MIT
POLITICAL SCIENCE

Massachusetts Institute of
Technology Politikatudományi
Tanszék

2020-2 számú kutatási dokumentum

A nagyhatalmi beavatkozás jövője: A katonai beavatkozás új alternatívái

Benjamin Harris, Massachusettsi Technológiai Intézet

A nagyhatalmi beavatkozás jövője: A katonai beavatkozás új alternatívái

Benjamin Harris

1994. április 6-án lelőtték Habyarimana ruandai elnök repülőgépét, megölve az elnököt, és megadva a szikrát a modern idők legsúlyosabb népirtásához.[1] A népirtást kezdettől fogva a Radio-Television Libres des Mille Collines (RTLM), egy szélsőséges szélsőséges rádióadó lázító adásai bátorították és segítették.

a Genocidaires által létrehozott állomás.[2]

Áprilisban az "Inyenzis" szót használva6,, ami azt jelenti.

"Csótányok" - mondta az animátor Hitimana a hallgatóságának -, "hozzátok beszélek! Ti, a Rugungában élők, azok, akik ott élnek Kanogóban, azok, akik Kanogóban, sőt, akik Mburabuturoban élnek, nézzetek be Mburabuturo erdejébe, nézzétek meg alaposan, hogy nincsenek-e benne inyenzik. Nézzétek meg alaposan, nézzétek meg, nézzétek meg, hogy nincsenek-e bent Inyenzik."[3] Az állomás konkrét erőszakos cselekményekre buzdított. Áprilisban a 12,népszerű

animateur Kantano, a lázadó harcosokra használt kifejezéssel buzdította hutu társait:

> És ti, akik lent éltek Rugunga közelében, még ha esik is, menjetek ki. Látni fogjátok Inkotanyi szalmakunyhóit a mocsárban, ahol lovakat tartanak. Világos tehát, hogy ez a hely Inkotanyinak ad menedéket. Úgy gondolom, hogy azoknak, akiknek van fegyverük, azonnal el kellene menniük ezekhez az inkotanyikhoz, mielőtt meghallgatnák az RTLM rádiót és elmenekülnének. Álljanak a hely közelébe, kerítsék be őket és öljék meg őket, mert ott vannak.
> [4]

---

[1] Alan J. Kuperman, *A humanitárius beavatkozás határai: Genocide in Rwanda* (Brookings Institution Press, 2004), 15.

[2] Alison De Forges, "'Ne hagyj senkit, hogy elmesélje a történetet': Népirtás Ruandában" (New York: Human Rights Watch, 1999), https://www.hrw.org/reports/1999/rwanda/Geno1-3-10.htm#P408_170340; Alain Destexhe, "The Third Genocide", *Foreign Policy*, no. 97 (1994): 3-17, 8.

[3] Noël Hitimana, "Április 6-i adás", ford. ENSZ (RTLM, 1994. április 6.), http://migs.concordia.ca/links/documents/RTLM_06Apr94_eng_tape0122x.pdf. Lásd Kennedy Ndahiro, "In Rwanda, We Know All About Dehumanizing Language", The Atlantic, 2019. április 13., https://www.theatlantic.com/ideas/archive/2019/04/rwanda-shows-how-hateful-speech-leads-violence/587041/ az "Inyenzi" jelentéséről.

[4] Kantano Habimana, "Adás 1994. április 12-én", ford. Fabien Nsengiyumva (RTLM, 1994. április 12.),

Concordia MIGS, http://migs.concordia.ca/links/documents/RTLM_16-17May94_eng_tape0002.pdf, 4.

A Hate Radio, ahogyan azt a nyugati megfigyelők is nevezték, fontossága nem veszett el. Az ENSZ békefenntartóinak parancsnoka, Roméo Dallaire kérte a rádió "semlegesítését".[5] A nyugati kormányok, elsősorban az Egyesült Államok, határozottan elutasították.

hogy saját erőket küldjenek, vagy akár több ENSZ-békefenntartót hagyjanak jóvá, de a népirtásra adott amerikai válaszlépések koordinálására összeállított amerikai ügynökségközi csoport fontolóra vette a rádióadások zavarását. Végül ezt a lehetőséget is elvetették, miután a Pentagon azzal érvelt, hogy "a zavarás hatástalan és költséges mechanizmus, amely nem éri el a célt", és hogy a segélyszállítmányok eljuttatása jobb alternatíva. [6] A népirtás a tutsi fegyveres erők katonai győzelméig töretlenül folytatódott.[7]

