

A TŰZFALAKON TÚL – NEMZETKÖZI KAPCSOLATOK A KIBERTÉRBEN

Borsfai Panna

C5A5YG

Nemzetközi Tanulmányok BA

2023

Konzulens: Dr. Szőke Júlia, egyetemi docens

Tartalom

Bevezetés	3
1. A kibervilág alapfogalmai	6
2. Nemzetközi jog a kibertérben.....	11
3. Kiberkémkedés	14
4. Nemzetközi szervezetek a kibertérben	18
4.1 Az Egyesült Nemzetek Szervezete	18
4.2 A Nemzetközi Távközlési Egyesület (ITU)	19
4.3 Az Európai Biztonsági és Együttműködési Szervezet (EBESZ)	19
5. A kiberdiplomácia.....	21
5.1 A kiberdiplomácia fogalma	21
6. Nagyhatalmak a kiberdiplomáciában.....	27
6.1. Az Egyesült Államok a kiberdiplomáciában	29
6.2. Kína sikere a kiberdiplomáciában	31
6.3. Oroszország a kiberdiplomáciában – avagy a kiberháborúzás mestere	36
7. A mesterséges intelligencia a diplomáciában.....	40
Összegzés	45
Irodalomjegyzék	47

Bevezetés

A 21. század elejére, de főként a 2010-es évektől kezdve a kibertér kétségtelenül a második életterülnké vált, a fizikai teret követve. A világ lakosságának mintegy fele napi rendszerességgel használja az internetet személyes és hivatalos ügyeinek intézésére. Emellett a különböző cégeknek és szervezeteknek is szükségük van azokra az eszközökre, amelyeket az infokommunikáció nyújt. Mind a magánszemélyek, mind a szervezetek és cégek részéről egyfajta függőség alakult ki a kibertér irányába. Utóbbiak viszont a feladatuk ellátásának szükségessége miatt már nehezen tudnak foglalkozni információs rendszereik védelmével. Megnőtt a digitális ellátási láncok összetettsége, amelynek törékenysége felfoghatatlan, mindaddig, míg nem sérülnek. Már a 2010-es években egy számítógépes hiba vagy egy, az ellátási láncban véghez vitt kibertámadás jelentős gazdasági károkat okozott. Az államok feladata az, hogy ezen támadásokra válaszoljanak, miközben megőrzik saját államuk biztonságát.¹

Természetesen az internet elterjedése mellett, az államok igyekeztek fenntartani védelmüket a kibertérben. A rendészet világában is létrejöttek olyan eljárasmódok, valamint ezekre vonatkozó jogi szabályozások, melyek segítik a kormányok munkáját. Ezáltal pedig sikerült redukálni a bűncselekmények számát. Később ehhez még inkább hozzájárult az, hogy olyan szervezeteket hoztak létre (például az ENISA, az Európai Unió Kiberbiztonsági Ügynökség), amelyek már képesek voltak információbiztonsági incidensek megelőzésére is. A kiberbűnözés számának és főleg az általuk okozott károknak a növekedése azonban arra a felismerésre vezetett, hogy a szervezett bűnözés a kibervilágot is felfedezte, mint eszközt, ezért nemzetközi együttműködésre van szükség a biztonság megőrzésének érdekében. Az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezménye 2001. november 23-án került aláírásra Budapesten, ez volt az első nemzetközi egyezmény, amely elindította a nemzetközi közös fellépést a kiberbűnözés ellen.²

Az internet elterjedése mellett az államok természetesen megpróbálták fenntartani biztonságukat a kibertérben. Az együttes fellépés viszont nem mindig szolgálja az országok érdekeit. Minden államnak célja a kiberbűnözés megelőzése, de nem érdeke annak teljes

¹ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszerológati Egyetem Közszerológati Továbbképzési Intézet, Budapest, p. 6. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20fel-elos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

² u.o.

felszámolása. Olykor előfordul, hogy a bűnözők eszközei és módszerei hatékonyan alkalmazhatóak az államok javára. A bűnmegelőzési nemzetközi együttműködési rendszert meglepetésként érte, hogy a bűncselekmények áldozatai és elkövetői nem egy országban, gyakran nem is ugyanazon a kontinensen tartózkodnak, ezért az elkövető országában működő jogi rendszerre kell támaszkodniuk, de gyakran nem kapnak elég segítséget az ott tevékenységet végző hatóságoktól. Jóllehet a fizikai térben a hatóságok jellemzően képesek megküzdeni a bűnözői alvilággal, a kibervilágban gyakran találhatják magukat szembe olyan csoportokkal, amelyek teljesen anonimek, így az elkövetett bűncselekményekre gyakran nem szabnak ki büntetést. További tényező pedig, hogy a hatóságok számára olykor nehéz megkülönböztetni a bűnözőket és az államok által megbízott kibertérben tevékenykedő katonai csoportokat. A helyzetet tovább bonyolítja, hogy az állami monopóliumnak számító hírszerzés a kibertérből származó maximális hasznot húzza, amennyiben információszerzésről van szó.³

Az emberiség történelmében még nem volt tapasztalható ilyen nagyságú információbőség, és az infokommunikációs rendszerekre való támaszkodás arra készítette a kormányokat, hogy valamelyest eltérjenek a normáktól. Az elmúlt évtized során pedig a kibertérben formálódó nemzetközi kapcsolatrendszerek nagyon fontossá váltak biztonságpolitikai szempontból, ennek ellenére továbbra is kevés szakértő foglalkozik a témával.⁴

A nemzetközi kapcsolatokkal a kibertérben a kiberdiplomácia foglalkozik, ami egy meglehetősen új terület a nemzetközi kapcsolatok terén. Mivel a kibertér szabályozásával kapcsolatban még rengeteg a nyitott kérdés, így az államok közötti incidensekből adódó feszültségek megoldására a diplomácia nyújt megoldást.

A fentiek alapján a dolgozat először is ismerteti a kibervilág alapfogalmait, tárgyalja a nemzetközi jog, valamint a kiberkémkedés, hírszerzés szerepét a kibertérben. Ezek után kitér a nemzetközi szervezetek szerepére, illetve a kiberdiplomácia és a nagyhatalmak részvételének fontosságára az Egyesült Államok, Kína és Oroszország példáján. Végül a meglehetősen új tényezőnek számító mesterséges intelligencia is említésre kerül. A kutatás tehát a nemzetközi kapcsolatok kibertérbeli aspektusait tanulmányozza, azt a kérdéskört körül járva, hogy milyen

³ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszerológati Közigazgatási Továbbképzési Intézet, Nemzeti Közszerológati Egyetem, Budapest, pp. 6-7. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

⁴ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszerológati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közszerológati Egyetem, Budapest, p. 7. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

veszélyeket rejthet magában az, ha nem sikerül közös megegyezésre jutni, sikerülhet-e valójában egy nemzetközi egyezményt létrehozni a kibertér ellenőrzésére és egyáltalán szükséges-e. A dolgozatot összegzés zárja.

1. A kibervilág alapfogalmai

Amennyiben a kibervilággal, de legfőképp a kiberdiplomáciával foglalkozunk, az első lépés, hogy néhány fogalmat tisztázzunk. Korunk emberei számára a kiber kifejezés már nem idegen. Ha általánosan vizsgáljuk a fogalomkört, a „kiber” szó minden olyan dologra utal, amely valamilyen számítógépen végzendő tevékenységgel függ össze. A kifejezés magában foglal minden olyan technológiát és technikai megoldást, amely számítógéphez, internethez, mobiltelefonokhoz vagy műholdas kommunikációhoz köthető.⁵ A fogalom az ókori görög „kormányzás” szóból ered, azonban a napjainkban használt kifejezés Norbert Wiener művéhez⁶, a Kibernetikához köthető. Jelenleg négy kibernetikai fogalmat különböztetünk meg, amelyek rendkívül hasonlítanak egymáshoz, de mégis fontos őket szétválasztani:

- a kiber és a kibernetika, ami a biztonsági területre fókuszál,
- az e- vagy elektronikus előtag, ami gazdasági ágazatokra utal,
- a digitális kifejezés, amely főként a közszférára összpontosít,
- illetve a virtuális kifejezés, ami előzőleg a fent említettek összefoglaló szinonimája volt, mára viszont főként a VR alapú, tehát a virtuális valóság alapú eszközökkel kapcsolatban használjuk.⁷

Mindezek közül a legnagyobb, legszélesebb térre kiterjedő kategóriát a kibernetika képviseli, és jelen dolgozat témáját tekintve ez nyújtja a legnagyobb segítséget az eligazodáshoz a kiberdiplomácia világában.⁸

A kibertér a nemzetek érdekérvényesítésének ötödik dimenziója. A szárazföld, a víz és a földrajzi terek állandó jellege mind a nemzeti érdekek érvényesítésének fontos helyszínei. Ezek mellett a 20. században újabb helyeket határoztak meg, először is a levegőt, majd az űrt is. A 21. század egyedi jellemzőjeként a geopolitika világa újabb térrel, a kibertér dimenziójával bővült. Az információs technológia, a számítógépes hálózatok és a mobiltechnológia rohamos modernizálódása vezetett az új tér kialakulásához, és egyben újabb aggodalmakhoz.⁹

⁵ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 308. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁶ Wiener, Norbert (1961): Cybernetics: Or Control and Communication in the Animal and the Machine. Paris, Hermann & Cie & Camb. Mass. (MIT Press) 2nd revised ed.

⁷ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 308. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁸ u.o.

⁹ Szilágyi István (2018): A geopolitika elmélete, Pallas Athéné Könyvkiadó Kft., Budapest

A kibertér definícióját illetően nincs egyelőre konszenzus, viszont általánosságban háromféleképpen értelmezhető: „a kibertér egy sajátos (képzeletbeli, virtuális) környezet, a kibertér egy tartomány, a kibertér egy hálózat”¹⁰. Itt fontos lehet tisztázni a kiberbiztonság fogalmát is, amely a következő: „a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kibertér megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez”.¹¹

A kibertér geopolitizálása mellett a tradicionális fegyvereken alapuló külpolitikai aggályokat – és az általuk okozott „kinetikus” konfliktusokat – az erőszak új, fegyver nélküli, de békésnek nem tekinthető eszközei váltják fel.¹² Ez a kiberhadviselés, a háborúk közelgő digitális korszaka. A geopolitikai ártalmak elkerülése vagy az ellenük való védekezés érdekében a technológiailag fejlett államok növelik kiberpotenciáljukat.¹³

Ezért érdemes megvizsgálni a kiberhadviselés fogalmát is, hiszen ahogy a hagyományos diplomáciát sem lehet elválasztani a hagyományos hadviseléstől, úgy a kiberdiplomácia sem választható el a kiberhadviseléstől. Ezzel a hadviselési formával kapcsolatban a legfőbb kérdés az, hogy hagyományos hadviselési formának lehet-e definiálni. Ahogy az eddigi kibertérrel összeköthető fogalmakkal kapcsolatban, így ebben a kérdésben sincs konszenzus, hiszen az egyik tábor szerint hagyományosnak tekinthető, a másik oldal szerint viszont nem, és a hagyományos hadviseléstől eltérő definícióra van szükség. Napjainkban ugyanakkor rendkívül fontos foglalkozni a kibertámadások jellegével, hiszen már egy számítógépes rendszer leállítása, megrongálása, egy kormányzati weboldal leállítása is következményeket vonhat maga után, viszont ennél sokkal súlyosabb problémák is okozhatóak. A kibertér könnyű utat nyújthat a támadó felek számára például egy atomreaktor vezérlőszoftveréhez, annak leállításával pedig maga a reaktor is leáll, és akár egy csernobili nagyságú katasztrófát is okozhat. Amint ebből is látható, a kibertámadások rendkívül széles skálát fedhetnek le, az egyszerű műveletektől kezdve, a weboldalak leállításán, meghamisításán keresztül a kémkedésig.¹⁴

¹⁰ Szkála Károly – Munk Sándor (2018): A kibertér fogalma, értelmezése és fejlődése, Földrajzi Közlemények, 142(4), p 345. <https://ojs.mtak.hu/index.php/fk/article/view/1127/933> (letöltés ideje: 2023. 10. 30.)

¹¹ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, <https://net.jogtar.hu/jogszabaly?docid=a1300050.tv> (letöltés ideje: 2023. 08. 30.)

¹² Choucri, Nazil (2012): Cyberpolitics in International Relations. Cambridge, MIT Press

¹³ Nyáry Gábor (2020): Kiberdiplomácia: hatalom, politika és technológia a geopolitika ötödik dimenziójában, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 327. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

¹⁴ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, pp. 312-313. <https://nkerepo.uni->

A kiberhadviselés tehát meglehetősen eltér a hagyományos hadviselési formáktól, ugyanúgy, mint ahogy a kiberdiplomácia is némileg különbözik a hagyományos diplomáciától. Az egyik jelentős különbségtétel az, hogy a kiberdiplomácia alanyai, összetevői nem kapcsolhatóak földrajzilag sehova. Ez ellentétben áll a hagyományos diplomácia szerkezetével, ahol is a földrajzi elhelyezkedés fontos elemnek tekinthető. A hagyományos diplomácia világában az államok nagyköveteik által képviseltetik magukat, ezen rendelkezésről az 1961. évi bécsi egyezmény számol be.¹⁵ Ezzel szemben a kiberdiplomáciában a határok megfoghatatlanok és szinte meghatározhatatlanok. Ennek legfőbb oka, hogy a kibertérben általában olyan személyeken vagy számítógépeken keresztül történnek a műveletek, amelyek nemhogy másik országban, de akár másik kontinensen is találhatóak. A másik eltérés a tevékenységet végző személyekkel kapcsolatos. A hagyományos diplomáciában fellelhető a hierarchia, hiszen a nagykövetek tevékenységei a küldő országhoz kötöttek, tehát felhatalmazást kap rá a képviselő személy.¹⁶

A kibertérben azonban ez sokkal összetettebb. Sokszor a műveleteket nem lehetséges társítani egy adott államhoz vagy személyhez, ez pedig komoly problémákhoz vezet. A kibertérbeli tevékenységek kiindulópontja gyakran homályos és könnyen elrejtethető. Kiváló példának mondható erre már egy nagyon egyszerű DDoS (azaz Distributed Denial of Service) támadás is, ami tulajdonképpen annyit jelent, hogy nagyszámú idegen számítógépről rohamoznak meg egy másikat, ezzel kiszorítva jogos felhasználóját. Továbbá az is jellemzője, hogy azonosítható a támadás végpontja, viszont a forrását sokkal nehezebb meghatározni, sőt az esetek nagy részében nem is lehet 100%-ban azonosítani. E különbség illusztrálására a szakértők egy nagyon egyszerű példát hoznak, mégpedig, hogy egy rakéta kiindulási pontja megállapítható röppálya és műszaki adatok alapján, míg egy kibertámadásnál akár hónapokig is eltarthat, vagy egyáltalán nem is lehetséges visszakövetni a támadás eredetét.¹⁷

Érdekeség, hogy a kibertérben a hadviselés gyakorlata a vártnál jóval régebbi: erre az első példa a hidegháború időszakában volt, amikor a szovjet transzszibériai csővezeték

nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

¹⁵ 1961. évi bécsi egyezmény a diplomáciai és konzuli képviselők feladatköréről, <https://net.jogtar.hu/jogszabaly?docid=96500022.tvr> (letöltés ideje: 2023.10.20.)

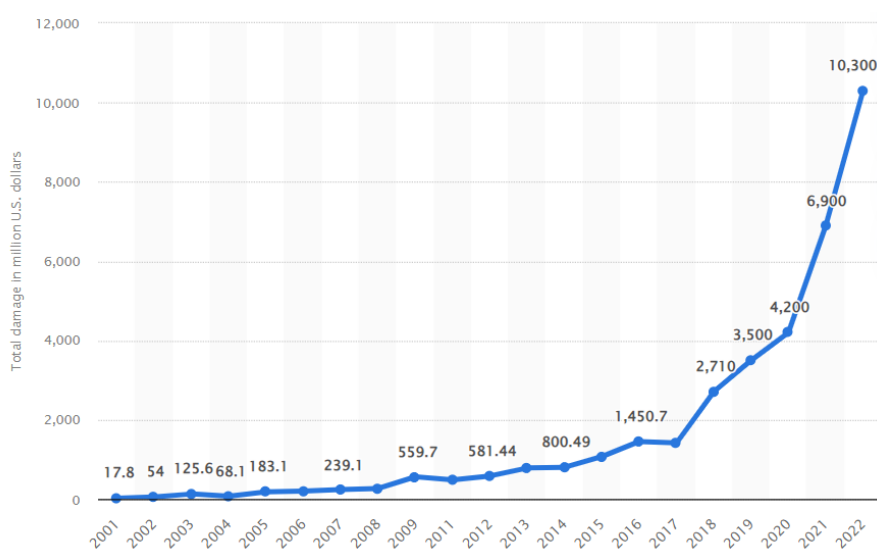
¹⁶ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 313. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

¹⁷ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 313. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

irányítórendszerét célzó kiberhadműveletre derült fény.¹⁸ Valamint ezek mellett a kínai kibernetikai katonai alakulatok már felismerték az Egyesült Államok digitális hálózatának sebezhetőségét. Ezt a 2010-es években az Egyesült Államok kormánya elleni növekvő kínai erőszak mutatta, ahol is a támadások célja elsősorban titkos információk megszerzése volt.¹⁹

Az 1. ábra illusztrálja a kiberbűncselekmények által az Egyesült Államokban okozott éves pénzügyi kár összegét 2001 és 2022 között. A 2000-es évek elejéhez képest már a 2010-es években is emelkedés volt tapasztalható, azonban 2018-tól kezdve jelentős növekedés kezdődött, a 2022-es évre pedig többszöröződött. Ebből következtethetünk arra, hogy az utóbbi néhány év során a kibertérbeli hadviselésnek még nagyobb szerepe lett.

