhöz kapcsolódó infrastruktúrák védelme, mint amilyenek a kórházak, kutatóközpontok és az ezeket ellátó infrastruktúrák. A cseh hatóságok 2020. április 16-án figyelmeztettek a kórházak elleni küszöbön álló, nagyszabású támadásokról, a Brnói Egyetemi Kórháznak át kellett ütemeznie a műtéteket, át kellett helyeznie a betegeket, és el kellett halasztania a Covid-19-teszteléseket egy 2020. március közepi kibertámadás miatt.[60] A Covid-19 elleni vakcinakutatás is érintve volt kibertámadás által, brit, amerikai és kanadai szakemberek oroszországi kiberszereplőket vádoltak meg a koronavírus ellenszerét kutató szervezetek elleni támadásokkal.[61] Az egészségügy elleni kibertámadások kapcsán az EU felszólított „minden országot, hogy gyakoroljon megfelelő gondosságot és tegyen megfelelő intézkedéseket a területéről ilyen tevékenységet folytató szereplők elleni fellépés kapcsán".[62] A „megfelelő gondosság" *(due diligence)* érdekes kérdést vet fel afelől, hogy az alkalmazandó-e a kibertérben. A „megfelelő gondosság" azt jelentené, hogy az államok kötelesek gondoskodni arról, hogy (kiber)területüket ne más államok kárára használják fel.[63] Ez azonban az effajta felügyelethez szükséges befektetéseken túl felvet adatvédelmi aggályokat is, a másik oldalról ellenben egy újabb deeszkalációs eszköz lehetne az államok kezébe: felszólítani egy másik államot, hogy a területéről történő kibertámadást állítson le, nem feltételezi az adott állam részvételét abban.

Az Unió „külügyminisztere" aztán július legvégén kemény bejelentést tett: nyilvánosságra hozta, hogy korlátozó intézkedéseket vezettek be több olyan személy, illetve szervezet ellen, akikről és amelyekről feltételezik, hogy különböző jellegű kiberakciókat intéztek az elmúlt évek során európai államok és vállalatok számítástechnikai rendszerei ellen. Josep Borrell, a közös kül- és biztonságpolitikáért felelős főbiztos nyilatkozatában megfogalmazta az eddigi megengedő uniós politikával gyökeresen szakító lépés célját: a Tanács által meghozott rendelkezésekkel a kibertérben tanúsított rossz szándékú magatartás hatékonyabb megelőzését, az ilyen cselekedetekre való hiteles reagálás demonstrálását és általánosságban az elrettentést reméli az európai

[60] Eugene E. G. Tan (2020): Cyber attacks on healtcare system: Infrastructure protection critical – Analysis. *Eurasiareview,* 2020. május 25.

[61] IntGovNews: *Internet Gov monthly brief (July): Geopolitics of 5G; COVID-19 vaccine hack controversy; UN E-Gov survey; US-EU data agreement invalidated; USMCA enforcement; E-waste in Africa; Brazil fake news bill; Turkey social media bill; G20, ISO, UNESCO, OECD on AI; Twitter hacked* (2020. szeptember 4.).

[62] European Council: *Declaration by the High Representative Josep Borell on behalf of the EU: European Union response to promote international security and stability in cyberspace* (2020. július 30.).

[63] Sico van der Meer (2020): Could the coronacrisis strengthen due diligence in cyberspace? *Clingendael,* 2020. május 13.

közösség vezetése. A bejelentett „korlátozó rendelkezések" (közkeletű nevükön: szankciók) az érintett személyek esetében (összesen hat főről van szó) utazási korlátozásokat jelentenek, valamint az Unió tagállamainak pénzintézeteiben vezetett bankszámláik befagyasztását. A rendszabály ugyanakkor kitér három érintett szervezetre is: ezeknél a pénz- és vagyoni eszközök zárolása jelenti a kirótt szankciót.