Amikor polgárháborúk dúlnak vagy népirtások törnek ki, a nagyhatalmak döntéshozóinak a teljes katonai beavatkozástól a diplomáciai tiltakozásig számos lehetőség áll a rendelkezésükre. Ez a tanulmány három érvet hoz fel az ilyen döntések meghozatalának módjáról. Először is, a vezetők döntései arról, hogy beavatkoznak-e és hogyan, racionális döntések, amelyek figyelembe veszik a költségeket, a hasznot és a siker valószínűségét. Másodszor, amikor a politikai döntéshozók a katonai beavatkozást fontolgatják, a nem kinetikus beavatkozásokat is mérlegelik.

Az "Inkotanyi" jelentéséhez lásd CatherineBond, "Listening Carefully, Looking Harder: The Role of Language in Media Coerage During the Rwandan Genocide, 1994," megtalálható Allan Thompson, *Media and Mass Atrocity: The Rwanda Genocide and Beyond* (McGill-Queen's Press - MQUP, 2019).

[5] Samantha Power, "Bystanders to Genocide", The Atlantic, 2001. szeptember 1., https://www.theatlantic.com/magazine/archive/2001/09/bystanders-to-genocide/304571/.

[6] Frank G. Wisner, "Memorandum az elnök nemzetbiztonsági ügyekért felelős helyettes asszisztense számára, Nemzetbiztonsági Tanács. Ruanda: Jamming Civilian Radio Broadcasts" (Védelmi Minisztérium, 19945,. május), https://nsarchive2.gwu.edu//NSAEBB/NSAEBB53/rw050594.pdf.

[7] Az, hogy az RTLM érdemben hozzájárult-e az erőszakhoz, tudományos vita tárgya. Számos érvet lásd David Yanagizawa-Drott, "Propaganda and Conflict: Evidence from the Rwandan Genocide," *The Quarterly Journal of Economics* 129, no. 4 (2014. november 1.): 1947-94,

https://doi.org/10.1093/qje/qju020; Gordon Danning, "Did Radio RTLM Really Contribute Meaningfully to the Rwandan Genocide?": Using Qualitative Information to Improve Causal Inference from Measures of Media Availability," *Civil Wars* 20, no. 4 (2018. október 2.): 529-54, https://doi.org/10.1080/13698249.2018.1525677; Scott Straus, "What Is the Relationship between Hate Radio and Violence? Rethinking Rwanda's 'Radio Machete'," *Politics & Society* 35, no. 4 (2007. december 1.): 609-37, https://doi.org/10.1177/0032329207308181.

a katonai beavatkozás alternatívái. Végezetül, az új technológiák a katonai beavatkozás új, alacsonyabb költségű alternatíváit teszik lehetővé: a befolyásolási kampányokat és a kibercsapásokat. Alacsonyabb költségeik miatt a döntéshozók várhatóan ezeket az alternatívákat választják.

Ez a dokumentum a következőképpen fog eljárni. Először is áttekintem a beavatkozásra vonatkozó racionális költség-haszon döntési keretet. Másodszor a beavatkozás új definícióját javaslom, hogy pontosan megragadhassuk a döntéshozók rendelkezésére álló döntési teret. Harmadszor, áttekintem a befolyásolási kampányok és a kibercsapás első alkalmazására vonatkozó esettanulmányokat. Negyedszer megvizsgálom ezen alternatív beavatkozások hipotetikus alkalmazását a lehetséges jövőbeli válsághelyzetekben. Végül a jövőbeli tendenciák és az amerikai döntéshozókra vonatkozó következmények rövid megvitatásával zárom.