1. ábra: A kiberbűncselekmények által az Egyesült Államokban okozott éves pénzügyi kár összege 2001 és 2022 között (millió amerikai dollárban)



Forrás: Statista, <https://www.statista.com/statistics/267132/total-damage-caused-by-by-cybercrime-in-the-us/> (letöltés ideje: 2023. 10. 27.)

Az országok közötti kibertérbeli összetűzések négy kategóriába sorolhatók: a legelső, az információgyűjtés, ezen kívül az akciók megpróbálhatják megzavarni, lebénítani, lelassítani, vagy teljesen tönkretenni a másik fél hálózatát, rendszereit. Emellett a kibertérben végzett tevékenységek a hagyományos katonai szférában további fellépések előmozdítását szolgálhatják. Végző soron a kibertámadások célja a szembenálló fél kiberkörnyezetének

¹⁸ Whyte, Christopher – Mazanec, Brian (2019): Understanding Cyber Warfare: Politics, Policy and Strategy. New York, Routledge, p. 100.

¹⁹ Domingo, Francis C. (2016): Conquering a new domain: Explaining great power competition in cyberspace. Comparative Strategy, 35(2), p. 162.

befolyásolása.²⁰ A kiberincidensek elmúlt néhány évtizedben történt előrehaladása alapján, különös tekintettel a két legfőbb versengő nagyhatalom kibertérbeli rivalizálására, nyilvánvaló, hogy a kibervilág most geopolitikai csatatérre emelkedik. Úgy tűnik, hogy a kiberhadviseléshez kapcsolódó informatikai módszerek terjedését nehéz megállítani. Ily módon a kiberhadviselés különböző módszerei, amelyek rendkívül hatékonynak bizonyulnak, egyre népszerűbbek lesznek a közepes hatalmak körében, de még kevésbé jelentős államok is alkalmazhatják ezeket. A nagyhatalmak azonban továbbra is meghatározó szerepet töltenek be a kibertérben, hiszen csak a jelentős technológiával rendelkező országok lesznek képesek összetett és bonyolult támadásokra. Végso soron, ami különösen nyugtalanító fejlemény, hogy a szakértők úgy vélik, hogy a kibertámadások és ellentámadások fejlődésével egyre hevesebbé válhatnak.²¹

²⁰ Whyte, Christopher – Mazanec, Brian (2019): *Understanding Cyber Warfare: Politics, Policy and Strategy*. New York, Routledge, p. 100.

²¹ Domingo, Francis C. (2016): *Conquering a new domain: Explaining great power competition in cyberspace*. *Comparative Strategy*, 35(2), p. 166.

2. Nemzetközi jog a kibertérben

A nemzetközi szervezeteknek jelentős szerepük van az állami normák kialakításában, de ezek főként önkéntesek alapon érvényesülnek, és legfőképp politikai elkötelezettséget jelentenek, ami persze fontos, de amennyiben jogilag ezeket nem biztosítják be, úgy nehéz hosszútávon megteremteni a globális biztonságot. Ezeket a biztosítékokat a már meglévő nemzetközi jogban szükséges keresni, ahogy azt a 2013-as GGE (Group of Governmental Experts, azaz Kormányzati Szakértők Csoportja) jelentés is dokumentálja. Viszont a kibertevékenységek sajátos tulajdonságokkal rendelkeznek, ezáltal pedig nem egyértelműsíthető a nemzetközi jog alkalmazásának szükségessége.²² Schmitt és Vihul úgy vélik, hogy a nemzetközi jognak két különálló területe van, amelyek kivetíthetők a kibertérre. Ezek közül az egyik az erő használatát, a másik a nemzetközi humanitárius jogot szabályozza. Mindkettőről elmondható, hogy olyan szabályozások ezek, amelyeket akár évszázadokkal korábban, a kibertér létrejötte előtt hoztak létre.²³

A dolgozat a következőkben néhány olyan esetet mutat be, amelyek során kérdésessé vált a nemzetközi jog alkalmazhatósága kiberincidensek tekintetében.

- Az Egyesült Államok 2016-os elnökválasztása kapcsán az ország úgy ítélte meg, hogy Oroszország beleavatkozott a választások menetébe, mégpedig olyan módon, hogy a pártok és munkatársaik által alkalmazott rendszerekbe behatolt, és a közösségi média eszközén keresztül igyekezett befolyásolni az amerikaiak szavazatait. Oroszország és Kína is különleges intézkedéseket hoz annak érdekében, hogy kitiltsák az olyan amerikai cégeket, mint az Apple, Facebook, vagy a Google a piacaikról, mindezt attól tartva, hogy az amerikai kormányzat ezeket a felületeket használja fel információk gyűjtésére. A kérdést tovább bonyolítja, hogy az említett cégek olyan fokú autonómiával rendelkeznek, amely nem függ az államoktól, a függőség hiánya pedig megnehezíti a nemzetközi vagy épp a nemzeti szabályozásukat. A Facebook esetében a moderálásának alapelvei, amelyek a szólásszabadság fokát jelentik a felületen, nem elég jól átláthatók,

²² Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszerológálati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közszerológálati Egyetem, Budapest, p. 15. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

²³ Schmitt, Michael N. – Vihul, Liis (2016): The Nature of International Law Cyber Norms. In: Osula, Anna-Maria – Rõigas, Henry (Eds.) International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn, pp. 23–48. https://www.ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch2.pdf (letöltés ideje: 2023. 09. 25.)

de mivel több, mint egy milliárdan használják a platformot, egyes esetekben meghatározó szereppel bír a politikai döntésekre.²⁴

- Elméletileg kibertámadások csak katonai célpontok ellen indíthatóak, ennek ellenére több olyan államilag támogatott ártalmas kód létezik, amelyeknek kifejezetten civilek a célpontjai. Erre egy példa lehet az állítólag oroszok által létrehozott BlackEnergy Trojan nevű trójai program, amely 2015-ben és 2016-ban is megtámadott néhány ukrainai erőművet. Másik példa a WannaCry zsarolóvírus, amelyet Észak-Koreából indíthattak, és teljesen tönkretette a brit egészségügyi rendszereket. Mindkét esetben az államok információs infrastruktúrái voltak az áldozatok.²⁵
- Egyre több katonaság alkalmaz szakembereket informatikai offenzívákra, azonban ezek a személyek gyakran nem egyenruhások, hanem csupán meghatalmazottak, akik egyáltalán nem kötődnek semmilyen hatósághoz. A magánszemélyek mellett gyakran alkalmaznak bűnözői csoportokat is, akik tevékenykedhetnek országon belül vagy kívül is. A támadó felek viszont tudtukon kívül is lehetnek azok, hiszen a valódi tettesek könnyen hamisíthatnak információkat, vagy akár civilek egy zsarolóvírus által összetett műveletekben vehetnek részt anélkül, hogy tudnák.²⁶

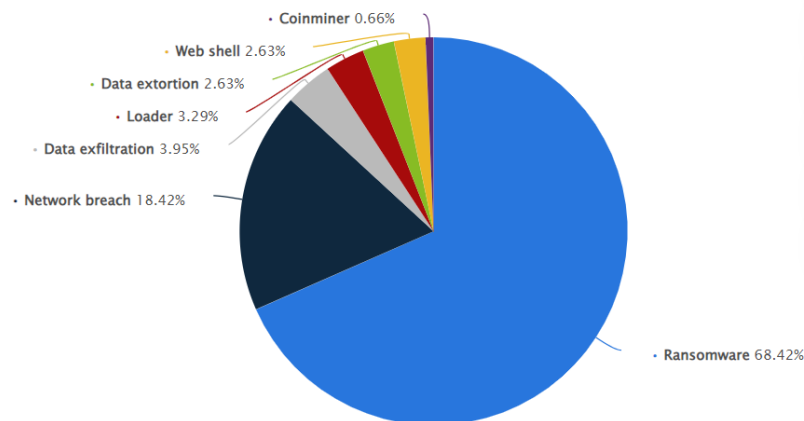
A 2. ábrán a 2022-es évben észlelt kibertámadások típusainak megoszlása látható világszerte. Az ábrán kék színnel jelölt cikket megtekintve is jól látható, hogy a zsarolóvírusok teszik ki a támadások több mint 68 százalékát, így a fenyegetés valós.

²⁴ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszerológati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közszerológati Egyetem, Budapest, p. 17. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

²⁵ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszerológati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közszerológati Egyetem, Budapest, p. 17. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

²⁶ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszerológati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közszerológati Egyetem, Budapest, pp. 17-18. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

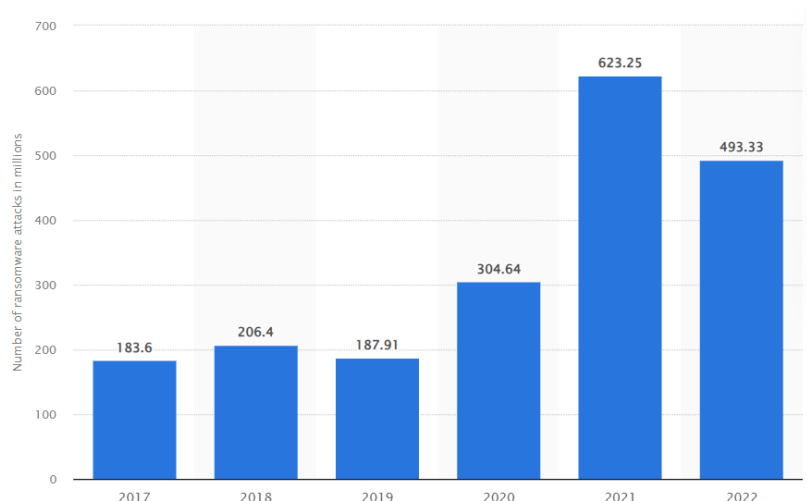
2. ábra: A 2022-es évben észlelt kibertámadások típusainak megoszlása világszerte



Forrás: Statista, <https://www.statista.com/statistics/1382266/cyber-attacks-worldwide-by-type/> (letöltés ideje: 2023. 10. 27.)

A 3. ábrán a zsarolóvírus-kísérletek éves száma (millióban) tekinthető meg világszinten. A statisztikán jól látható, hogy a 2021-es évre jelentős mértékben nőtt a zsarolóvírusok száma, tulajdonképpen megkétszereződött. Habár a 2022-es évre csökkent ez a szám, de még mindig nagyon magasnak mondható.

3. ábra: A zsarolóvírus-kísérletek éves száma világszerte 2017-től 2022-ig (millióban)



Forrás: Statista, <https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide/> (letöltés ideje: 2023. 10. 27.)

3. Kiberkémkedés

Míg a kibertérben véghez vitt tevékenységek elemzése a nemzetközi jog szempontjából viszonylag előrehaladott, a valóságban nem feltétlenül érezhető hatása. A kiberkémkedés gyakorlata, azaz a hírszerzési célú elektronikus rendszerekben történő információtárolás támadása szinte mindennapi az államok számára, miközben a nemzetközi jogban nincs erre vonatkozó ellenőrzés. Ennek eredményeként nem meglepő, hogy a szakmai közvélemény főként hírszerzési incidensekkel találkozhatott csak a kibertérben. Ezek az akciók már az 1990-es években megkezdődtek, ilyen volt például a vélhetően Oroszország által indított Moonlight Maze projekt. Ez azért is érdekes, mivel az Egyesült Nemzetek Szervezete kibertérbeli tevékenységeinek szabályozását elsőként Oroszország kezdeményezte 1998-ban. Mindez arra utal, hogy a nagyhatalmak, legfőképp Oroszország és az Egyesült Államok az 1990-es évek végén már alkalmazták a kiberteret titkos hírszerzési műveletekre. Ide sorolható azonban Kína is, hisz az állam az első ilyen jellegű műveletét 2003-ban bonyolította le, Titan Rain néven, ebből pedig következtethetünk arra, hogy már az 1990-es évek végén megkezdődött részükről is a képességfejlesztés. Emiatt a nemzetközi kapcsolatokat érintő kibertevékenységek már azelőtt is az állami gyakorlatok részét képezték, hogy a nyilvánosságnak tudomása lett volna róla. Mára az információs technológia kiterjedésével a hírszerzés még nem volt olyan egyszerű, mint napjainkban.²⁷

Mivel manapság elsősorban digitális formában tárolják, továbbítják és dolgozzák fel az információkat, a hírszerzési tevékenységgel foglalkozó szakemberek dolga a releváns információkat tartalmazó számítógépek megtalálása. Ezek felkutatásához pedig az esetek nagy részében nincs szükség arra, hogy a hírszerző elhagyja saját országát, hiszen a kibertér határok nélkülsége lehetővé teszi, hogy a határok átlépése nélkül hozzáférjenek a keresett információkhoz. A helyzetet leegyszerűsíti a már nyilvánosan hozzáférhető információk tömkelege. Az olyan platformok pedig, mint a Facebook vagy a Google-szolgáltatások, lehetővé teszik az emberekről, intézményekről, eseményekről szóló szinte minden információ begyűjtését.²⁸

²⁷ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszerológati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közszerológati Egyetem, Budapest, p. 23. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

²⁸ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszerológati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közszerológati Egyetem, Budapest, p. 23. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3>

Az államok által kezdeményezett kiberkémkedés és a nemzetközi jog közötti összefüggésben Buchan úgy vélekedett, hogy nincs egyetlen megállapodás sem, amely szabályozná a kémkedés ezen fajtáját, és nincs egyetlen olyan egyezmény sem, amely közvetlenül alkalmazható lenne erre, legfőképp békeidőben. A nemzetközi jog viszont az államok egyenjogúságából ered, ami azt jelenti, hogy ez a cselekmény ütközhet a nemzetközi jog által kitűzött normákkal, emellett elmondható az is, hogy a hírszerzők kibertérbeli tevékenységeinek ellenőrzése a nemzetközi kapcsolatokban a szuverenitás perspektívájából történik.²⁹

A területi szuverenitás fogalma a digitális szférában kétféleképpen magyarázható. Egyrészt a kibertér egy olyan virtuális tér, amely nem tartozik egy állam területéhez sem, ugyanilyen például a világűr is. Ebben az összefüggésben a semleges területre vonatkozó jogot kell alkalmazni. Egyes országok (például Oroszország és Kína) viszont kinyilvánították, hogy szuverenitást kívánnak gyakorolni saját virtuális terük felett, ezért ma már hasonlóképp kezelik ezt a mesterségesen létrehozott területet, mint a fizikálisat. Ez többek között Magyarországon is így van, 2013-ban fogadták el ugyanis a Nemzeti Kiberbiztonsági Stratégiát, amely kimondja, hogy Magyarország kontrollt kíván szerezni a nemzeti kibertér felett.³⁰

A virtuális tér feletti szuverenitás abból az elképzelésből ered, hogy a kibertér nem is létezne fizikai infrastruktúra, például szerverek, hozzáférési pontok, és más számítógépes összetevők nélkül. Ennek eredményeként, ha ezek az összetevők az ország területén találhatók, a hozzájuk kapcsolódó, a rajtuk tárolt információk megsértésével végzett titkosszolgálati tevékenység sértheti az adott állam szuverenitását. Így tehát nem meglepő, hogy egyre több állam igyekszik határokon belül tartani az érzékeny információkat.³¹

nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20IBTV.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3 (letöltés ideje: 2023.09.25.)

²⁹ Buchan, Russell (2016): The International Legal Regulation of State-Sponsored Cyber Espionage. In: Osula, Anna-Maria – Rõigas, Henry (Eds.): International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn, pp. 65–86. https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch4.pdf (letöltés ideje: 2023. 09. 26.)