Az uniós szankció nem csupán „elsősége" okán keltheti fel a megfigyelők érdeklődését; a most bejelentett intézkedés jó néhány, több mint érdekes részletet tartalmaz. A feketelistára vett személyek közül ketten kínai állampolgárok; ellenük a vád az, hogy az APT10 néven azonosított kiberhírszerző csoport tagjaiként részt vettek 2017-ben a „Cloud Hopper-hadműveletként" azonosított informatikai támadásban. Az akcióban a Föld szinte minden kontinensén működő multinacionális felhőszolgáltató cégek szervereit érte támadás, amelynek célja információk eltulajdonítása (kémkedés) volt. A szankciós listára a két kínai mellett négy orosz állampolgár is felkerült. Ők (a leírás szerint az Orosz Katonai Hírszerzés, azaz a GRU kötelékében) egy nemzetközi szervezet, a hollandiai székhelyű Vegyifegyver Tilalmi Szervezet (OPCW) wifirendszerére igyekeztek illetéktelenül rákapcsolódni 2018-ban. A szankcionált szervezetek között egy kínait, egy oroszt és egy észak-koreait találunk. A kínai, egy technológiai cég, a vád szerint az említett Cloud Hopper-akció műszaki-informatikai hátterét biztosította. A listára került észak-koreai szervezet a feltételezések szerint a WannaCry néven ismert zsarolóvírusos támadás felelőse (és így azonos az APT38 néven azonosított hackerszervezettel): a 2017-ben történt akciósorozatnak egy lengyel állami szervezet rendszerei mellett a Sony cégcsoport szerverei estek áldozatul, illetve több vietnámi és bangladeshi pénzintézet is a károsultak között volt. A harmadik szankcióval büntetendő szervezet az Orosz Vezérkar Központi Különleges Technológiai Intézete: az indokolás szerint ez a szervezet a felelős a 2015-ben ukrán számítástechnikai rendszerek elleni indított NotPetya fantázianevű hackertámadásokért (amelyeket 2017-ben újabb kibercsapás követett, szintén ukrán célpontok ellen).

Összességében nehéz szabadulni attól a benyomástól, hogy az elmúlt évben fokozatosan elmérgesedő, majd a koronavírus-járvány nyomán végképp elszabaduló globális geopolitikai szembenállás, a már-már második hidegháborúként[64] emlegetett hatalmi politikai konfliktus áll a mostani uniós lépés hátterében, erősítve ezzel az a szakmai vélekedést, miszerint egyre inkább a kibertér válik a nagypolitikai vetélkedés, a geopolitikai szembenállás első számú hadszínterévé. Ugyanakkor konkrét jelzés lehet arra is, hogy az egyre élesedő amerikai–kínai konfliktusban „középen manőverezni akaró" Európai Unió milyen lépésekre kényszerül ebben a bonyolult helyzetben. Hogy fogalmazott Borell 2019 decemberében, újonnan beiktatott külügyi főbiztosként adott programbeszédében? „Az EU-nak meg kell tanulnia az erő nyelvén beszélni." Kérdés azonban, hogy a bejelentett szankció érdemben csökkenteni tudja-e a már amúgy is aggasztóan növekvő geopolitikai feszültséget.

[64] Niall Ferguson: Now we are in Cold War II. *Belfer Center,* 2020. április 28.

Kitekintés – egy még inkább versengő kibertér felé

A koronavírus-járvány komor díszletei között felerősödő hatalmi játszmák egy keményebb, kíméletlenebb kibervilágot sejtetnek. A hajdani, az eredeti hidegháború viszonyaihoz képest, ahol a két pólus normativitása bizonyos stabilitást adott a világnak (ami persze a feltétlen igazodás biztonságában merült ki), ebben az újfajta hidegháborúban különös, nehezen követhető logikák érvényesülnek a valóságos geopolitikai terekben és a kiberdimenzióban egyaránt. Eseti ügyszövetségek alakulnak és bomlanak fel szinte havonta, hogy aztán újabb konstellációban rendeződjenek össze az érdekeiket érvényesíteni akaró nemzetközi szereplők. Tisztázatlanok a törésvonalak: hol húzódnak, kiket választanak el, és kiket kötnek össze? Az érdekek sokrétegűek: az egyik egy adott csoportosuláshoz közelít, míg mások más szövetségek irányába tolnak el egy-egy államot.