A népirtás után egy interjúban a Pentagon feljegyzésének szerzője, aki elutasította az RTLM zavarását, kifejtette, hogy döntését részben az motiválta, hogy

hogy a zavarás felállítása heteket vett volna igénybe, és nem valószínű, hogy teljesen

elnyomja az RTLM- Más szóval, a zavarás költségei túl magasak voltak, tekintve a et.[8]

a siker bizonytalan valószínűsége. Ha az Egyesült Államok akkoriban modern kiberhadviselési képességekkel rendelkezett volna, és egy kibercsapással megbízhatóan és gyorsan ki tudta volna iktatni a rádióállomás sugárzási képességét, a racionális költség-haszon számítás egészen más lett volna. Talán elhallgattatták volna a gyűlölet jelzőfényét.

[8] Power, "A népirtás bámészkodói".

Elmélet

A nagyhatalmi beavatkozás számos tudományos megközelítése a költségek és hasznok nyelvezetére hivatkozik, akár implicit módon, akár explicit módon. Benjamin Miller a hidegháború utáni amerikai katonai beavatkozásokat azzal védte, hogy azok "a költségek és hasznok logikáját" követték.[9] Miller megfigyelése jó kiindulópont, de a a racionális költség-haszon döntés koncepcióját alaposabban meg kell vizsgálni.

A racionális költség-haszon döntés arról, hogy beavatkozzunk-e egy adott helyzetben, három összetevőből áll: a várható költségek, az észlelt előnyök és a siker becsült valószínűsége. Ezen összetevők mindegyikének több dimenziója van.

A költség és a haszon négy elsődleges dimenzión osztozik: 1) geopolitikai érdek, az elszenvedendő geopolitikai kár vagy a realizálandó geopolitikai előnyök; 2) anyagiak, az elköltendő "kincsek" mennyisége vagy a megnyerendő hadizsákmány; 3) belpolitika, a vezetők által a döntés meghozatalára fordított politikai tőke vagy a döntés meghozatalától várt rally-hatás; és 4) nemzetközi, a nemzetközi közösségnek a beavatkozásra adott válasza által létrehozott költségek vagy előnyök. A költségnek van egy ötödik dimenziója is: az emberi, a beavatkozás során elszenvedett áldozatok.

Bizonyos költségeket a kudarctól vagy a győzelemtől függetlenül kell megfizetni, és bizonyos előnyök az eredménytől függetlenül realizálódnak. Sok költséget és hasznot azonban csak az határoz meg, hogy a beavatkozás sikeres lesz-e. Ezért bármely lehetőség várható értékének kiszámításához a vezetőknek fel kell mérniük a siker valószínűségét. Formálisan fogalmazva,

[9] Benjamin Miller, "The Logic of US Military Interventions in the Post-cold War Era", *Contemporary*

Security Policy no19,. 3 (19981,. december): 72-109, https://doi.org/10.1080/13523269808404202, 73.

$$EV = (Bs - {}_{Cs})_{Ls} + (Bf - Cf)_{Lf}$$

Ahol EV a várható érték, B a haszon, C a költség, L a valószínűség, s a siker, f pedig a kudarc.

A racionális költség-haszon döntések sosem légüres térben születnek. Minden esetben különböző alternatívákat mérlegelnek egymással szemben, és az egyik alternatíva mindig az, hogy nem teszünk semmit. A többi alternatívához hasonlóan a status quo fenntartása is a fent vázolt dimenziók mentén hordoz előnyöket és költségeket. A vezetők azt a lehetőséget választják, amelyik a legmagasabb várható értékkel bír. A Pearl Harbor megtámadására vonatkozó japán döntéshez hasonlóan a várható

a döntés értéke lehet negatív is, amíg az alternatívák közül még mindig a legmagasabb.
[10]

A különböző válságok különböző ösztönzőket teremtenek. Egy távoli országban elkövetett népirtás jelentős nemzetközi előnyökkel járhat a beavatkozás szempontjából, de jelentős hazai tőkét igényelhet. Ezzel szemben, ha egy közeli szövetségest megtámadnak, a vezetőknek sokkal nagyobb belpolitikai károkat okozhat, ha nem avatkoznak be, mint ha a szövetséges segítségére sietnek. Nemzetközi szinten a vezetőknek a szuverenitás és a védelmi felelősség (R2P) egymással versengő normái között kell egyensúlyozniuk.[11]

[10] A Pearl Harbor megtámadásáról szóló japán döntésről a "gyalázatos dátumról" lásd Scott D. Sagan, "The Origins of the Pacific War", *The Journal of Interdisciplinary History* 18, no. 4 (1988): 893-922,