³⁰ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közsolgálati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közsolgálati Egyetem, Budapest, pp. 24-25. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20IBTV.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

³¹ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára Nemzeti Közsolgálati Egyetem, Budapest, p. 25. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20IBTV.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

Előfordul azonban, hogy nem könnyű az információkat határokon belül tartani. A felhőszolgáltatók jelentik az egyik legnagyobb kihívást, hiszen ebben az esetben a szolgáltatók adatközpontjai közötti folyamatos adatszinkronizálás miatt továbbra sem lehet biztosra menni azzal kapcsolatban, hogy az információ mely államban található. Az adatátvitelt érintő támadásokra azonban még mindig nem találtak megoldást. Az internet működtetésére használt routing protokoll felel a megbízható adatkapcsolatokért a világhálón, ha efelett megszerzik az irányítást, úgy könnyű átirányítani az adatokat egy másik országba. 2017-ben is történt egy ilyen eset, mégpedig a Facebook, a Google, és a Microsoft szervereit támadták meg, és három percen keresztül minden adatot Oroszország felé irányítottak. Feltételezések alapján ezalatt a három perc alatt az orosz hírszerző ügynökségek hozzáfértek az Egyesült Államok IT-óriásainak teljes forgalmához, ezek pedig nagyon értékes információnak számítanak, annak ellenére, hogy titkosítva voltak, és valószínűleg nem is képesek teljesen dekódolni azokat.³²

Ebben az esetben a területi szuverenitás nem jön létre. A nemzetközi jogban megfogalmazott be nem avatkozás elve viszont érvényesül, hiszen célja az, hogy az államok szuverenitását minden külső beavatkozástól megóvja. A be nem avatkozás elvének megsértését követi el egy ország, amikor olyat cselekszik, ami negatívan érinti egy másik ország szuverén jogait.³³ Buchan ezt a kibertérre kivetítve úgy magyarázza, hogy ha egy állam titkosnak minősített információkat tárol vagy oszt meg egy másik ország felhőszolgáltatásában, akkor ezeket az adatokat az ország szuverenitásának részeként kell kezelni, abban az esetben, ha az információk az adott ország közfeladatainak ellátását segítik elő. Ha viszont például információszerzés céljából behatolnak egy állam külföldi képviselteinek információs rendszereibe, az már sérti a be nem avatkozás elvét.³⁴ Az ilyen jellegű támadások pedig gyakran mondhatóak. A kelet-európai térségben pedig különösen sok ilyen eset történt a 2010-es években, amikor is nagy számban támadták meg a nagykövetségek informatikai rendszereit. Többek között a WhiteBear

³² Goodin, Dan (2017): "Suspicious" event routes traffic for big-name sites through Russia. <https://arstechnica.com/information-technology/2017/12/suspicious-event-route-traffic-for-big-name-sites-through-russia/> (letöltés ideje: 2023. 09. 26.)

³³ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszerződési Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közszerződési Egyetem, Budapest, p. 25. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

³⁴ Buchan, Russell (2016): The International Legal Regulation of State-Sponsored Cyber Espionage. In: Osula, Anna-Maria – Rõigas, Henry (Eds.): International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn, pp. 65–86. https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch4.pdf (letöltés ideje: 2023. 09. 26.)

csoport is ennek szenteli tevékenységeit, kifejezetten Oroszországot szeretnék kiszolgálni ezen intézmények információival.³⁵

További feltétel a kényszer alkalmazása. Ez tulajdonképpen azt jelenti, hogy egy állam olyan tevékenységben vesz részt, amelyre egy másik ország kényszerítette, és ami jogszabályait és állami feladatainak ellátását akadályozza. A nyilvános kiberbiztonsági incidensek sorában erre már nehezebb példát találni, mivel természetüknél fogva csak később kerülnek nyilvánosságra. Mindaddig azonban, amíg az efféle eseteket nem dokumentálják, és a Nemzetközi Bíróság sem nyilatkozik azokról, addig csak elméletben következtethetünk arra, hogy a kiberkémkedés bizonyos helyzetekben sértheti a nemzetközi jogot.³⁶

Gyakorlatban viszont elmondható, hogy ez a kellő erőforrással bíró országok napi rendjéhez tartozik, amelyet nem korlátoz semmilyen nemzetközi szabályrendszer. Ebből kifolyólag pedig az államok közötti titkos információgyűjtés nagyon is gyakori, mégpedig a saját hazájukból indítva ezeket a műveleteket. Ezzel szemben a titkosszolgálati ügynökök jellemzően terepen tevékenykednek, ami azt jelenti, hogy a célország területén hajtanak végre támadásokat az információs rendszerek ellen. Ennek oka, hogy gyakran a célba vett rendszerek el vannak szigetelve a nyílt virtuális tértől, és zárt hálózaton működnek, emiatt pedig szükségessé válik a fizikai hozzáférés. A szokásjog alapján az államok igyekeznek megakadályozni ezeket a tevékenységeket, vagy legalábbis mérsékelni próbálják őket, például hamisított információkkal.³⁷

Összességében tehát, a kibertér létrejötte új kapukat nyitott meg a hírszerzés számára, ezzel együtt pedig az információk sokkal inkább veszélybe kerültek, ami azért lehet aggasztó, mivel ezek az adatok rossz kézbe kerülve súlyos következményeket vonhatnak maguk után, ilyen lehet az is akár, ha titkos állami információk megszerzése után közzéteszik bármilyen médiában, ami által egy állam sebezhetővé válhat, illetve belpolitikai ellentéteket szülhet.

³⁵ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közsolgálati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közsolgálati Egyetem, Budapest, p. 25. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

³⁶ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közsolgálati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közsolgálati Egyetem, Budapest, pp. 25-26. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

³⁷ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közsolgálati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közsolgálati Egyetem, Budapest, p. 26. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

4. Nemzetközi szervezetek a kibertérben

4.1 Az Egyesült Nemzetek Szervezete

Az Egyesült Nemzetek Szervezete (ENSZ) 1945-ben, a második világháborút követően létrejött univerzális szervezet. A tagországok célja a nemzetközi béke és biztonság előmozdítása, az államok közötti barátságos kapcsolatok ápolása, illetve az emberi jogok és az életszínvonal javítása.³⁸ A 193 tagország folyamatos tárgyalásai elősegítik, hogy a fejlett országok előtt álló kihívások is feltárulhassanak. Ezért van nagy jelentősége az ENSZ tevékenységének a kiberbiztonságban.³⁹

Az ENSZ a 2000-es évek kezdete óta alapvető céljának tekinti az infokommunikáció kiterjesztését. Az évezred elejétől egészen 2015-ig tartó időszakra a tervezett Millenniumi Fejlesztési Célok (MDG) egyik pontja az új technológiához való hozzáférés elősegítése volt. Ezeket a fejlesztési célokat követte a 2030-ig kitűzött újabb tervezet, az Agenda for Sustainable Development (SDG) program, amely 17 fenntartható fejlődési célt határoz meg. Habár ebben közvetlenül nem lettek megfogalmazva információtechnológiához köthető célok, de mindegyik cél megvalósításához szükséges lehet. Ezzel együtt kijelenthető, hogy az informatika a jólét alapja, így az informatika biztonságossá tétele nagyon is fontos.⁴⁰

Az ENSZ kiberbiztonsággal kapcsolatos erőfeszítései két elsődleges irányt vettek. A szervezetnél 1998-ban kezdődtek meg a kiberbiztonsággal kapcsolatos érdemi tevékenységek, amikor is az orosz vezetés kérte a Közgyűlést támogató Első Bizottságot, amely a Leszerelési és Nemzetközi Biztonsági Bizottság nevet kapta, hogy foglaljanak állást a kiberhadviseléssel és kiberbűnözéssel kapcsolatosan. Oroszország és az Egyesült Államok nézetei között már ekkor kialakultak eltérések. Az Egyesült Államok kiterjedtebb összefogást várt a kiberbűnözés kapcsán, ám ez orosz nézőpont szerint sértette volna az alkotmányukat, mert a nemzetközi hatóságok vizsgálnák az állam kibertérbeli tevékenységét. Oroszország így olyan kérelmet nyújtott be, amely korlátozná a kibertérben használt fegyvertípusokat, az amerikaiak viszont erről úgy vélekedtek, hogy az Orosz Föderáció célja ezzel az lenne, hogy megakadályozza az erőegyensúly felbomlását, az Egyesült Államok előnyére. Egy másik vitatott terület a Biztonsági Tanács két tagja között az online szólásszabadság. Az orosz kormányzat úgy véli,

³⁸ ENSZ. Általános információ az ENSZről. www.unis.unvienna.org/unis/hu/topics/un-general (Letöltés ideje: 2023. 09. 05.)

³⁹ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszerológati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közszerológati Egyetem, Budapest, p. 10. <https://nkerpo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

⁴⁰ u.o.

hogy ez politikai instabilitáshoz vezethet az országban. Ezzel az állásponttal Kína is egyetért, habár az ázsiai ország jellemzően kevészer nyilvánította ki véleményét az országok közötti vita során.⁴¹

4.2 A Nemzetközi Távközlési Egyesület (ITU)

A Nemzetközi Távközlési Egyesület (ITU) az ENSZ infokommunikációs technológiára szakosodott szervezete. Jelentős szerepe van műholdak pályáinak kezelésében, a spektrumgazdálkodásban, illetve hatáskörébe tartozik az infokommunikációra vonatkozó szabványok kezelése, és az internet globális elérésének elősegítése. 193 tagországa és több mint 800 tagja van a magánszektorban és a tudományos területeken. Genfben található a székhelye.⁴²

Szakosított intézményként az ITU elsősorban a kibertérhez kapcsolódó technikai aggályok kezeléséért felel, emellett a kiberbiztonság fenntartásában is nagy szerepe van. Korábban már említésre került, hogy az infokommunikációs technológiák kulcsfontosságúak az ENSZ Fenntartható Fejlődési Céljainak elérésében. Az ITU kínál teret a World Summit on the Information Society (WSIS) keretein belül 2004 óta évente az SDG-k és a technológia közötti kapcsolat megvitatására, ahol állami és nem állami szereplők is részt vesznek.⁴³

4.3 Az Európai Biztonsági és Együttműködési Szervezet (EBESZ)

Az Európai Biztonsági és Együttműködési Szervezet a legkiterjedtebb nemzetközi szervezet, amely kizárólag biztonsággal foglalkozik, de elsősorban a „soft security”, tehát a nem katonai biztonság területén. Célja a fegyverek szabályozása, az emberi jogok előmozdítása, a sajtószabadság ellenőrzése, és a választások integritásának felügyelete. A Titkársága Bécsben ülésezik. Tagjai elsősorban európai országok, de több, európai biztonságra befolyást gyakorló ország, a korábbi Szovjetunió néhány tagországa is tagja, illetve 11 társult országgal is rendelkezik. Létrejötté egészen 1973-ra vezethető vissza, amikor is megtartották az Európai

⁴¹ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszerológati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közszerológati Egyetem, Budapest, pp. 10-11. <https://nkerpo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20feles%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

⁴² ITU általános története: <https://www.itu.int/en/history/Pages/ITUsHistory.aspx> (letöltés ideje: 2023.10.20.)

⁴³ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszerológati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közszerológati Egyetem, Budapest, pp. 11-12. <https://nkerpo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20feles%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

Biztonsági és Együttműködési Értekezletet (CSCE). Jelenlegi felépítése 1995 óta áll fenn, az 1994-es budapesti kongresszus eredményeként.⁴⁴

Az EBESZ kiberbiztonsághoz kapcsolódó tevékenysége rendkívül fontosnak számít a kibertér biztonságának megtartásában, ugyanis az EBESZ-szel kötött megállapodások, szabályozások önkéntesek, és főként politikai elkötelezettséggel hozhatóak összefüggésbe, így a tagországoknak több mozgástere van, mint többek között az ENSZ-ben. Ezeket confidence building measure-nek (CBM) nevezik, amelyek eredeti célja a hidegháborúval kapcsolatos feszültség csökkentése volt. A kibertérben végzett tevékenységek eredendően ugyanolyan pusztítóak lehetnek, mint az atomfegyverek használata, így a CBM-ek hasznosak lehetnek az kiberkonfliktusok elterjedésének elkerülésében, már csak azért is, mert az államok kibertérben történő erőszak alkalmazásához való joga még mindig nem teljesen meghatározott.⁴⁵

⁴⁴ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszerológati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közszerológati Egyetem, Budapest, p. 13. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

⁴⁵ Krasznay Csaba (2020): Nemzetközi kapcsolatok a kibertérben, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszerológati Egyetem Közigazgatási Továbbképzési Intézet, Nemzeti Közszerológati Egyetem, Budapest, pp. 13-14. <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3> (letöltés ideje: 2023. 09. 25.)

5. A kiberdiplomácia

5.1 A kiberdiplomácia fogalma

A kiberdiplomácia számos definícióval jellemezhető, ezek közül a tudományos körökben leginkább elfogadott André Barrinha és Thomas Renard megfogalmazása, miszerint a kiberdiplomácia a kibertérrel kapcsolatos diplomácia, vagy a digitális erőforrások hasznosítása és a digitális világban lévő diplomáciai feladatok ellátása a nemzetek érdekének védelmében.⁴⁶ A kiberdiplomácia sikerességéhez kapcsolódó célok és érdekek a kiberbiztonsági stratégiákban kerülnek kifejtésre. A kiberdiplomácia legjelentősebb résztvevői a mindenki által ismert, hagyományos diplomaták, valamint az e területen jelentős szerepet betöltő intézmények, szervezetek és ügynökségek szereplői.⁴⁷ Napjainkban a nagyhatalmak között egyre nagyobb feszültség észlelhető a kibertérbeli cselekményekkel kapcsolatban, így egyre nagyobb szükség van nemzetközi tárgyalások folytatására és az efféle konfliktusok rendezésére vonatkozó megállapodások megkötésére.⁴⁸

Ahhoz, hogy megérthessük a kiberdiplomácia fogalmát, először is egy kitérőt szükséges tenni a tradicionális diplomácia megismeréséhez. A diplomácia fő szereplői az államok és a nemzetközi szervezetek. Az országok a nemzetközi organizálódás fő alkotói, alapvető szereppel rendelkeznek a nemzetközi kapcsolatok alakításában. A diplomácia az országok közötti kapcsolatok fenntartása, ápolása, valamint a nemzetközi jog meghatározása szerint az államok és nemzetközi szervezetek közötti kapcsolatok békés, tárgyalás alapú rendezésére szolgál. Összességében a kiberdiplomácia alapvetően úgy értelmezhető, mint a kibertérben folytatott diplomácia, de természetesen ennél sokkal összetettebb. Habár a kiberdiplomáciának több tudományos definíciója is van, egyelőre nem sikerült konszenzusra jutni meghatározásával kapcsolatban a tudományos körökben. A fogalom viszont meglehetősen új, és főként az angolszász akadémiai területen van jelen, leginkább az Egyesült Államok által, amely országról elmondható, hogy a kiberdiplomácia területén vezető szerepet tölt be.⁴⁹

Fontos elkülönítenünk továbbá a kiberdiplomáciát a digitális diplomáciától, hiszen a kettő nem azonos. Habár bizonyos tekintetben hasonlítanak, mégis eltérő meghatározással

⁴⁶ Barrinha, André – Renard, Thomas (2017): Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, 3(4–5), p. 3.

⁴⁷ u.o

⁴⁸ Renard, Thomas (2018): EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society*, 19(3), pp. 321–337.