Ha előretekintünk a jövőbe, egy olyan kibertér sejlik fel a szemeink előtt, ahol a konfliktusok gyakorisága és dimenziója egyaránt gyorsan növekszik. A koronavírus-járványnak, ha az emberiség túl is jut annak pusztító csúcsain, továbbra is szerepe lesz ebben a fejlődési trendben. A járvány, és főleg annak negatív társadalmi, gazdasági következményei, még egy ideig itt marad körülöttünk. A súlyosabban érintett vagy csak gyengébb gazdasági potenciállal rendelkező államok átcsoportosíthatják erőforrásaik egy részét a Covid-19-járvány hatásainak enyhítésére. Az így meggyengült védelmi vonalakkal körbebástyázott kiberterek ugyanakkor vonzó terepet kínálhatnak a mások gyengeségét kihasználni akaró aktoroknak (államoknak és szubállami szereplőknek egyaránt). Ezzel párhuzamos, ám furcsa paradoxonként a sebezhetőséget növelő tényező lehet a társadalmak digitalizációjának felgyorsulása, amelyhez éppen a járvány okozta vészhelyzet ad erős lökést. Ezzel ugyanis növekszik a támadható „társadalmi felület" is.[65] Elterjedt vélekedés az is, hogy mindezzel különösen a kis államok kiberterei válnak veszélyessé. A nagyok árnyékában manőverező kicsiknek a társadalmi (intézményi és „össznépi") ellenálló képesség, a ma sokat emlegetett reziliencia erősítése lehet a kiút. Fontos szerep jut a multilaterális kapcsolatoknak is (bár látni kell ezek erős korlátait is) és különösen az erőforrásokkal jól sáfárkodó, mozgékony, rugalmas, felkészült és éles eszű diplomáciának: egy professzionálisan megtervezett és kivitelezett kiberdiplomáciának.

[65] Hogy világosan lássuk az ellentmondást, elég, ha arra gondolunk: a Zoom, ez a cseppet sem rendkívüli vagy egyedi számítógépes alkalmazás néhány hónap alatt társadalmak sokaságának életében vált a szó legszorosabb értelmében létfontosságúvá. Zavara esetén nincsen digitális oktatás, nem tanácskoznak külügyminiszterek távoli követségeikkel, de a nagy multilaterális szervezetek munkája is megáll. Januárban még teljesen hétköznapi, egyszerű videókonferencia-alkalmazás – ma pedig már több kormány is a kritikus nemzeti infrastruktúra körébe utalná.

Felhasznált irodalom

ASEAN: *ASEAN-EU statement on cybersecurity cooperation* (2019). Online: https://asean.org/storage/2019/08/ASEAN-EU-Statement-on-Cybersecurity-Cooperation-FINAL.pdf

Barnes, Julian E.: Data for China. *The New York Times,* 2020. július 21. Online: https://www.nytimes.com/2020/07/21/us/politics/china-hacking-coronavirus-vaccine.html

Barnes, Julian E.: Russia is trying to steal virus vaccine data, Western Nations say. *The New York Times,* 2020. július 16. Online: https://www.nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia.html?action=click&module=RelatedLinks&pgtype=Article

Barrinha, André – Thomas Renard: Power and diplomacy in the post-liberal cyberspace. *International Affairs,* 96. (2020), 3. 749–766. Online: https://doi.org/10.1093/ia/iiz274

Barrinha, André – Thomas Renard: The emergence of cyber diplomacy in an increasingly post-liberal cyberspace. *Council on Foreign Relations,* 2020. június 10. Online: https://www.cfr.org/blog/emergence-cyber-diplomacy-increasingly-post-liberal-cyberspace

Bassot, Etienne: The von der Leyen Commission's priorities for 2019–2024. *European Parliament,* 2020. január 28. Online: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)646148

Bendiek, Annegret: The EU as a force for peace in international cyber diplomacy. *SWP Comment,* 19. (2018. április 19.) Online: https://www.swp-berlin.org/fileadmin/contents/products/comments/2018C19_bdk.pdf

Berzsenyi Dániel – Krasznay Csaba: *Nemzetközi kapcsolatok a kibertérben*. Budapest, Nemzeti Közszolgálati Egyetem. (Megjelenés alatt.)