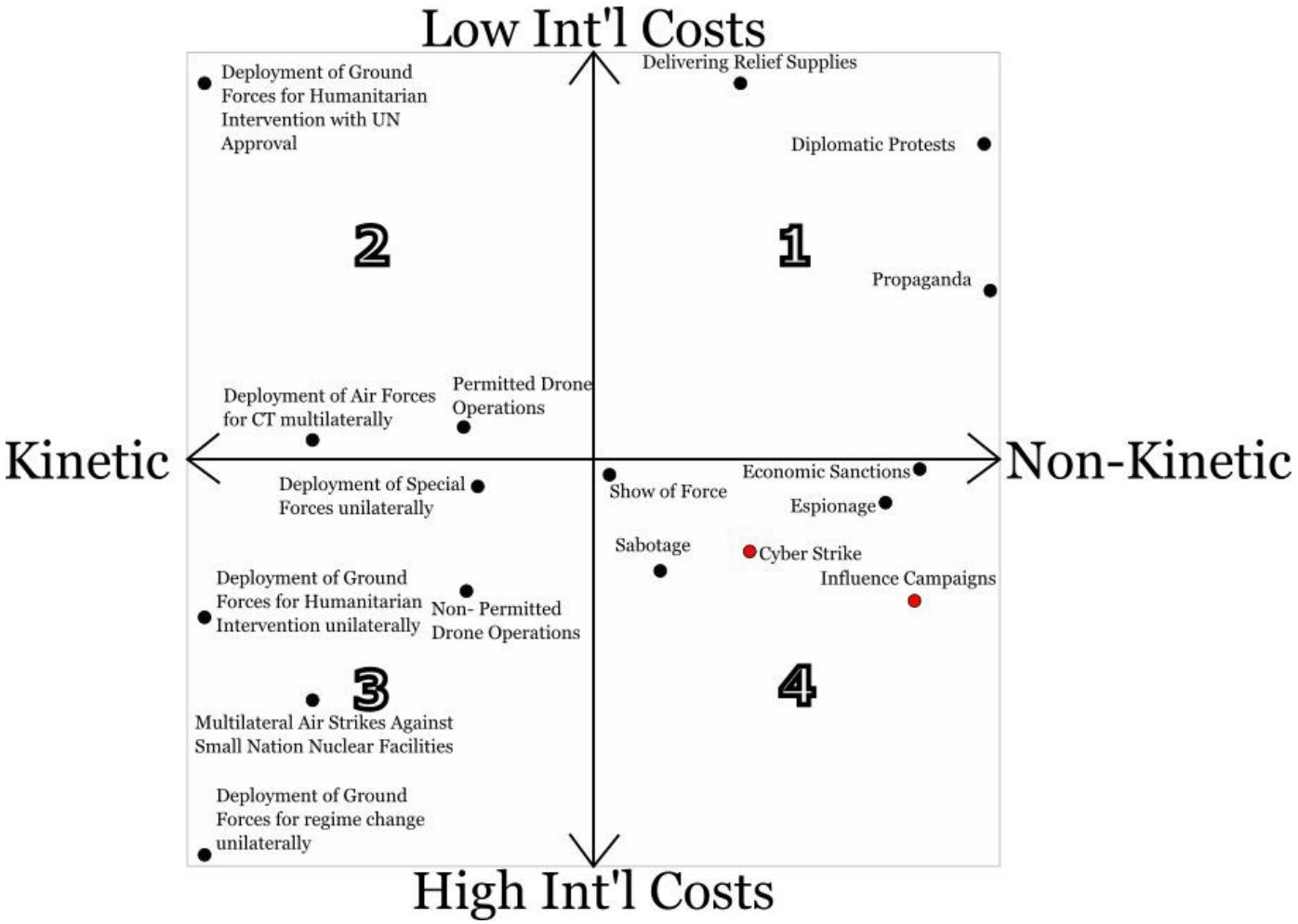
https://doi.org/10.2307/204828; Bruce M. Russett, "Pearl Harbor: Deterrence Theory and Decision Theory," *Journal of Peace Research* 4, no. 2 (June 1, 1967): 89-105, https://doi.org/10.1177/002234336700400201.