⁴⁹ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, *Információ- és kiberbiztonság*, Ludovika Egyetemi Kiadó, Budapest, pp. 309-310. https://nkerpo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

magyarázhatóak. A digitális diplomácia különbözik a kiberdiplomáciától, viszont az e-diplomáciával egyenlőnek mondható. Míg a kiberdiplomácia a külpolitikával áll összefüggésben, amelyet egy speciális térben, a kibertérben folytatnak, úgy a digitális diplomácia a valódi diplomáciai tevékenységeket foglalja magában. Az előbbire megfelelő példa egy nemzeti álláspont megtárgyalása vagy kinyilvánítása egy nemzetközi szerződés kapcsán az internet felhasználásáról, az utóbbira pedig példa lehet egy ország külügyminisztériumának üzenete, gratulációja egy másik állam felé valamilyen közösségi média platformon. Tehát az e-diplomácia az infokommunikációs eszközök használata a diplomáciában, a kiberdiplomácia pedig konfliktuskezelésre, a kibertérbeli megállapodásokra és a kapcsolódó politikákra vonatkozik.⁵⁰

Mint ahogy a politika világában általában, a kibertér szabályozására vonatkozó javaslatok tekintetében sincs egyetértés az országok között. Nincs konszenzus a kibertér irányításának és szabályozásának módját illetően sem, emiatt viszont eddig nemigen volt sikeres az előrelépés. Az államok évek óta tárgyalnak a kibertérre vonatkozó jogszabályokról, de továbbra is jellemzőek a nézeteltérések. Az államok azonban nemcsak önállóan folytathatnak kiberdiplomáciát. Két- vagy többoldalú szerveződések, szövetségek keretében is végezhető, attól függően, hogy milyen érdekeik és közös nézeteik vannak.⁵¹

Az Egyesült Államok, az Észak-atlanti Szerződés Szervezete (NATO) és az Európai Unió tagállamai alapvetően azt támogatják, hogy a kibertér szabad, biztonságos, demokratikus és jogállamiságon alapuló rendszer szerint működjön. A nyugati megközelítés alapján a kibertér demokratikusságának garantálása az állam, a kormányzat és a civil társadalom együttes felelőssége, a nemzetközi jogot pedig tiszteletben kell tartani a diplomácia ezen terén is. A szabályokon alapuló multilaterális vélekedés mintájaként a NATO tagállamai a Tallini Kézikönyvben⁵² olyan iránymutatásokat fogalmaztak meg, amelyek segítik az államok és nem állami résztvevők számára a kibertérben való helyes eljárások megismerését. Ebből tehát

⁵⁰ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 310. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁵¹ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 310. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁵² NATO (2017): Tallin Manual 2.0. On The International Law Applicable To Cyber Operations, Cambridge University Press

következtethetünk arra, hogy a NATO-tagállamok egyetértenek a kibertér államoktól független ellenőrzésével kapcsolatban.⁵³

A nyugati államok álláspontjával ellentétben Oroszország, Kína és néhány fejlődő ország (pl. Irán, Észak-Korea) támogatja az országok hagyományos szuverenitásának kibertérre való bővítését, és kifejezetten ellenzi az együttműködést ezen a téren. Véleményük több pontban is eltér, többek között úgy gondolják, hogy a hadviselésről szóló nemzetközi jognak nem kellene a kibertérre vonatkoznia. Mivel ezek a megközelítések szöges ellentétben állnak egymással, a kiberdiplomácia által kínált békés módszerek nélkül a kibertér használata eredményének a kibertámadások, és esetleges kiberháborúk tekinthetők.⁵⁴

A kiberdiplomácia definíciójának megértése során a céljai is fontos kérdésnek számítanak. A kiberdiplomáciával foglalkozó szakirodalom három fő csoportra osztható annak mentén, hogy a nemzetközi kapcsolatok elméletének mely fő tanát követik a kutatók. Az első csoportba azok a tudósok sorolhatóak, akik a kiberdiplomácia és a hatalom közötti kapcsolatokkal foglalkoznak (pl. Nye⁵⁵). A második fő csoport (pl. Kosseff⁵⁶) a kölcsönösséget hangsúlyozza, gyakran törvényekre és jogi megállapodásokra összpontosítva. Végül az utolsó csoport (pl. Schmitt⁵⁷) a kiberdiplomácia legfontosabb szempontjának a viselkedéshez, normákhoz való kapcsolódást tekinti. Ezek a csoportok a realizmust, liberalizmust, konstruktivizmust követik, ezáltal pedig ezt a három fő megközelítést alkalmazzuk a kibertér és kiberdiplomácia területén. A megközelítések a normákra, kölcsönösségre, hatalomra összpontosítanak, de a kérdés az, hogy az államközi kapcsolatokban mely eszmék fognak jobban érvényesülni és sikerül-e a kibertér szereplőinek konszenzusra jutniuk ezzel kapcsolatban.⁵⁸

⁵³ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 311. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁵⁴ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 311. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁵⁵ Nye, Joseph S. (2011): Nuclear Lessons From Cyber Security? Strategic Studies Quarterly, Vol 5. No. 4. pp. 18-31.

⁵⁶ Kosseff, Jeff (2017): Cybersecurity Law, John Wiley & Sons Inc., Hoboken, pp. 269-286.

⁵⁷ Schmitt, Michael N. – Vihul, Liis (2016): The Nature of International Law Cyber Norms. In: Osula, Anna-Maria – Rõigas, Henry (Eds.) International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn, pp. 23–48. https://www.ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch2.pdf (letöltés ideje: 2023. 09. 25.)

⁵⁸ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 314. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

A realisták a kiberdiplomáciát a háborúzás kiegészítőjének tekintik. A csoport szerint a kiberdiplomácia a katonai törekvések kontextusában értelmezhető a legjobban, ugyanis ezt az államok védelme mellett végzett cselekedetek sorozatának tekintik. A kiberdiplomácia ezen felfogása hagyományos kérdésekre fókuszál, mint például a gazdasági és katonai hatalom. Ezen elképzelések elemei a realista irodalomban más téren is megjelennek. A kutatók azt állítják, hogy a hatalom szerepe a kiberdiplomácia területén rendkívüli jelentőséggel bír, legfőbb erőforrásai pedig a katonai eszközök. A realista kutatók (pl. Jørgensen⁵⁹) a kiberdiplomáciára az erőszak alkalmazásának kiegészítőjeként tekintenek. Kutatásaik során kiemelt figyelmet fordítottak az olyan fogalmakra, mint a kibernelrettetés, a kibervédelem és a kiberkényszer, és úgy vélik, hogy a kiberdiplomácia rendkívül hasonló a nukleáris diplomáciához.⁶⁰

A liberális megközelítés a kölcsönösségre, egymásrautaltságra, valamint a nemzetközi szervezetek és államok közötti jogi szerződésekre helyezi a hangsúlyt. A liberalista nézet (pl. Eriksson⁶¹) a kiberdiplomácia katonai erővel szemben betöltött kiemelkedő szerepére összpontosít a kibervilág irányítása és kiberbiztonság növelése érdekében. A szakirodalom felülvizsgálja a gazdasági függőség alapelveit, a nemzetközi szervezetek szerepét és a békeelméletet.⁶²

Az utolsó csoport, a konstruktivisták csoportja a normák társadalmi konstrukcióinak jelentőségét hirdetik a kiberdiplomácia vizsgálatában. A szakértők vizsgálatai itt elsősorban nem a kibertámadásokra vagy azok előfordulására vonatkoznak, hanem azt igyekeznek megérteni, hogy miért következnek be a támadások.⁶³ A konstruktivizmust valló kutatók (pl. Cavelt⁶⁴) feltételezése szerint a normák hatással lehetnek a kibertámadások gyakoriságára. A nemzetközi szintén, beleértve a kibertérre is, léteznek normák az állami cselekvések szabályozására. Az egyes normák befolyásának mértéke azonban államonként eltérő. Ez a

⁵⁹ Jørgensen, K. E. (2010). *International Relations Theory: A New Introduction* p.84

⁶⁰ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 314. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁶¹ Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR) relevant Theory? *International Political Science Review*, 27(3), 221-244.

⁶² Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 315. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁶³ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 315. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁶⁴ Cavelt, M. D. (2010). Cyberwar. In G. Kassimeris & J. Buckley (Eds.), *The Ashgate Research Companion to Modern Warfare* (pp. 123-144)

sajátos megközelítés azt állítja, hogy a nemkormányzati szervezetek (NGO-k) és az egyének gyakorolják a legjelentősebb hatást. Valójában eszerint a felfogás szerint a normák az állami magatartás elsődleges tényezői.⁶⁵

A három álláspont jelentős különbséget mutat a kiberdiplomácia megértésében. Az eltérések ellenére a mindennapi politikára is jelentős hatást gyakorol, hiszen a kiberdiplomácia digitális szférában betöltött szerepét vizsgáljuk. Amennyiben a realista filozófia az elsődleges, akkor az országok nemzetközi felügyelet nélkül, lényegében megőrzik szuverenitásukat a kibertér felett, ahol igyekeznek érdekeiket képviselni. A liberalista nézet a kiberdiplomáciát egy nemzetközi jogon és intézményeken alapuló rendszernek tekinti, ahol az államok legalizált, nemzetközi egyezmények által meghatározott szerepek keretein belül vesznek részt. Úgy vélekednek, hogy ellentmondásos esetekben a jog a nyomásgyakorlás leghatékonyabb formája, nem pedig az erőszak, és javasolják, hogy az ilyen ügyekre koncentráló „kiberbíróságot” hozzanak létre. A konstruktivisták álláspontja szerint nem a jogi légkör, illetve a nemzetközi szervezetek jelenléte vagy hiánya az, ami elsősorban az államok kiberdiplomáciai magatartását befolyásolja, hanem sokkal inkább az államok között elterjedt magatartási vagy erkölcsi minták.⁶⁶

Például az Egyesült Államokban jellemzően realista filozófia van, amennyiben republikánus vezetés van, és liberálisabb, amennyiben demokrata vezetés alatt áll az ország. Más államokat, például Oroszországot, amely továbbra is támogatja egy széleskörű, az ENSZ által támogatott, de Kína nemzeti hatalmát nem csökkentő szerződés megkötését, a valósággal összhangban állónak tekintik. Mivel nincs egyetemes megállapodás a nagyhatalmak között, várhatóan az Egyesült Nemzetek Szervezete lesz az egyetlen hivatalos szervezet, amely a kiberdiplomáciával foglalkozik.⁶⁷ A kiberdiplomácia terén az Egyesült Nemzetek Szervezetének két fő szerve is jelentős szerepet játszik. E kettő a Biztonsági Tanács, valamint a Nemzetközi Titkárság.⁶⁸

Az ENSZ Biztonsági Tanácsában a kiberdiplomáciával kapcsolatos ügyek 1998-ban kerültek először napirendre. Ekkor Oroszország az ENSZ Biztonsági Tanácsának állandó tagja, egy

⁶⁵ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 315. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁶⁶ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 315. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁶⁷ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, pp. 315-316. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁶⁸ ENSZ. Általános információ az ENSZről. www.unis.unvienna.org/unis/hu/topics/un-general (Letöltés ideje: 2023. 09. 05.)

olyan javaslatot nyújtott be, amely megtiltaná az elektronikus fegyverek használatát. Az ENSZ főtitkára szintén önálló szereppel bír a tagállamok tekintetében. A főtitkár kormányzati tudományos csoportot (Egyesült Nemzetek Kormányzati Szakértői Csoportja) hozott létre, amely 2004 óta látja el feladatát, valamint létrehozott egy OEWG-ot (open ended working group) is, amely számtalanszor foglalkozott a témakörrel. Ezen csoportok léte és működése azt sugallja, hogy a rengeteg megoldatlan kérdés ellenére az Egyesült Nemzetek Szervezete, mint fórum még mindig az első kísérlet helyszíne a vitatott kérdések megoldására.⁶⁹

⁶⁹ Mártonffy Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 316. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

6. Nagyhatalmak a kiberdiplomáciában

A világ vezető hatalmai a biztonság minden területére jelentős hatást gyakorolnak, ez igaz a kiberbiztonságra is. Manapság azonban nincs egyetértés azzal kapcsolatban, hogy hogyan kellene az államok kibertérben szükséges magatartását és szabályait rögzíteni. A legfontosabb kérdés ezzel kapcsolatban az, hogy valóban szükséges-e létrehozni egy nemzetközi egyezményt a dimenzió használatával kapcsolatban. Ez valószínűleg nem tud bekövetkezni a nagyon gyors technológiai fejlődés okozta új akadályok, illetve az egyezményben foglaltak végrehajtása nyomán követésének nehézségei miatt. Ehelyett az államok az informális partnerséget és a stratégiai megelőzést tartják a leghatékonyabb eszköznek. Ugyanakkor egy fegyverkorlátozásról szóló nemzetközi szerződés megalkotása szükséges lenne, és példaként hivatkozhatunk a sikeresnek mondható 20. századi fegyverkorlátozási egyezményekre. Vélhetőleg egy nemzetközi kiberkormány megkönnyítené az elsődleges kérdések megvitatását az államok számára, és hozzájárulhatna a hatékony kibervédelemhez.⁷⁰

A kiberkormányzattal szemben számos ellenérv felhozható.⁷¹ Egyrészt a kiberfegyverek tulajdonságai miatt nem lehetséges megfigyelő és kényszerítő mechanizmusokat beépíteni. Ennek oka, hogy az ellenőrzést a fegyverfejlesztés időszakában kellene elkezdni és nem pedig magának a fegyvernek a használatakor.⁷² További szempont, hogy a tárgyalások nagyon elhúzódnának, illetve a gyors technológiai fejlődéshez nem minden állam tud alkalmazkodni, így túl korai lenne formális egyezményt alkotni. Ráadásuk csak a valóban elkötelezett országok vennének részt egy ilyen egyezményben, számukra a kényszer a részvétel egy formája lenne. Lehetséges, hogy a kiberrezsím lazább szabályozási keretek között tudna csak felépülni a hagyományos struktúrákhoz képest. Ebben az esetben fontos szerepet játszana a bizalom kiépítését szorgalmazó intézkedések sora, erre jó példa lehet az EBESZ és az ASEAN, vagyis a Délkelet-ázsiai Nemzetek Szövetsége gyakorlata is az elmúlt évtizedből.⁷³

⁷⁰ Molnár Dóra (2020): Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 357. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁷¹ Nabeel, Fahrad (2018): International Cyber Regime: A Comparative Analysis of the US-China-Russia Approaches. Strategem Vol. 1, No. 2, pp. 8–27. www.academia.edu/38296708/International_Cyber_Regime_A_Comparative_Analysis_of_the_US-China-Russia_Approaches (letöltés ideje: 2023. 10. 20.)

⁷² Eilstrup-Sangiovanni, Mette (2018): Why the World Needs an International Cyberwar Convention. Philosophy & Technology, 30(3), p. 399.

⁷³ Molnár Dóra (2020): Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 357. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

Az Obama-kormányzat kibertérre vonatkozó új nemzetközi politikájának bejelentését követően az Egyesült Államok a vezető nemzet lett az EBESZ kibertérrel kapcsolatos terveinek segítésében. A szervezet kiberalapját és kiberbiztonsági stratégiai megközelítését a Biztonsági Együttműködési Fórum és az Állandó Tanács ülésén, 2010-ben alakították ki. Az Egyesült Államok javasolta az univerzális szabályok megvitatását, egy évvel ezután pedig a bizalomépítéshez szükséges intézkedések kidolgozását. Ezenkívül az USA és az Orosz Föderáció tárgyalásokat kezdeményezett a kiberbiztonság megteremtéséhez szükséges kezdeti intézkedésekről⁷⁴, majd ezeket az intézkedéseket 2013-ban egy megállapodásban rögzítették. Az egyezmény alapvető elemei az alábbiak:⁷⁵

- kommunikációs csatornák létrehozása a CERT-tek (Computer Emergency Response Team, azaz számítógépes vészhelyzeteket ellátó csoport) között és az információmegosztási megállapodás lezárása a fontos információs rendszerek megőrzése érdekében;
- közvetlen kommunikációs csatorna használatának lehetővé tétele az országok nukleáris kockázatsökkentő központjai között (az USA Washingtonban található Külügyminisztériuma és a Moszkvában található orosz Védelmi Minisztérium között);
- közvetlen telefonos kapcsolat létrehozása az amerikai kiberbiztonsági vezetés és Oroszország Biztonsági Tanácsának főtárhelyettese között;
- egy hónapon belül az infokommunikációs technológia veszélyeivel foglalkozó munkacsoport felállítása.

Ami az EBESZ-en belül kialakítandó irányelveket illeti, minden állam különböző kezdeményezéseket javasolt. Németország a bizalomépítéshez szükséges intézkedéseket két nagy csoportba sorolta: az egyik az átláthatóságra, a másik a stabilitásra fókuszál. Míg az első a kockázatsökkentést és az információcserét (a nemzetközi joggal, szervezeti struktúrákkal, stratégiákkal és partnerekkel kapcsolatos intézkedések) tartotta iránymutatónak, addig a másik az egységes kibergyakorlatot, valamint a válságos helyzeteknél alkalmazandó kommunikációs csatornák és a CERT-ek kialakítását vette célba.⁷⁶

⁷⁴ Ziolkowski, Katharina (ed.) (2013): Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, Tallinn, NATO CCDCOE Publication.

⁷⁵ 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

⁷⁶ Cyber security: confidence and security-building measures (CSBMs). Federal Foreign Office website, www.auswaertiges-amt.de/EN/Aussenpolitik/Friedenspolitik/Abruestung/_KonvRueKontrolle/VN-Konventionelle-Abruestung-Ruestungskontrolle_node.html (letöltés ideje: 2023. 10. 20.)