Bing, Christopher – Marisa Taylor: Exclusive: China-backed hackers' targeted COVID-19 vaccine firm Moderna. *Reuters,* 2020. július 30. Online: https://www.reuters.com/article/us-health-coronavirus-moderna-cyber-excl/exclusive-china-backed-hackers-targeted-covid-19-vaccine-firm-moderna-idUSKCN24V38M

Bjola, Corneliu: Digital diplomacy 2.0. Trends and counter-trends. *Revista Mexicana de Política Exterior*, 113. (2018), 35–52. Online: https://revistadigital.sre.gob.mx/images/stories/numeros/n113/bjolai.pdf

Blount, P. J.: *Reprogramming the world. Cyberspace and the geography of global order.* Bristol, E-International Relations Publishing, 2019.

Choucri, Nazil: *Cyberpolitics in international relations.* Cambridge (US-MA), MIT Press, 2012. Online: https://doi.org/10.7551/mitpress/7736.001.0001

Cook, Lorne: First-ever EU cyber sanctions hit Russian, Chinese, NKoreans. *APNews,* 2020. július 31. Online: https://apnews.com/978f1494313a545e6e7e568e5f9782bf

Corera, Gordon: Coronavirus: Cyber-spies hunt COVID-19 research, US and UK warns. *BBC,* 2020. május 5. Online: https://www.bbc.com/news/technology-52551023

Council of Europe: *CyberEast.* Online: https://www.coe.int/en/web/cybercrime/cybereast

Dee, Megan: *The European Union in a multipolar world. World trade, global governance and the case of the WTO*. London, Palgrave MacMillan, 2015. Online: https://doi.org/10.1057/9781137434203

Desforges, Alix: Representations of cyberspace: A Geopolitical tool. *Hérodote,* 152–153. (2014), 1–2. 67–81. Online: https://doi.org/10.3917/her.152.0067

Domingo, Francis C.: Conquering a new domain: Explaining great power competition in cyberspace. *Comparative Strategy,* 35. (2016), 2. 154–168. Online: https://doi.org/10.1080/01495933.2016.1176467

EEAS: *West African response on cybersecurity and fight against cybercrime (OCWAR – C).* (2019. január 7.) Online: https://eeas.europa.eu/headquarters/headQuarters-homepage/56223/west-african-response-cybersecurity-and-fight-against-cybercrime-ocwar---c_uz

ENISA: *Cyber Europe 2020.* Online: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2020

EPRS: *EU strategic partnerships with third countries.* (2012. október 2.) Online: https://epthinktank.eu/2012/10/02/eu-strategic-partnerships-with-third-countries

Eubulletin: *HR/VP Josep Borell: Embracing 'geopolitical' Europe's power.* (2020. február 13.) Online: https://www.eubulletin.com/10653-hr-vp-josep-borrell-embracing-geopolitical-europes-power.html

European Commission: *A global actor in search of a strategy. European Union foreign policy between multilateralism and bilateralism*. Luxembourg, Publications Office of the European Union, 2014. Online: https://ec.europa.eu/research/social-sciences/pdf/policy_reviews/kina26572enc.pdf

European Commission: *EU Cyber Security strategy: An open, safe and secure Cyberspace.* (2013. február 7.) Online: https://ec.europa.eu/home-affairs/what-is-new/news/news/2013/20130207_01_en

