Molnár Dóra

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Az Egyesült Államok mint kiberdiplomáciai óriás

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

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

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

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

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

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

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

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

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

Kína és a kiberdiplomácia: egy újabb sikertörténet?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[23] Internet Assigned Numbers Authority.

[24] International Corporation for Assigned Names and Numbers.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Oroszország és a kiberdiplomácia

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

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

[38] DSR 2020, 2.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Összegzés

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

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

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

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

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

Felhasznált irodalom

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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