Az Orosz Föderáció listája ennél még kiterjedtebb volt. A 2011-ben megjelent Oroszország információs térbeli fegyveres erőinek tevékenységéről szóló dokumentum (Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space) alapján az erők célja az információs tér katonai alkalmazásával kapcsolatos bizalom körének kialakítása volt. 2012-ben egy új dokumentumban megtörtént az ezzel kapcsolatos lépések összefoglalása. Ide tartozik a nemzeti törvények szabványosítása, az információbiztonság egyetemes fogalmának kidolgozása, a hatóságok közötti együttműködés és intézményi keretek létrehozása.⁷⁷

Mindezek jelentős erőfeszítést jelentenek a nemzetközi közösség számára, azonban egy globális kiberkormány is csak akkor tudna működni, ha minél több állam vállalna szerepet benne. Kulcsfontosságú szereppel bír a vezető hatalmak részvétele a kiberbiztonság megteremtésében, de a rendszer legfontosabb kérdéseit illetően továbbra is jelentős nézeteltérések vannak a nyugati világ és a Kína által vezetett fejlődő országok között. Példaként visszaemlékezhetünk 2018-ra, amikor is több mint 50 állam, valamint magánvállalatok és tudományos szervezetek vettek részt egy nemzetközi konferencián, ahol kiberbiztonságról szóló egyezményt kötöttek, az aláírók között azonban nem volt ott Kína, Oroszország, Észak-Korea, Ausztrália, Szaúd-Arábia, Irán, Izrael, az Egyesült Államok, illetve a két legnagyobb kínai infokommunikációs cég, a Huawei és a ZTE sem.⁷⁸

6.1. Az Egyesült Államok a kiberdiplomáciában

Az Egyesült Államok kiberdiplomáciájának alapját a 2011-ben elfogadott kibertérrel kapcsolatos nemzetközi stratégiájának elfogadása tette le.⁷⁹ A dokumentum megjelenésével az Egyesült Államok kezdeményezte a kiberdiplomácia szabályrendszerének létrehozását, és megteremtette a szervezeti kereteit is. Az okmány tartalmazza a kiberdiplomácia amerikai definícióját, illetve magában foglalja a kibertérrel kapcsolatos amerikai érdekek teljes spektrumát. Többek között nemcsak a kiberbiztonság megteremtését, hanem az internetszabályozást, az internet katonai felhasználását is az innováció és gazdasági növekedés

⁷⁷ Fedosov, Sergey (2012): Statement by the Russian participant at the UNIDIR Cyber Security Conference 'What does a Stable Cyber Environment Look Like? Geneva, UNIDIR. 8–9 November 2012, www.unidir.ch/files/conferences/pdfs/pdf-conf1922.pdf (letöltés ideje: 2023. 10. 20.)

⁷⁸ UK and 50 nations sign cyber security pact. 2018. november 13. www.itproportal.com/news/uk-and-50-nations-sign-cyber-security-pact/ (letöltés ideje: 2023. 10. 23.)

⁷⁹ International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. United States, 2011. május. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf (letöltés ideje: 2023. 10. 21.)

érdekében. Az Egyesült Államok külügyminisztériuma létrehozta a Kiberkoordinátori Hivatalt (Office of the Coordinator for Cyber Issues). A kiberdiplomácia elengedhetetlenné vált az amerikai kormány nemzetbiztonságának megőrzéséhez. Kicsivel több mint hatéves működése során az iroda számos többoldalú partnetkapcsolatot alakított ki szerte a világon kiberügyekkel kapcsolatban.⁸⁰

Több javaslat is született a további kiberdiplomácia fejlesztésének szükségességére vonatkozóan, de a Trump-kormányzat máshogy látta ennek a kérdésnek a jövőjét, így Tillerson külügyminiszter úgy döntött megszünteti a hivatalt. Ezzel a lépéssel nagy űr keletkezett, amit a 2017-ben megjelent elnöki rendeletben⁸¹ előírt új kiberstratégia kihirdetésével próbáltak pótolni, de ennek sikertelensége nagy bizonytalanságot okozott a diplomáciai közösségben. A kiberdiplomáciáról szóló törvényjavaslatot hosszas jogalkotási folyamat követte, ami végül 2019. elején fejeződött be. Az elfogadott dokumentumban az állam egy hozzáférhető, átjárható, megbízható kibertérre kíván létrehozni, más államokkal együttesen. Ennek eredményeként az USA továbbra is a többoldalú együttműködés híve, szemben az Oroszország és Kína által vezetett másik állásponttal, miszerint ezek a nagyhatalmak meg akarják őrizni szuverenitásukat a kibertérben is. Az Egyesült Államok ezt az ellentétet azzal erősíti, hogy kategorizálja azokat az országokat és szervezeteket, amelyek veszélyt jelenthetnek a kibertér biztonságára. Az első helyen Oroszország áll, őt követi Kína, Észak-Korea és Irán, illetve a globális bűnözői és terrorista szervezetek. Emellett az okmány leírja a bilaterális kapcsolatok jelentőségét, valamint a 2014 és 2018 között létrejött kibermegállapodásokat is említi, amelyeket az Egyesült Államok nemzetközi kiberpolitikájának részeként kötöttek. A globális problémák megoldására a nagyhatalom javasolta a Nemzetközi Kiberpolitikai Hivatal (Office of International Cyberspace Policy) felállítását, amely egy olyan központi szerv lenne, amelyet egy, az elnök által kinevezett kibernagykövet felügyelne.⁸²

A jövővel kapcsolatban az egészen biztos volt, hogy nem lesz elegendő az új tervezet és szervezet felállítása sem, amely az ország digitális szférában felmerülő konfrontációira és dilemmáira válaszolna, de a konkrét részletek kidolgozása még folyamatban van. Ha az USA

⁸⁰ Painter, Christopher (2018): The rise of the internet and cyber technologies constitutes one of the central foreign policy issues of the 21st century. The Foreign Service Journal, June 2018, www.afsa.org/diplomacy-cyberspace (letöltés ideje: 2023. 10. 19.)

⁸¹ Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 2017. május 11. www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/, (letöltés ideje: 2023. 10. 19.)

⁸² Molnár Dóra (2020): Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberponton, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 360. https://nkrepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

ezen a téren is sikereket szeretne elkönyvelni magának, kerülni kell a nyílt konfliktust Kínával és Oroszországgal egyaránt, és a világ más nemzetei felé azt kell sugározni, hogy együtt tud működni ezen államokkal. Megoldás lehet viszont, ha az Egyesült Államok meggyőzi az európai, afrikai, dél-amerikai, valamint a közép-, dél-, és délkelet-ázsiai országokat, hogy válasszanak ki régiójukból olyan államokat, akik képviselik területüket a kiberdiplomáciában, és támogatják az Egyesült Államok álláspontját a kibertér szabályozását illetően. Ez ellensúlyozná a kínai és orosz befolyást. Ami biztos, hogy az Egyesült Államoknak nagy szerepe van a kiberdiplomáciai kapcsolatok alakulásában.⁸³

6.2. Kína sikere a kiberdiplomáciában

Kínáról elmondható, hogy az utóbbi években átvette a vezetést a diplomáciában. Ezt nagyon jól szemlélteti az állam diplomáciai hálózatának nagysága, amelyet a globális befolyás egy formájának is tartanak. 2019-re Kínának 276 diplomáciai állomása volt világszerte, ami több, mint az Egyesült Államoké, amely korábban töltötte be a diplomáciai vezető szerepet.⁸⁴ Ez jelentős fordulóponthoz vezet a hatalmi harcokban is, mivel Kína készen áll erejének hasznosítására. Az is kijelenthető, hogy Kína nemcsak kibernagyhatalom, hanem kiber szuperhatalommá is vált.⁸⁵ Ez nem véletlen, ha megvizsgáljuk a kínai elnök 2016-os beszédét, amelyben elhangzott, hogy nincs nemzetbiztonság kiberbiztonság, modernizáció pedig informatizáció nélkül.⁸⁶

A diplomáciai folyamat alapja a 2017 tavaszán megjelent Együttműködés a kibertérben nemzetközi stratégia (International Strategy of Cooperation on Cyberspace)⁸⁷ kiberbiztonsági dokumentum. Már a stratégia neve is arra utal, hogy Kína úgy gondolja, hogy a kibertérben végbemenő konfliktusok megoldásának kulcsa az együttműködésen és a technológia békés felhasználásán alapul, ebben pedig a kiberdiplomáciának fontos szerep jut.

⁸³ Chapman, Justin (2019): Threats and Opportunities of Cyber Diplomacy at PolicyWest. 2019. 12. 24. www.pacificcouncil.org/newsroom/threats-and-opportunities-cyber-diplomacy-policywest (letöltés ideje: 2023. 10. 23.)

⁸⁴ Bley, Bonnie (2019): The New Geography of Global Diplomacy. China Advances as the United States Retreats. 2019. november 27. www.foreignaffairs.com/articles/china/2019-11-27/new-geography-global-diplomacy (letöltés ideje: 2023. 10. 20.)

⁸⁵ Segal, Adam (2018): Year in Review: Chinese Cyber Sovereignty in Action. 2018. január 8. www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action (letöltés ideje: 2023. 10. 18.)

⁸⁶ Xi Jinping gives speech at Cybersecurity and Informatization World Conference. 2016. április 19. <https://chinacopyrightandmedia.wordpress.com/2016/04/19/xi-jinping-gives-speech-at-cybersecurity-and-informatization-work-conference/> (letöltés ideje: 2023. 10. 18.)

⁸⁷ International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. United States, 2011. május. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf (letöltés ideje: 2023. 10. 18.)

Az okmány kimondja, hogy a kibertér jövőjében minden nemzet osztozik, az országok közötti digitális szakadék ellenére a nemzetközi közösségnek továbbra is egy egészként kellene együttműködnie a kölcsönös tisztelet és megértés jegyében, az internet szuverenitásának megőrzése érdekében. A szuverenitást a dokumentum a négy alapelv egyikének tekinti a megosztott kormányzás és előnyök, valamint a béke mellett. Ebben az összefüggésben az internet szuverenitása a rendelkezés egészében érződik, hiszen Kínában az autoriter vezetést demokratikusnak álcázzák, ebből adódóan a be nem avatkozás szerepel az elsődleges elvek között. A stratégia ismerteti a kiberbiztonság definícióját is. A nemzeteknek el kell ismerniük egymás jogát, hogy saját kiberfejlesztési útvonalat, kibertér szabályozási modellt, és internetpolitikát választhassanak, és biztosítaniuk kell, hogy egyenlő esélyekkel vegyenek részt a kibertér irányításában. Egyetlen ország sem kísérelheti meg az internet feletti teljes ellenőrzés átvételét, nem szólhat bele egy másik állam belügyeibe, és nem támogathat olyan információs tevékenységeket, amelyek negatívan befolyásolják egy másik ország nemzetbiztonságát. A szuverenitás fogalma a stratégiai célokban is megmutatkozik, amelyek közül az első a szuverenitás és biztonság garantálása. Ezt a stratégiai célt Kína elsősorban békés módszerekkel kívánja elérni, illetve célul tűzte ki azt is az állam, hogy megakadályozza, hogy a kibertér új hadszíntér legyen. Ez kissé ellentmondásos, hiszen Kína nagymértékben hasznosítja a kibertér védelmének erősítésére, és hadseregének is fontos szerepet szán ebben. Sőt, szándékában áll egy kiberhadsereg létrehozása.⁸⁸

A dokumentum céljai közül másodikként a nemzetközi szabályrendszer létrehozását, harmadikként az internetszabályozás kérdéskörét érdemes tanulmányozni. Az előbbivel kapcsolatban Kína egy kölcsönösen kíváncsi, az ENSZ-en alapuló nemzetközi szabály- és normarendszer létrehozását szorgalmazza. Ennek a rendszernek az a célja, hogy elősegítse az államok viselkedésére vonatkozó szabványok kialakítását a kibertérben. Utóbbi kapcsán a dokumentum egy többoldalú, demokratikus és átlátható internetkormányzási mód szükségességét szorgalmazza, amely az egyenlő részvételen és a kollektív döntéshozatalon alapul. A többoldalú mutatót azért érdemes kiemelni, mert ez az egyik elsődleges konfliktusforrás a nyugati hatalmakkal, akik többpárti internetszabályozási rendszert kívánnak megvalósítani.⁸⁹

⁸⁸ Molnár Dóra (2020): Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 361. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁸⁹ u.o. pp. 361-362.

Kína külpolitikájának három legfőbb célja az internet és információmegosztás fenyegetésének csökkentése a stabilitás és a legitimáció érdekében, és a kibertér olyan formálása, amely növeli az állam gazdasági, politikai és katonai befolyását, ezzel ellensúlyozva az amerikaiakat.⁹⁰ Hszi Csin-Ping elnöksége alatt Kína más megközelítéssel állt kiberpolitikájához, ugyanis a folyamatos kiberdiplomácia művelése mellett döntöttek céljaik gyors elérése érdekében. Peking számára a kiberbiztonság egyszerre mérsékelheti a terrorveszélyt, elősegítheti a regionális befolyást, és szoros kapcsolatokat ápolhat olyan jelentős partnerekkel, mint az Egyesült Államok. 2014-ben Kína adott otthont az első nemzetközi internetes konferenciának Wuzhenben. A kínai elnök azonban csak az egy évvel későbbi konferencián vett részt személyesen, ezzel megmutatta a kiberbiztonság megnövekedett jelentőségét Kína számára. A fórumon az elnök beszédében az internet szuverenitása mellett az internet globális kormányzására, azon belül is a multilateralizmus terjesztésére fókuszált. Medvegyev orosz elnök egy apró, de jelentős gesztusként, azonnal reagált a kínai elnök beszédére, és kifejezte támogatását.⁹¹

Kína kiberdiplomáciája a be nem avatkozás és a részvétel egyenlőségének koncepcióján, a kapacitásépítésen, a segítségnyújtás fontosságán, valamint az Egyesült Nemzetek Szervezetének és más szervezeteknek a támogatásán alapul. Kína úgy gondolja, hogy az internet napjainkban elengedhetetlen fontossággal bír a gazdasági növekedés és hatalom biztosításának eszközeként, de egyben potenciális veszélynek gondolja a belső stabilitásra és a rendszer legitimitására. Az állam elsősorban a hazai cenzúrán keresztül kívánja szabályozni ezt (Great Firewall), de a nemzetközi együttműködést is szorgalmazza.⁹²

Kína kiberdiplomáciai erőfeszítései között régóta ott áll az internet forrásának igazságtalan elosztása, ugyanis a világon található 13 főszerverből 10 az Egyesült Államokban van.⁹³ Ennek eredményeként nem váratlan, hogy Kína támogatja az együttműködést a kibertér kezelésében, hogy megdöntsék az amerikai fölényt.

A digitális szféra egyre jelentősebbé válik Kína nemzetközi és helyi kapcsolataiban. Többek között a kiberbiztonságot alkalmazza, hogy javítsa regionális pozícióját, miközben megőrzi

⁹⁰ Segal, Adam (2018): Year in Review: Chinese Cyber Sovereignty in Action. 2018. január 8. www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action (letöltés ideje: 2023. 10. 18.)

⁹¹ Bandurski, David (2015): China's cyber-diplomacy. 2015. december 21. <http://chinamediaproject.org/2015/12/21/chinas-cyber-diplomacy/> (letöltés ideje: 2023. 10. 10.)

⁹² Molnár Dóra (2020): Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 362. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁹³ Swaine, Michael D. (2013): Chinese View on Cybersecurity in Foreign Relations. China Leadership Monitor, No. 42. https://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf (letöltés ideje: 2023. 10. 10.)

vezető szerepét a régió más országaihoz és a fejlődő világhoz képest. Erős kapcsolatot tart fenn az USA-val, de a két hatalomnak számos nézeteltérése volt a kiberkérdésekkel kapcsolatban. A bilaterális kapcsolatok fejlesztését eleinte az Egyesült Államok kezdeményezte, de a kapcsolatok főként a gazdaságra fókuszáltak. Ez részben annak volt köszönhető, hogy a kínai diplomata nem rendelkeztek kibertérrel kapcsolatos ismerettel, ugyanis a küldöttek a külügyminisztériumból érkeztek. Az Egyesült Államok azonban fenntartásokkal kezdte el kezelni a Kínával való kapcsolatot. A 2013-as kaliforniai elnöki találkozón Obama figyelmeztette a kínai képviselőt, hogy a kiberkémkedés nagyon káros a kapcsolatukra. Később több ilyen incidens is nyilvánosságra került (pl. Snowden-ügy), amelynek hatására az Egyesült Államok több kínai hacker ellen is vádat emelt. Kína válasza erre a két ország közötti tárgyalások leállítása volt. Ez idő alatt két nagy, mindkét országban kiberbiztonsággal foglalkozó intézmény adott ki éves jelentést a kiberbiztonság akkori helyzetéről (amerikai CSIS - Center for Strategic and International Studies, kínai CICIR - China Institute of Contemporary International Relations). A kapcsolatok rendezésére csak a kínai hackerek elleni vádak ejtése után került sor. 2015-ben Hszi elnök Washingtonba látogatott. A tárgyalás eredménye egy történelmi jelentőségű megállapodás volt a két hatalom között, amely a kiberbiztonság témájára terjedt ki. A megállapodás aláírása azért is volt jelentőségteljes, mert Németország és más nyugati országok számára is példaként szolgált a kiberkapcsolatok kialakítására.⁹⁴

A megállapodás⁹⁵ kimondja, hogy a feleknek együtt kell működniük a kiberbűnözés felderítésében, és a bizonyítékok gyűjtésében, illetve tájékoztatást kell adniuk a nyomozás aktuális eredményeiről. Abban is megegyeztek, hogy egyik állam sem vesz részt, vagy nem támogat olyan tevékenységet a kibertérben, amelynek célja szellemi tulajdon ellopása. A felek továbbá támogatják a kibertérben érvényesülő normák kialakítását, ezt a kérdést pedig egy szakértői csoport fogja alaposabban megvitatni a strukturáltabb szemlélet kialakítása érdekében. Végül egy egyedi mechanizmus jön létre a kiberbűnözéshez kapcsolódó kérdések megvitatására. Az erre szolgáló testület évente két alkalommal ülésezik.⁹⁶

⁹⁴ Molnár Dóra (2020): Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 363. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

⁹⁵ Fact sheet: President Xi Jinping's State Visit to the United States. The White House, Office of the Press Secretary, 2015. szeptember 25. <https://obamawhitehouse.archives.gov/the-pressoffice/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states> (letöltés ideje: 2023. 10. 20.)