European Commission: *Cybersecurity package 'resilience, deterrence and defence: Building strong cybersecurity for the EU'.* (2017. július 19.) Online: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-package-resilience-deterrence-and-defence-building-strong-cybersecurity-eu

European Commission: *Proposal for a European Cybersecurity Competence Network and Centre.* (2018) Online: https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre

European Commission: *Commission Work Programme 2020. A Union that strives for more COM/2020/37 final.* (2020. január 29.) Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=-1581957029354&uri=CELEX:52020DC0037

European Commission: *10th African Union Commission – European Commission Meeting – Joint Communique.* (2020. február 29.) Online: https://ec.europa.eu/commission/presscorner/detail/en/statement_20_365

European Council: *Council Conclusions on Cyber Diplomacy (6122/15).* (2015. február 11.) Online: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

European Council: *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities (13007/17).* (2017. október 9.) Online: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf

European Council: *Declaration by the High Representative Josep Borell on behalf of the EU: European Union response to promote international security and stability in cyberspace.* (2020. július 30.) Online: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-eu-european-union-response-to-promote-international-security-and-stability-in-cyberspace

European Parliament: *Global Trends to 2035. Geo-politics and international power.* (2017. szeptember 20.) Online: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603263/EPRS_STU(2017)603263_EN.pdf

European Parliament: *ENISA and a new cybersecurity act.* (2019. július 5.) Online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf

EU Cyber Direct. 2020. Online: https://eucyberdirect.eu/about

EU4Digital Online: https://eufordigital.eu

Ferguson, Niall: Now we are in Cold War II. *Belfer Center,* 2020. április 28. Online: https://www.belfercenter.org/publication/niall-ferguson-now-we-are-cold-war-ii

Fiott, Daniel: *EUISS Yearbook of European Security 2019.* Paris, EUISS, 2019. Online: https://www.iss.europa.eu/content/euiss-yearbook-european-security-2019

Goodin, Dan: Iranian state hackers caught with their pants down in intercepted videos. *Arstechnica,* 2020. július 17. Online: https://arstechnica.com/information-technology/2020/07/iran-state-hackers-caught-with-their-pants-down-in-intercepted-videos/?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioscodebook&stream=technology

Huizhong, Wu: In China, US protests a hot topic on state media. *Reuters,* 2020. június 1. Online: https://uk.reuters.com/article/uk-usa-china-media/in-china-u-s-protests-a-hot-topic-on-state-social-media-idUKKBN23824W?il=0

IntGovNews: *Internet Gov monthly brief (July): Geopolitics of 5G; COVID-19 vaccine hack controversy; UN E-Gov survey; US-EU data agreement invalidated; USMCA enforcement; E-waste in Africa; Brazil fake news bill; Turkey social media bill; G20, ISO, UNESCO, OECD on AI; Twitter hacked.* 2020. szeptember 4. Online: https://internetgov.news/internet-gov-monthly-brief-july-geopolitics-of-5g-covid-19-vaccine-hack-controversy-un-e-gov-survey-us-eu-data-agreement-invalidated-usmca-enforcement-e-waste-in-africa-brazil-fake-news-bill

ITU: *Global Cybersecurity Index (GCI) 2018.* Geneva, ITU Publications, 2018. Online: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Kargar, Simin: What the Natanz explosion signalled to Iran's disinformation apparatus. *Medium.com,* 2020. július 24. Online: https://medium.com/dfrlab/what-the-natanz-explosion-signaled-to-irans-disinformation-apparatus-df0668fb4ccf

Lieberman, Amy: UN enlists 10,000 digital volunteers to fight COVID-19 misinformation. *Devex.com,* 2020. július 2. Online: https://www.devex.com/news/un-enlists-10-000-digital-volunteers-to-fight-covid-19-misinformation-97615

Lehne, Stefan: Is there hope for EU foreign policy? *Carnegie Europe,* 2017. december 5. Online: https://carnegieeurope.eu/2017/12/05/is-there-hope-for-eu-foreign-policy-pub-74909

Manor, Ilan: *What is digital diplomacy, and how is it practiced around the world?* (2016.) Online: https://www.researchgate.net/publication/310952363_What_is_Digital_Diplomacy_and_how_is_it_Practiced_around_the_World_A_brief_introduction/link/583b591708ae3a74b4a06b2f/download

Mattingly, Daniel C. – James Sundquist: *How public diplomacy builds China's soft power.* New Haven (US-CT), Yale University Department of Political Science, 2020.