⁹⁶ Renard, Thomas (2015): US–China cybersecurity agreement: a good case of cyber diplomacy. 2015. október 1. www.egmontinstitute.be/us-china-cybersecurity-agreement-a-good-case-of-cyber-diplomacy/ (letöltés ideje: 2023. 10. 20.)

A megállapodást követően alacsonyabb szintre csökkent az országok közötti kiberkémkedés, de nem kizárt, hogy ismét növekedni fog, így az amerikai-kínai kapcsolatok nagyon képlékenyek. Ennek másik oka, hogy a két nagyhatalom álláspontja között jelentős különbségek vannak. Ez a vita a kibertér militarizálásáról, a nemzetközi jog alkalmazásáról, valamint a kiberkémkedés hatóköréről és céljáról szól. Emiatt a feszültség miatt azonban fennáll egy jelentősebb konfliktus veszélye. E konfliktus elkerülése érdekében a fegyverkorlátozás logikáját és célrendszerét lehetne alkalmazni, ugyanúgy, mint a hidegháború során a nukleáris fegyverkezésre kiszabott korlátozás esetében.⁹⁷ Ha viszont az amerikai vezetés a jövőben is egyoldalú diplomáciai lépéseket tesz, úgy további feszültség várható.⁹⁸

Az elkötelezett kétoldalú kapcsolatok közül a kínai-orosz kapcsolatokat is érdemes kiemelni. 2015-ben az országok 32 bilaterális egyezményt írtak alá – köztük a nemzetközi információbiztonságról szóló partnerségi megállapodást.⁹⁹ Ebben a megállapodásban kötelezettséget vállaltak, hogy nem vesznek részt egymás elleni hackertámadásokban, és elítélik a politikai destabilizáció céljával indított kibertámadásokat. Egy másik nagyobb előrelépés a közös kiberprojektek lebonyolításáról szóló együttműködés kezdeményezése volt.¹⁰⁰

A bilaterális kapcsolatok közül kiemelendő a 2012-ben létrejött szövetség az Európai Unióval. Az évente megrendezésre kerülő Európai Unió és Kína közötti csúcstalálkozón az EU-Kína kiberbiztonsággal foglalkozó csoport is üléseik. Itt aggodalmaikat fejezhetik ki, valamint a kibertér kormányzásával kapcsolatos javaslataikat oszthatják meg.¹⁰¹ Kína az európai államok közül évente tárgyal az Egyesült Királysággal is, főként a kiberbűnözés témaköréről.¹⁰²

⁹⁷ Levite, Ariel (Eli) – Jinghua, Lyu (2019): Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation. 2019. 01. 24. <https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213> (letöltés ideje: 2023. 10. 20.)

⁹⁸ Dollar, David – Hass, Ryan – Bader, Jeffrey A. (2019): Assessing U.S.-China relations 2 years into the Trump presidency. 2019. január 15. www.brookings.edu/blog/order-from-chaos/2019/01/15/assessing-u-s-china-relations-2-years-into-the-trump-presidency/ (letöltés ideje: 2023. 10. 20.)

⁹⁹ Roth, Andrew (2015): Russia and China Sign Cooperation Pacts. The New York Times, 2015. május 8. www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=0 (letöltés ideje: 2023. 10. 15.)

¹⁰⁰ Molnár Dóra (2020): Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 364. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

¹⁰¹ Pawlak, Patryk (2015): Cyber Diplomacy: EU Dialogue with Third Countries. European Parliament Think Tank, 2015. június 29. [www.europarl.europa.eu/RegData/etudes/BRIE/2015/564374/EPRS_BRI\(2015\)564374_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/564374/EPRS_BRI(2015)564374_EN.pdf) (letöltés ideje: 2023. 10. 10.)

¹⁰² Molnár Dóra (2020): Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 364. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

Az ország diplomáciai stratégiájában feltehetőleg továbbra is a kibertér szuverenitásának kérdése lesz a legfontosabb, és pozícióját a kibertérben gazdasági növekedésével fogja előreláthatólag javítani. A kínai kiberdiplomácia egyik fejlesztés alatt álló kategóriája a kereskedelmi és befektetési politika, amelyet a gazdasági és politikai hatalom egy formájaként használnak. Azáltal, hogy új piacok felé orientálódik a világban, új támogatói lesznek, akik Kínát külpolitikájában és kiberpolitikájában is támogatják. A befektetések viszont nem minden esetben jelennek meg közvetlen politikai hatalomként, ez gyakran indirekt formát ölt. A közvetlen befolyás egyik példája a Huawei részvétele az afrikai piacon. 2005-ben a vállalat iskolát alapított Nigéria fővárosában, ezután öt évvel később már 50 afrikai országban volt jelen, 300 millió felhasználóval. Egy másik példa az Egy övezet, egy út kezdeményezés, amely két részből áll. Egyrészt a Selyemút gazdasági övezete, amely összeköti Kínát a Perzsa-öböllel, a Földközi-tengerrel és az Indiai-óceánnal, valamint a napjainkban használatos tengeri selyemút vízi útvonalait kapcsolja össze. Ezzel összefüggésben egy információs selyemút megépítését is tervezik, amely eredetileg optikai szálak telepítését jelentette, és a tervek szerint Kínát 48 afrikai országgal kötné össze.¹⁰³ Ezt a tervet azonban később kiegészítették, a jövőben különböző portokat és szoftvereket is telepíteni kívánnak.¹⁰⁴

Kína kiberdiplomáciáját és politikáját előreláthatólag két erő fogja befolyásolni. Az egyik az amerikai folyamatok alakulása, ugyanis, ha az USA a belső problémáival foglalkozna, az azt jelenté, hogy Kínának lehetősége lenne részt venni a kibertér szabályozásának létrehozásában. A másik tényező a kibertér biztonságának alakulása, ugyanis jelenleg egyre veszélyesebbnek látszik, és előfordulhat a kibertér militarizálódása. Azonban Kína biztosan folytatja a megfontolt politikai és gazdasági lépéseinek megtételét, amihez hozzátartozik a kiberdiplomácia békés művelése is.¹⁰⁵

6.3. Oroszország a kiberdiplomáciában – avagy a kiberháborúzás mestere

Oroszország kiberpotenciálját az egyik legnagyobbnak és technológiailag legfejlettebbnek tartják a világon, az amerikai és kínai mellett. Az utóbbi években viszont az állam számtalanszor

¹⁰³ Chinese Firm Hopes to Wire Continent with Same Strategy that Boosted Internet Access Across China. Global Times, 2017. március 13. www.globaltimes.cn/content/1037500.shtml (letöltés ideje: 2023. 10. 15.)

¹⁰⁴ China's Digital Silk Road (DSR): The new frontier in the Digital Arms Race. 2020. 02. 19. www.silkroadbriefing.com/news/2020/02/19/chinas-digital-silk-road-dsr-new-frontier-digital-arms-race/ (letöltés ideje: 2023. 10. 15.)

¹⁰⁵ Molnár Dóra (2020): Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 365. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

alkalmazta ezeket a képességeket támadásra – erre példa Georgia és Észtország esete is, de ez történt az Egyesült Államokkal szemben is. A kiberkonfliktusok Oroszország stratégiájához tartoznak, ugyanis ezt használja fel kitűzött céljainak elérése érdekében. Ezek a támadások viszont ritkán történnek a posztszovjet térség határain kívül, ennek oka pedig pontosan az, hogy az Orosz Föderáció érdekei és célkitűzései főként erre a térségre vonatkoznak, a globális világ meghódítása pedig csak másodlagos számukra, ez pedig igaz a kibertérre is.¹⁰⁶

A kiberplatformok közötti interakciókat vizsgálva¹⁰⁷ megállapítható, hogy Oroszország az Egyesült Államokhoz és Kínához képest lemaradásban van ezen a téren. Ez azt jelenti, hogy Oroszország nem tartja olyan fontosnak a kiberdiplomáciát, ehelyett a kibertérben felmerülő vitákat a diplomácia formális rendszerének segítségével kívánja megoldani, főként erejét kihasználva.¹⁰⁸

A 21. század elején az ország még aktív szerepet vállalt a globális és regionális tanácskozásokon a kibertér szabályozását illetően, de mivel számára nem hoztak ezek sikert, a diplomácia helyét az offenzív kiberakciók váltották fel.¹⁰⁹

A kezdeti időszakban a diplomáciai lépések az összetűzések elkerülésére és nemzetek közötti digitális fegyverkezési verseny megakadályozására irányultak. Ennek egyik hozománya volt az 1999-ben Oroszország kezdeményezésére meghozott ENSZ Közgyűlés határozata.¹¹⁰ Az orosz külügyminiszter a kibertér militarizálásának lehetséges veszélyeit már ekkorra felvetette, és hangsúlyozta a kiberfegyverek káros hatásait is.¹¹¹ Ez azonban akkoriban nem keltette fel más államok figyelmét, hiszen az internet használata még nem volt olyan elterjedt. Oroszország továbbra is az ENSZ-által kínált diplomáciai rendszerben keresett megoldást, és támogatta a Kormányzati Szakértői Csoport 2004-ben történt létrehozását. Az orosz

¹⁰⁶ Molnár Dóra (2020): Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberpöröndön, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 366. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

¹⁰⁷ Brandon, Valeriano – Maness, Ryan C. (2014): The Dynamics of Cyber Conflict between Rival Antagonists, 2001–2011. *Journal of Peace Research*, 51(3), pp. 347–360. www.researchgate.net/publication/256046745_The_Dynamics_of_Cyber_Conflict_between_Rival_Antagonists_2001-2011 (letöltés ideje: 2023. 10. 11.)

¹⁰⁸ McNabb, David E. (2016): Vladimir Putin and Russia's Imperial Revival. CRC Press

¹⁰⁹ Wirtz, James J. (2015): Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. In GEERS, Kenneth: Cyber War in Perspective: Russian Aggression Against Ukraine. Tallinn, NATO CCD COE Publications. https://ccdcoe.org/uploads/2018/10/Ch03_CyberWarinPerspective_Wirtz.pdf (letöltés ideje: 2023. 10. 23.)

¹¹⁰ UN General Assembly, Resolution A/RES/53/70. <https://research.un.org/en/docs/ga/quick/regular/53> (letöltés ideje: 2023. 10. 27.)

¹¹¹ Dam, Kenneth W. – Owens, William (2009): Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. Committee on Offensive Information Warfare, National Research Council. <https://lawfare.s3-us-west-2.amazonaws.com/staging/s3fs-public/uploads/2013/01/NRC-Report.pdf> (letöltés ideje: 2023. 10. 23.)

kiberdiplomácia célja azonban már megváltozott, és a szabályozást helyezte előtérbe a megelőzés helyett, még pedig azért, mert ekkorra már a legtöbb állam nagymértékben fókuszált a kibertechnológia fejlesztésére. Az első eredményeket azonban csak 2014-ben érték el, amikor is a Szakértői Csoport jelentésében kimondta, hogy a nemzetközi jog a kibertérre is vonatkozik. A tárgyalások folytatódtak, és 2015-ben újabb megállapodás született egy magatartási kódex létrehozásáról a kibertérben, de ezek után a folyamatok megakadtak.¹¹²

Ezenkívül Oroszország regionálisan is támogatta a kódex létrehozását, 2011-ben pedig közzétette a Nemzetközi Információbiztonsági Konvenció tervezetét is. Ez a dokumentum hangsúlyozza az állami szuverenitás megtartását a kibertér tekintetében. Az orosz akarat a BRICS-államok¹¹³ körében is érvényesült határozatok elfogadtatásával és munkacsoportok létrehozásával.¹¹⁴

Végül pedig az orosz diplomáciai vezetés a kibertérrel is megkísérelte szabályozni a kétoldalú partnerkapcsolatok segítségével. Az első nemzetközi kiberügyekről szóló megállapodás 2013-ban jött létre az Egyesült Államok és Oroszország között. A megállapodás azonban nem volt kifejezetten sikeres, mert csak a technikai kérdésekről tárgyaltak. A dokumentumban rögzítésre került a CERT-ek közötti információmegosztás és egy kibertér működéséhez kapcsolódó forródrót létrehozása. Az oroszok abban bíztak, hogy lehetséges lenne egy kiterjedtebb megállapodás az amerikaiakkal, de ismét megakadtak a tárgyalások.¹¹⁵ Ezek után 2017-ben Oroszország újra kezdeményezte egy közös egyezmény létrehozását, de az amerikai fél a véglegesítése előtti napon visszalépett ettől. Oroszország több országgal is kötött megállapodást, köztük Indiával, Dél-Afrikával, Kínával, Fehéroroszországgal és Kubával is.¹¹⁶

¹¹² Molnár Dóra (2020): Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 367. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

¹¹³ BRICS-államok, azaz a világ leggyorsabban fejlődő gazdaságainak társulása. Jelenleg hat tagállama van (Brazília, Oroszország, India, Kína és a Dél-Afrikai Köztársaság) azonban a közeljövőben több állam csatlakozása várható.

¹¹⁴ Molnár Dóra (2020): Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 367. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

¹¹⁵ Popescu, Nicu – Secieru, Stanislav (eds.) (2018): Hacks, leaks and disruptions. Russian cyber strategy. Chaillot Papers No. 148., 2018. október, European Union Institute for Security Studies. www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf (letöltés ideje: 2023. 10. 23.)

¹¹⁶ Molnár Dóra (2020): Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, pp. 367-368. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

Az állam már több évtizeddel korábban felismerte a kibertér nemzetközi felügyeletének szükségességét Kínával együtt, és továbbra is kitart a kibertérre vonatkozó normák kialakításának elve, valamint az állami szuverenitás megtartása mellett. A nyugati táborral való szembenállás negatív hatással van Oroszország Egyesült Államokkal és Európával való kapcsolataira, ennek következtében csökken a globális megegyezés valószínűsége, annak ellenére, hogy az ENSZ főtitkára is szorgalmazza egy nemzetközi szabályrendszer kialakítását.¹¹⁷

Számos mérőszámot használnak az egyes államok kiberbiztonságának felmérésére, ezek közül kiemelendő az ITU által közzétett Globális kiberbiztonsági index. Az ötödik összehasonlítási alap az együttműködés, ahol a bi- és multilaterális egyezmények számát, illetve a szervezetekben való tagságot vizsgálják. Az index összértékelése azt mutatja, hogy az Egyesült Államok a második, Oroszország a 26., Kína pedig a 27. helyen áll a listán.¹¹⁸ Ez kimutatja, hogy az Egyesült Államok a kiberdiplomáciában is vezető szereppel bír. Kína helyezése a listán feltételezhetőleg amiatt van, mert az ország a közelmúltban kezdett el aktív szerepet vállalni a kiberdiplomáciában, amelynek hatása még nem mutatkozott meg a statisztikában. Oroszország esetében az eredmény nem váratlan, hiszen az oroszok nem feltétlenül érdekeltek a kiterjedt kapcsolatrendszerük kiberbiztonságban való hasznosításában. Emellett a legtöbb országról elmondható, hogy alacsony együttműködési mutatóval rendelkezik, így a kiberdiplomácia területén várhatóan jelentős változások várhatóak.¹¹⁹

¹¹⁷ US Chief Calls for Regulatory Scheme for Cyberwarfare (2018) Radio Free Europe/Radio Liberty, 2018. február 19. www.rferl.org/a/un-guterres-calls-for-cyberwarfare-rules/29049069.html (letöltés ideje: 2023. 10. 23.)

¹¹⁸ Global Cybersecurity Index, ITU, 2020, <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTML-E> (2023. 10. 23.)

¹¹⁹ Molnár Dóra (2020): Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 368. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

7. A mesterséges intelligencia a diplomáciában

Vlagyimir Putyin orosz elnök már néhány évvel ezelőtt is úgy vélekedett a mesterséges intelligencia-kutatásról, hogy az az állam, amely előnyre tesz szert ezen a téren, az fogja uralni a világot.¹²⁰ Az innovációt kutató tudósok felismerték, hogy az „általános célú technológiák” (GPT-k) képesek jelentős társadalmi változások katalizálására. Ezek olyan technológiai fejlesztések, amelyek nagy hatással vannak a mindennapi emberi életre és az üzleti világra.¹²¹ Az utóbbi kétszáz évben négy jelentős technológiai találmány jött létre, amely meghatározta az emberiség fejlődésének történetét: először a gőzgépet találták fel, majd ezt követte az elektromosság és az információs technológia. A negyedik hullámot a mesterséges intelligencia jelenti.¹²²

Az újdonságban rejlő politikai és gazdasági potenciált a népszerű amerikai politikus, Brzezinski sakktábla-metaforával jellemezte.¹²³ Igazi technológiai versenynek lehetünk most szemlélői. A szakértők úgy vélik, hogy Oroszországnak nehéz dolga lesz ennek a versenynek a megnyerésében. Ma Kínát tartják erre a legesélyesebbnek. Már 2015-ben bejelentette az állam az 1,36 billió amerikai dolláros fejlesztési programját, amelyet a mesterséges intelligencia (MI) fejlesztésére fordítanak. Más államok tervezett beruházásai meg sem közelítik ezt az összeget. A versenyben viszont sokat számíthat az Egyesült Államok innovációbarát légköre vagy az Európai Unió jogi rendszere. A nyilvánvaló pénzügyi egyenlőtlenség ellenére Nagy-Britannia, Franciaország, Németország, Japán, Oroszország és Kanada továbbra is intenzíven jelen van az MI-forradalomban.¹²⁴

Emiatt a versengés kiélezettnek tekinthető és egyre növekszik. A jelenlegi és elkövetkezendő évtized meghatározó lesz ennek kibontakozásában. Amennyiben valóban a kibertér a geopolitikai érdekképviselő új és legfontosabb dimenziója, a nemzeti érdekképviselőt

¹²⁰ Meyer, David (2017): Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World, Fortune, 2017. 09. 04. <https://fortune.com/2017/09/04/ai-artificial-intelligence-putin-rule-world/> (letöltés ideje: 2023. 10. 20.)

¹²¹ Gill, Indermit (2020): Whoever leads in artificial intelligence in 2030 will rule the world until 2100. www.brookings.edu/blog/future-development/2020/01/17/whoever-leads-in-artificial-intelligence-in-2030-will-rule-the-world-until-2100/?fbclid=IwAR3UJSDfUG4aFGXpHRDdch76HQu9ZgDIOQXG (letöltés ideje: 2023. 10. 20.)

¹²² Nyáry Gábor (2020): Kiberbiztonság és külgazdasági kapcsolatok: a digitális gazdaság dilemmái, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 397. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

¹²³ Brzezinski, Zbigniew (1999): A nagy sakktábla. Budapest, Európa Könyvkiadó

¹²⁴ Nyáry Gábor (2020): Kiberbiztonság és külgazdasági kapcsolatok: a digitális gazdaság dilemmái, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 397. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

folytatott harcban a játékosok a 21. század sakktábláján küzdenek, a mesterséges intelligencia pedig a királynő.¹²⁵

Először is fontos meghatározni azt, hogy a mesterséges intelligencia nem egy egyedi technológiai törekvést jelöl, hanem a számítástechnika több tudományágát érintő területe. Az MI, az emberekre intelligens folyamatainak számítógépes szimulációját testesíti meg.¹²⁶ Ilyen folyamat például a tanulási képesség, az érvelés, valamint a hibák kijavításának képessége. Fontos megemlíteni azt is, hogy az MI a „big data”-hoz kapcsolódik, ami azt jelenti, hogy nagy és rendkívül összetett adatokat jelent, amelyek gyorsan változnak. Ezeket a nagy mennyiségű adatokat nem lehet tradicionális módszerekkel kezelni (adatbázis-kezelőkkel), a mesterséges intelligencia ezt könnyíti meg. Ezenkívül kimondható, hogy a gépi tanulási módszerek, amelyek az egyik legjelentősebb mesterséges intelligenciával kapcsolatos folyamatok, nem képzelhetők el a nagy mennyiségű adat nélkül, amely az algoritmusok kialakításában játszik szerepet.¹²⁷

A bevezetőben szó esett arról, hogy a mesterséges intelligencia várhatóan át fogja formálni a geopolitikát. Azonban a mesterséges intelligencia nemcsak, hogy a nemzetközi környezetet, az államok közötti versenyt változtathatja meg jelentősen, de a békés intézményi érdekérvényesítési rendszert, a diplomácia módszereit is. A nagy adatalapú eszközök, valamint az MI eszközrendszer a digitális diplomácia alapját képezik több területen is, ideértve az információgyűjtést és -feldolgozást, valamint a szoftveres külpolitikai döntéshozatalt. A mesterséges intelligencia olyan szervezetek eszköze, amelyek politikai végrehajtással és diplomáciával foglalkoznak.¹²⁸

Az információszerzés és az információátadás továbbra is a diplomácia elsődleges szerepe. Ezen túlmenően, sok MI projekt szól arról, hogy az információgyűjtést, elemzést és bemutatást új, minőségi szintre tudják növelni. Eközben egyre több az információfeldolgozási

¹²⁵ Nyáry Gábor (2020): Kiberbiztonság és külgazdasági kapcsolatok: a digitális gazdaság dilemmái, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 397. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

¹²⁶ Futó Iván (1999): Mesterséges Intelligencia, Budapest, Aula Kiadó Kft.

¹²⁷ Nyáry Gábor (2020): Kiberbiztonság és külgazdasági kapcsolatok: a digitális gazdaság dilemmái, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, pp. 398-399. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

¹²⁸ Mapping the challenges and opportunities of artificial intelligence for the conduct of diplomacy (2019), Geneva, DiploFoundation. <https://www.diplomacy.edu/wp-content/uploads/2022/12/AI-diplo-report.pdf> (letöltés ideje: 2023. 10. 20.)

problémákkal foglalkozó kezdeményezés, ezek főként az álhírek elleni küzdelemre irányulnak.¹²⁹

A mesterséges intelligencia és az adattudomány hasznosításának jó példáját mutatja be a brit külpolitikai szervezet kezdeményezése is. Az általuk kifejlesztett MI támogatott rendszer több százezer információforrást képes automatikusan felmérni különböző nyelveken, ezeket a forrásokat lefordítják angolra, és megjelenítik a felhasználói felületen. Korábban nagy probléma volt a diplomataknak számára, hogy sok időt töltöttek a hírlapok olvasásával. Ebben nagy segítségükre van a technológia. Ezek a külpolitikai csoportok rövid időn belül olyan nagy mennyiségű információt tudnak feldolgozni, amely korábban lehetetlenségnek tűnt.¹³⁰

A külügyi szervezetek kiemelt adminisztratív feladatai jellemzően visszatérő, gyakori problémák megoldására irányulnak, de általában rövid határidőt kapnak rá. A mesterséges intelligencia leggyakoribb és legnépszerűbb alkalmazásai a chatbot technológiára támaszkodnak. A konzuli chatbotok legfőképp utazással kapcsolatos kérdésekben segítenek az ügyfeleknek, de olyan vészhelyzeti információkkal is tudnak szolgálni, amelyek bármikor felhasználhatóak. A humán és anyagi erőforrásbeli hiányokkal küzdő szervezetek azonban egyre nehezebben tudják kielégíteni a kereskedelmi hálózataikkal és külföldi képviselőikkel járó megnövekedett igényeket. Nem meglepő tehát, hogy a diplomáciának ez a speciális ágazata magas elvárásokkal rendelkezik az IKT-technológia, és különösen az MI erősokszorozó potenciáljával kapcsolatban.¹³¹

A mesterséges intelligencia legérdekesebb aspektusa a külpolitikai stratégiaalkotásban rejlik. A Kínai Tudományos Akadémia kifejlesztett egy külpolitikai döntéstámogató mesterséges intelligencia-alapú rendszert, amelynek prototípusát már alkalmazták is. A szoftver nagy mennyiségű információt dolgoz fel, beleértve a nemzetbiztonsági kezdeményezésektől kezdve a diplomáciai rendezvényeken terjedő pletykákig mindent. Ha a külpolitikai döntéshozók egy bonyolult helyzetben mérlegelésre szorulnak, a szoftver nagyon gyorsan, több

¹²⁹ Nyáry Gábor (2020): Kiberbiztonság és külgazdasági kapcsolatok: a digitális gazdaság dilemmái, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 400. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

¹³⁰ Exclusive: Meet the UK's „Data Diplomat”. <https://govinsider.asia/innovation/uk-foreign-office-open-source-unit-data-diplomat-graham-nelson/> (letöltés ideje: 2023. 10. 11.)

¹³¹ Nyáry Gábor (2020): Kiberbiztonság és külgazdasági kapcsolatok: a digitális gazdaság dilemmái, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 400. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

alternatívát is kínál számukra. Azaz nemcsak a mesterséges intelligencia segíti a diplomácia működését, hanem fordítva is.¹³²

Megfigyelhető, hogy az új technológia jelentőséggel bír a geopolitikai kapcsolatokban is. Ami viszont szintén fontos, hogy a mesterséges intelligencia, annak technikai vonatkozásai, a személyes adatok védelme és még etikai szempontból is komoly aggodalomra adnak okot a nemzetközi közvélemény számára. Ezért egyre nagyobb igény mutatkozik ezen helyzetekre vonatkozó nemzetközi szabályok megalkotására. Az már most biztos, hogy az MI a diplomácia és a nemzetközi kapcsolatok egyik legjelentősebb befolyásolója lesz a jövőben. A mesterséges intelligencia kutatásához, fejlesztéséhez és alkalmazásához szükséges feltételek felügyelete elengedhetetlen. A technológia hihetetlen erővel bír, így egészen biztosan szükség lesz szabályok alkotására. Emiatt a következő években a kiberdiplomata figyelmének fókuszra valószínűleg erre a területre fog összpontosítani. Emellett a mesterséges intelligencia szabályozását és a kapcsolódó kérdéseket körülvevő nemzetközi jogi környezet még fejlődési szakaszban van. A mesterséges intelligencia szabályozása magában foglalja a technikai, gazdasági és társadalmi összetevők kombinációját. A jogi szabályozási környezet kialakítása elsősorban a következő fő témákat érinti: adatvédelmi és biztonsági kérdések, valamint a rendszerek felelőssége és elszámoltathatósága.¹³³

A 2010-es évtized közepétől multilaterális fórumokon a szabályrendszer létrehozása egyre népszerűbbé vált. 2018-ban Kanada és Franciaország közös kezdeményezése volt egy olyan testület létrehozása, amely megvizsgálja az új technológia hatásait.¹³⁴ 2019 tavaszán az OECD (Gazdasági Együttműködési és Fejlesztési Szervezet) elfogadta a Mesterséges Intelligencia Ajánlásait, néhány hónappal később a G20 Mesterséges Intelligencia Alapelvét. Ezenkívül 2019-ben a Világgazdasági Fórum kiadott egy protokollt, amely segíti a kormányok számára az MI beszerzését. A vezető nemzetközi egyesülésekhez hasonlóan az Európai Unió is a mesterséges intelligencia szabályozásának előmozdítása mellett döntött. 2018-ban a Bizottság magas szintű szakértői csoportot hozott létre az MI-vel kapcsolatos kérdések kivizsgálására, különös tekintettel annak megbízhatóságára. 2020-ban az EU Bizottság kiadta a Mesterséges

¹³² Nyáry, Gábor (2020): Kiber geopolitika. Mesterséges Intelligencia alkalmazások az államigazgatás külpolitikai alrendszeireiben. Új Magyar Közigazgatás, 2020/1., p. 37.

¹³³ Nyáry Gábor (2020): Kiberbiztonság és külgazdasági kapcsolatok: a digitális gazdaság dilemmái, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, pp. 400-402. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

¹³⁴ Findlay, Buddle (2020): Artificial intelligence and the regulatory landscape. www.lexology.com/library/detail.aspx?g=4c845762-e954-4f47-8809-f5ad0f5d3716 (letöltés ideje: 2023. 10. 22.)

Intelligencia Fehér Könyvét¹³⁵, ez jelentős előrelépésnek tekinthető a szabályozás terén. Az okmány leírta a mesterséges intelligencia alkalmazásával járó legnagyobb veszélyeket: az alapvető jogok törékenységet, az adatokkal kapcsolatos jogok sebezhetőségét, a biztonsággal kapcsolatok kérdéseket, valamint a felelősségre vonás kérdését. A Bizottság úgy döntött, hogy a fejlesztés e korai szakaszában nem tesz még közzé átfogó szabályozási dokumentumot, ehelyett olyan jogszabályi követelményeket tett közzé, amelyek a mesterséges intelligencia megbízhatóságára vonatkozó jövőbeni szabályozások tárgyát képezik, és amelyek az Európai Unió alapelveit és értékeit helyezik előtérbe. A követelmények tartalmazzák az EU jogszabályainak alkalmazási területeit, valamint az ezen követelmények értelmezéséhez szükséges műszaki előírásokat.¹³⁶

A mesterséges intelligencia fejlődése tehát nemcsak a hétköznapiakra lesz nagy hatással a közeljövőben, hanem a hivatalos életre is. Mivel nagyon gyorsan fejlődik ez, így nehéz naprakésznek maradni, de mindenképp további megfigyelések szükségesek a témával kapcsolatban.

¹³⁵ White Paper on Artificial Intelligence. A European approach to excellence and trust (2020). Brussels, European Commission.

¹³⁶ Nyáry Gábor (2020): Kiberbiztonság és külgazdasági kapcsolatok: a digitális gazdaság dilemmái, Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, p. 402. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)

Összegzés

A dolgozat átfogó betekintést nyújtott a 21. századi nemzetközi kapcsolatok kibertérbeli alakulásába. Ahogy a tanulmányban is olvasható volt, az idő teltével jelentősen megváltozhatnak az érdekképviselőre alkalmas terek. Jelen esetben, a 21. században feltehetőleg a kibertér az egyik legmeghatározóbb, és vélhetően nagy szereppel fog bírni a kapcsolatok változásának terén.

A napjainkban ismert világrend folyamatos átalakuláson megy keresztül, amiben a technológia fejlettségének mértéke fogja eldönteni, hogy mely országok válnak a legnagyobb hatalmakká. A kibertérbeli állami kapcsolatok témakörének áttekintése során pedig megbizonyosodhattunk arról, hogy a diplomácia óriási jelentőséggel bír a békés együttélés megtartásában. Természetesen, mivel maga a kibertér egy nagyon bizonytalan és nem teljesen kiismert dimenzió, így biztosan további újdonságokat várhatunk, a hivatalos kapcsolatokban pedig szükség lesz a naprakészség megőrzésére.

Az egészen biztos, hogy a kibertér szabályozására van szükség, mégpedig globális együttműködés keretei között. A bizonytalanság, a veszélyeztetettség, amit a kiberbűnözés és a kiberhadműveletek okoznak akár egy egész világra kiterjedő konfliktushoz vezethetnek. Ez pedig lehet akár egy nukleáris fegyver indítókulcsának ellopása, vagy érzékeny dokumentumok, információk eltulajdonítása, amelyek nyilvánosságra hozása olyan mértékű társadalmi megosztottságot és bizalmatlanságot okozhat, amely akár globális szintű instabilitáshoz vezethet. Emellett a mesterséges intelligencia megjelenése további kérdéseket vet fel, hiszen az új technológia határaitól olyan keveset tudunk egyelőre, hogy elképzelni sem tudjuk milyen erővel bírhat. Az az állam pedig, amely a mesterséges intelligencia-kutatás terén előnyt szerez magának, elképzelhető, hogy uralni fogja világot.

Így amíg az államok nem tudnak megegyezni abban, hogy hogyan is kezeljék a kiberteret, valamint nem hajlandók betartani a már megkötött egyezségeket, addig egészen biztosan nem fog tudni egyik szervezet sem nagy sikereket elérni a tér kezelésében. Nagymértékű együttműködésre lenne szükség, de mivel jelenleg ezen technológiából tudják a legtöbb hasznot húzni a nemzetek, hiszen végtelen számú lehetőséggel bír, így egyelőre konszenzusra jutás nem várható.