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. *Ips-journal.eu,* 2019. április 12. Online: https://www.ips-journal.eu/regions/europe/article/show/a-truly-geopolitical-eu-commission-3918

National Cyber Security Centre: *Advisory: APT29 targets COVID-19 vaccine development.* (2020. július 16.) Online: https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf

ENISA: *National Cyber Security Strategies – Interactive Map.* (2020) Online: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

Nyáry Gábor: A digitális állam a külpolitikai térben. A Twittertől az adattudományig. *Új Magyar Közigazgatás,* 12. (2019), 2. 75–83. Online: http://www.kozszov.org.hu/dokumentumok/UMK_2019/2/08_Ekozig_Digitalis_allam.pdf

Pawlak, Patryk: Rebooting the EU's cyber diplomac. *Eucyberdirect.eu,* 2019. november. Online: https://eucyberdirect.eu/wp-content/uploads/2019/11/rebooting-cyber-diplomacy-final-1.pdf

Renard, Thomas: EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society,* 19. (2018), 3. 1–17. Online: https://doi.org/10.1080/23745118.2018.1430720

Riordan, Shaun: *Cyberdiplomacy. Managing security and governance online.* Cambridge, Polity, 2019.

Shrivastava, Rahul: India bans 47 Chinese apps, over 250 more under scanner for user privacy violation. *India Today,* 2020. július 27. Online: https://www.indiatoday.in/india/story/pubg-alibaba-xiaomi-to-be-banned-india-prepares-list-of-over-250-chinese-apps-1704814-2020-07-27

Speranza, Lauren: China is NATO's new problem. *Foreignpolicy.com,* 2020. július 8. Online: https://foreignpolicy.com/2020/07/08/china-nato-hybrid-threats-europe-cyber

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

Tan, Eugene E. G.: Cyber attacks on healtcare system: Infrastructure protection critical – Analysis. *Eurasiareview,* 2020. május 25. Online: https://www.eurasiareview.com/25052020-cyber-attacks-on-healthcare-systems-infrastructure-protection-critical-analysis

Tianjiao, Jiang: From offense dominance to deterrence: China's evolving strategic thinking on cyberwar. *Chinese Journal of International Review,* 1. (2019), 2. 1–23. Online: https://doi.org/10.1142/S2630531319500021

Tikk, Eneken: International law in cyberspace: Mind the gap. *EU Cyber Direct,* 2020. március 4. Online: https://eucyberdirect.eu/content_research/international-law-in-cyberspace-mind-the-gap

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

Van der meer, Sico: Could the coronacrisis strengthen due diligence in cyberspace? *Clingendael,* 2020. május 13. Online: https://www.clingendael.org/publication/could-corona-crisis-strengthen-due-diligence-cyberspace

Whyte, Christopher – Brian Mazanec: *Understanding cyber warfare: Politics, policy and strategy*. New York, Routledge, 2019. Online: https://doi.org/10.4324/9781315636504

Yaksha: *Cybersecurity Awareness and Knowledge Systemic High-level Application.* (2020) Online: https://project-yaksha.eu/project

Zen, Shoo – Sarah Dai: How did Huawei fall foul of the US government and find itself at the epicentre of a new tech war? *South China Morning Post,* 2020. április 6. Online: https://www.scmp.com/tech/enterprises/article/3078451/how-did-huawei-fall-foul-us-government-and-find-itself-epicentre

Zhaoyin, Feng: China and Twitter. The year China got louder on social media. *BBC,* 2019. december 29. Online: https://www.bbc.com/news/world-asia-china-50832915