Azt, hogy lehetséges-e egy univerzális kiterjesztésű egyezményt létrehozni, nagyon nehéz megállapítani, hiszen olyan alapvető elvek alapján tér el az államok véleménye, amelyek szükségesek lennének a keretrendszer kialakításához. Ilyen a szuverenitás és a nemzetközi jog használatának elve is. A szabályrendszernek azonban nagyon határozottnak kellene lennie,

hiszen pont abból kifolyólag, hogy nem ismerjük a tér kihasználhatóságának mértékét, egészen biztos, hogy megtalálnák az államok a módot arra, hogy kibújhassanak az egyezményekben foglaltak alól.

Kijelenthetjük, hogy az Egyesült Államok és Oroszország, de jelenleg és várhatóan a jövőben legfőképp Kína fog hozzájárulni a kibertér fejlődéséhez, ezáltal a még mindig fejlődő országnak számító állam válhat az új szuperhatalommá. Viszont természetesen a másik két nagyhatalom is meghatározó lesz a kibertér és kiberdiplomácia alakulásában. Ezen államok mellett pedig mindenképp érdemes lesz figyelni az elkövetkezendő évtizedben a jelenleg technológiailag gyorsan fejlődő országokra is, mint például Irán és Észak-Korea.

A téma mindenképp további megfigyelést igényel, szinte napról-napra követhetjük az újabb innovációkat, kutatásokat a témában. Abban biztosak lehetünk, hogy a kibertér megismerésével kapcsolatban zajló folyamatok mindannyiunk jövőjére nagy hatással lesznek. Az pedig, hogy állami szinten vagy globális szinten történik meg egy szabályrendszer létrehozása meghatározza majd világunk nemzetközi kapcsolatainak alakulását.

Irodalomjegyzék

1961. évi bécsi egyezmény a diplomáciai és konzuli képviseletek feladatköréről.
<https://net.jogtar.hu/jogszabaly?docid=96500022.tvr> (letöltés ideje: 2023. 10. 20.)
2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
- Bandurski, David (2015): *China's cyber-diplomacy*. 2015. december 21.
<http://chinamediaproject.org/2015/12/21/chinas-cyber-diplomacy/> (letöltés ideje: 2023.10.10.)
- Barrinha, André – Renard, Thomas (2017): Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, 3(4–5), p. 3.
- Bley, Bonnie (2019): *The New Geography of Global Diplomacy. China Advances as the United States Retreats*. 2019. november 27. www.foreignaffairs.com/articles/china/2019-11-27/new-geography-global-diplomacy (letöltés ideje: 2023.10.20.)
- Brandon, Valeriano – Maness, Ryan C. (2014): The Dynamics of Cyber Conflict between Rival Antagonists, 2001–2011. *Journal of Peace Research* 51(3). pp. 347–360.
www.researchgate.net/publication/256046745_The_Dynamics_of_Cyber_Conflict_between_Rival_Antagonists_2001-2011 (letöltés ideje: 2023. 10. 11.)
- Brzezinski, Zbigniew (1999): *A nagy sakktábla*. Budapest, Európa Könyvkiadó
- Buchan, Russell (2016): The International Legal Regulation of State-Sponsored Cyber Espionage. In: Osula, Anna-Maria – Rõigas, Henry (Eds.): *International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications*, Tallinn, pp. 65–86.
https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch4.pdf (letöltés ideje: 2023.09.26.)
- Cavelty, M. D. (2010). *Cyberwar*. In G. Kassimeris & J. Buckley (Eds.), *The Ashgate Research Companion to Modern Warfare* (pp. 123-144)
- Chapman, Justin (2019): *Threats and Opportunities of Cyber Diplomacy at PolicyWest*. 2019. 12. 24. www.pacificcouncil.org/newsroom/threats-and-opportunities-cyber-diplomacy-policywest (letöltés ideje: 2023.10.23.)
- China's Digital Silk Road (DSR): *The new frontier in the Digital Arms Race* 2020. 02. 19.
www.silkroadbriefing.com/news/2020/02/19/chinas-digital-silk-road-dsr-new-frontier-digital-arms-race/ (letöltés ideje: 2023. 10. 15.)

Chinese Firm Hopes to Wire Continent with Same Strategy that Boosted Internet Access Across China. *Global Times*, 2017. március 13. www.globaltimes.cn/content/1037500.shtml, (letöltés ideje: 2023. 10. 15.)

Choucri, Nazil (2012): *Cyberpolitics in International Relations*. Cambridge, *MIT Press*
Cyber security: confidence and security-building measures (CSBMs). *Federal Foreign Office website*, www.auswaertiges-amt.de/EN/Aussenpolitik/Friedenspolitik/Abruestung_/KonvRueKontrolle/VN-Konventionelle-Abruestung-Ruestungskontrolle_node.html (letöltés ideje: 2023.10.20.)

Dam, Kenneth W. – Owens, William (2009): Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. *Committee on Offensive Information Warfare*, National Research Council. <https://lawfare.s3-us-west-2.amazonaws.com/staging/s3fs-public/uploads/2013/01/NRC-Report.pdf> (letöltés ideje: 2023. 10. 23.)

Dollar, David – Hass, Ryan – Bader, Jeffrey A. (2019): *Assessing U.S.-China relations 2 years into the Trump presidency*. 2019. január 15. www.brookings.edu/blog/order-from-chaos/2019/01/15/assessing-u-s-china-relations-2-years-into-the-trump-presidency/ (letöltés ideje: 2023.10.20.)

Domingo, Francis C. (2016): Conquering a new domain: Explaining great power competition in cyberspace. *Comparative Strategy*, 35(2), p. 162.

Eilstrup-Sangiovanni, Mette (2018): Why the World Needs an International Cyberwar Convention. *Philosophy&Technology* 30, no. 3. p. 399

ENSZ. Általános információ az ENSZről. www.unis.unvienna.org/unis/hu/topics/un-general (Letöltés ideje: 2023. 09. 05.)

Eriksson, J., & Giacomello, G. (2006). *The Information Revolution, Security, and International Relations: (IR) relevant Theory?* *International Political Science Review*, 27(3), pp. 221-244.

Exclusive: Meet the UK's „Data Diplomat”. <https://govinsider.asia/innovation/uk-foreign-office-open-source-unit-data-diplomat-graham-nelson/> (letöltés ideje: 2023.10.11.)

Fact sheet: President Xi Jinping's State Visit to the United States. *The White House, Office of the Press Secretary*, 2015. szeptember 25. <https://obamawhitehouse.archives.gov/the-pressoffice/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states> (letöltés ideje: 2023. 10. 20.)

Fedosov, Sergey (2012): *Statement by the Russian participant at the UNIDIR Cyber Security Conference ‘What does a Stable Cyber Environment Look Like? Geneva, UNIDIR. 8–9*

- november 2012, www.unidir.ch/files/conferences/pdfs/pdf-conf1922.pdf (letöltés ideje: 2023. 10. 20.)
- Findlay, Buddle (2020): *Artificial intelligence and the regulatory landscape*. www.lexology.com/library/detail.aspx?g=4c845762-e954-4f47-8809-f5ad0f5d3716 (letöltés ideje: 2023. 10. 22.)
- Futó Iván (1999): *Mesterséges Intelligencia*, Budapest, Aula Kiadó Kft.
- Gill, Indermit (2020): *Whoever leads in artificial intelligence in 2030 will rule the world until 2100*. www.brookings.edu/blog/future-development/2020/01/17/whoever-leads-in-artificial-intelligence-in2030-will-rule-the-world-until-2100/?fbclid=IwAR3UJSDfUG4aFGXpHRDdch76HQu9ZgDIOQXGZo2t8iVjn-0HIQPNPnD42MM (letöltés ideje: 2023.10.20.)
- Global Cybersecurity Index, ITU, 2020, <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E>
- Goodin, Dan (2017): *"Suspicious" event routes traffic for big-name sites through Russia*. <https://arstechnica.com/information-technology/2017/12/suspicious-event-routetraffic-for-big-name-sites-through-russia/> (letöltés ideje: 2023.09.26.)
- <https://net.jogtar.hu/jogszabaly?docid=a1300050.tv> (letöltés ideje: 2023. 08.30.)
- International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. United States, 2011. május. obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf (letöltés ideje: 2023. 10. 21.)
- ITU általános története: <https://www.itu.int/en/history/Pages/ITUsHistory.aspx> (letöltés ideje: 2023.10.20.)
- 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
- Jørgensen, K. E. (2010). *International Relations Theory: A New Introduction* p.84
- Kosseff, Jeff (2017): *Cybersecurity Law*, John Wiley & Sons Inc., Hoboken, pp. 269-286.
- Krasznay, Csaba (2020): *Nemzetközi kapcsolatok a kibertérben*, IBTV. gyakorlata éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, *Nemzeti Közszerológati Egyetem Közigazgatási Továbbképzési Intézet*, Nemzeti Közszerológati Egyetem, Budapest, pp. 6-14.
- Levite, Ariel (Eli) – Jinghua, Lyu (2019): *Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation*. 2019. 01. 24. <https://carnegieendowment.org/2019/01/24/>

- chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213 (letöltés ideje: 2023. 10. 20.)
- Mapping the challenges and opportunities of artificial intelligence for the conduct of diplomacy (2019), Geneva, *DiploFoundation*, <https://www.diplomacy.edu/wp-content/uploads/2022/12/AI-diplo-report.pdf> (letöltés ideje: 2023. 10. 20.)
- Mártonffy, Balázs (2020): Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták, *Információ- és kiberbiztonság*, Ludovika Egyetemi Kiadó, Budapest, pp. 308-316. [nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1](https://nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1) (letöltés ideje: 2023. 08. 30.)
- McNabb, David E. (2016): Vladimir Putin and Russia's Imperial Revival. *CRC Press*
- Meyer, David (2017): Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World, *Fortune*, 2017. 09. 04., <https://fortune.com/2017/09/04/ai-artificial-intelligence-putin-rule-world/> (letöltés ideje: 2023.10.20.)
- Molnár, Dóra (2020): Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon, *Információ- és kiberbiztonság*, Ludovika Egyetemi Kiadó, Budapest, pp. 357-368. [nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1](https://nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1) (letöltés ideje: 2023. 08. 30.)
- Nabeel, Fahrad (2018): International Cyber Regime: A Comparative Analysis of the US-China-Russia Approaches. *Strategem* Vol. 1, No. 2, december 2018. pp. 8–27., www.academia.edu/38296708/International_Cyber_Regime_A_Comparative_Analysis_o_the_US-China-Russia_Approaches (letöltés ideje: 2023. 10. 20.)
- NATO (2017): Tallin Manual 2.0. On The International Law Applicable To Cyber Operations, *Cambridge University Press* [nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1](https://nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1) (letöltés ideje: 2023. 08. 30.)
- [nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3](https://nke.hu/xmlui/bitstream/handle/123456789/15928/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20szemely.pdf?sequence=3) (letöltés ideje: 2023.09.25.)
- [nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1](https://nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1) (letöltés ideje: 2023. 08. 30.)
- Nyáry, Gábor (2020): Kiber geopolitika. Mesterséges Intelligencia alkalmazások az államigazgatás külpolitikai alrendszerében. *Új Magyar Közigazgatás*, 2020. 1., p. 37.

- Nyáry, Gábor (2020): Kiberbiztonság és külgazdasági kapcsolatok: a digitális gazdaság dilemmái, *Információ- és kiberbiztonság*, Ludovika Egyetemi Kiadó, Budapest, pp. 397-402. nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1 (letöltés ideje: 2023. 08. 30.)
- Nyáry, Gábor (2020): Kiberdiplomácia: hatalom, politika és technológia a geopolitika ötödik dimenziójában, *Információ- és kiberbiztonság*, Ludovika Egyetemi Kiadó, Budapest, p. 327. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1
- Nye, Joseph S. (2011): Nuclear Lessons From Cyber Security? *Strategic Studies Quarterly*, Vol 5. No. 4. pp. 18-31.
- Painter, Christopher (2018): The rise of the internet and cyber technologies constitutes one of the central foreign policy issues of the 21st century. *The Foreign Service Journal*, 2018. június, www.afsa.org/diplomacy-cyberspace (letöltés ideje: 2023.10.19.)
- Pawlak, Patryk (2015): *Cyber Diplomacy: EU Dialogue with Third Countries*. *European Parliament Think Tank*, 2015. június 29. [www.europarl.europa.eu/RegData/etudes/BRIE/2015/564374/EPRS_BRI\(2015\)564374_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/564374/EPRS_BRI(2015)564374_EN.pdf) (letöltés ideje: 2023. 10. 10.)
- Popescu, Nicu – Secieru, Stanislav eds. (2018): Hacks, leaks and disruptions. Russian cyber strategy. *Chaillot Papers* No. 148., 2018. október, European Union Institute for Security Studies. www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf (letöltés ideje: 2023. 10. 23.)
- Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 2017. május 11. www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/, (letöltés ideje: 2023.10.19.)
- Renard, Thomas (2015): *US–China cybersecurity agreement: a good case of cyber diplomacy*. 2015. október 1. www.egmontinstitute.be/us-china-cybersecurity-agreement-a-good-case-of-cyber-diplomacy/ (letöltés ideje: 2023.10.20.)
- Renard, Thomas (2018): EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society*, 19(3), pp. 321–337.
- Roth, Andrew (2015): Russia and China Sign Cooperation Pacts. *The New York Times*, 2015. május 8. www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=0 (letöltés ideje: 2023. 10. 15.)

- Schmitt, Michael N. – Vihul, Liis (2016): The Nature of International Law Cyber Norms. In: Osula, Anna-Maria – Rõigas, Henry (Eds.) *International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications*, Tallinn, pp. 23–48. https://www.ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch2.pdf (letöltés ideje: 2023.09.25.)
- Segal, Adam (2018): *Year in Review: Chinese Cyber Sovereignty in Action*. 2018. január 8. www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action (letöltés ideje: 2023. 10. 18)
- Statista, A 2022-es évben észlelt kibertámadások típusainak megoszlása világszerte, <https://statista.com/statistics/1382266/cyber-attacks-worldwide-by-type/> (letöltés ideje: 2023. 10. 27.)
- Statista, A kiberűncselekmények által az Egyesült Államokban okozott éves pénzügyi kár összege 2001 és 2022 között (millió amerikai dollárban), <https://www.statista.com/statistics/267132/total-damage-caused-by-by-cybercrime-in-the-us/> (letöltés ideje: 2023. 10. 27.)
- Statista, A zsarolóvírus-kísérletek éves száma világszerte 2017-től 2022-ig (millióban), <https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide> (letöltés ideje: 2023. 10. 27.)
- Swaine, Michael D. (2013): Chinese View on Cybersecurity in Foreign Relations. *China Leadership Monitor*, No. 42. https://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf (letöltés ideje: 2023.10.10.)
- Szilágyi István (2018): A geopolitika elmélete, *Pallas Athéné Könyvkiadó Kft.*, Budapest
- Szkála Károly – Munk Sándor (2018): A kibertér fogalma, értelmezése és fejlődése, *Földrajzi Közlemények* 2018. 142. 4. p 345. <https://ojs.mtak.hu/index.php/fk/article/view/1127/933> (letöltés ideje: 2023. 10. 30.)
- UK and 50 nations sign cyber security pact. 2018. november 13. www.itproportal.com/news/uk-and-50-nations-sign-cyber-security-pact/ (letöltés ideje: 2023. 10. 23.))
- UN General Assembly, *Resolution A/RES/53/70*. <https://research.un.org/en/docs/ga/quick/regular/53> (letöltés ideje: 2023. 10. 27.)
- US Chief Calls for Regulatory Scheme for Cyberwarfare. (2018) *Radio Free Europe/Radio Liberty*, 2018. február 19. www.rferl.org/a/un-guterres-calls-for-cyberwarfare-rules/29049069.html (letöltés ideje: 2023. 10. 23.)

- White Paper on Artificial Intelligence. A European approach to excellence and trust (2020). Brussels, European Commission.
- Whyte, Christopher – Mazanec, Brian (2019): *Understanding Cyber Warfare: Politics, Policy and Strategy*. New York, Routledge.
- Wiener, Norbert (1961): *Cybernetics: Or Control and Communication in the Animal and the Machine*. Paris, Hermann & Cie & Camb. Mass. (MIT Press) 2nd revised ed.
- Wirtz, James J. (2015): *Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy*. In GEERS, Keneth: *Cyber War in Perspective: Russian Agression Against Ukraine*. Tallinn, NATO CCD COE Publications. https://ccdcoe.org/uploads/2018/10/Ch03_CyberWarinPerspective_Wirtz.pdf (letöltés ideje: 2023. 10. 23.)
- Xi Jinping gives speech at Cybersecurity and Informatization World Conference. 2016. április 19. <https://chinacopyrightandmedia.wordpress.com/2016/04/19/xi-jinping-gives-speech-at-cybersecurity-and-informatization-work-conference/> (letöltés ideje: 2023. 10. 18.)
- Ziolkowski, Katharina ed. (2013): *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, Tallinn, NATO CCDCOE Publication.