[11] Gareth Evans, Ramesh Thakur és Robert A. Pape, "Levelezés: A humanitárius beavatkozás és a védelmi felelősség", *International Security* 37, no. 4 (April 2013): 199-214, https://doi.org/10.1162/ISEC_c_00119.

A különböző típusú válságok esetében a költségek, az előnyök és a siker valószínűsége eltérőek, de ez nagyrészt a vezetők befolyásolási lehetőségein kívül esik. A vezetők azonban választanak a különböző típusú beavatkozások között. Ha például egy tömeggyilkosság kezdetével szembesülnek, a vezetők választhatnak a szárazföldi erőkkel történő beavatkozás vagy a kizárólag légi erővel történő beavatkozás között. Az előbbi sokkal valószínűbb, hogy sikeres lesz, de drámaian magasabb költségekkel jár.

A nagyhatalmak vezetői a lehetséges problémák és lehetőségek szédítő sokaságával szembesülnek, amelyek beavatkozáshoz vezethetnek - a polgárháborúktól és népirtásoktól kezdve az ellenséges nagyhatalmi beavatkozásokon át a saját hatalomátvétel lehetőségeiig -, és a válaszlehetőségek sokaságával rendelkeznek. Katonai beavatkozás esetén a nagyhatalmak szárazföldi erőket, különleges erőket küldhetnek be, vagy támaszkodhatnak a légierőre. Ezt megtehetik egyoldalúan, vagy a "tenni akarók koalíciójának" részeként, vagy az ENSZ hivatalos áldásával. A nem kinetikus beavatkozások esetében a nagyhatalmak diplomáciai tiltakozásokat tehetnek, szankciókat vezethetnek be, vagy szabotázst hajthatnak végre. Az alábbi ábra nagyjából bemutatja a politikai döntéshozók rendelkezésére álló válaszlehetőségek körét, bár nem teljes körű.

1. ábra: A beavatkozási lehetőségek tere



Az ábra 1egy durva heurisztika, amely a döntéshozók rendelkezésére álló lehetőségeket mutatja be. Az x-tengely azt mutatja, hogy a beavatkozási lehetőség mennyire kinetikus. Kvadránsok és 23ezért katonai beavatkozások. Az y-tengely a nemzetközi költséget jelöli, amely nagyjából azt mutatja, hogy a beavatkozás eszköze mennyire elfogadható a nemzetközi közösség számára (az ábrát úgy is létre lehetett volna hozni, hogy az y-tengelyen a költség más dimenzióit, vagy helyette a haszon egyik dimenzióját használják).

Az 1. ábra hasznossága nem a felsorolt lehetőségek pontos koordinátáiban rejlik, hanem abban, hogy megmutatja, hogy amikor a vezetők a beavatkozás mellett döntenek,

csak néhány

a beavatkozási lehetőségek katonai jellegűek lesznek, és képtelenség a lehetőségek csak felét figyelembe venni. A beavatkozók számára nem az alkalmazott eszközök számítanak, hanem csak az elért cél (a várható érték).

A vezetők ritkán tökéletesen racionálisak. Sok tényleges politikai tanácskozás során a költségeket lekicsinylik, az előnyöket eltúlozzák, és a siker valószínűségét felfújják. A fenti racionális költség-haszon keretrendszer azonban hasznos, bár szükségszerűen leegyszerűsített modell annak megértéséhez, hogy a vezetők hogyan hoznak döntéseket a beavatkozásról.

A keretrendszer legfontosabb következménye az, hogy ha a technológiai vagy stratégiai innovációk a meglévő lehetőségekhez képest alacsonyabb költségű alternatívát kínálnak - minden más tényező változatlansága mellett -, a döntéshozók valószínűleg ezt az alternatívát választják. Ez az egyértelmű ösztönzés látható a légi erő elsőbbségében a nyugati katonai beavatkozásokban, amióta annak hatékonysága az Öböl-háborúban bebizonyosodott. A légierő alacsonyabb költségű alternatívát kínált a nagyszabású szárazföldi műveletekkel járó nehézségekkel szemben.

Ez az írás a 4. kvadránsban található két új, a modern technológia által lehetővé tett beavatkozási lehetőségre összpontosít: a kibercsapásokra és a befolyásolási kampányokra. Mindkét lehetőség drámaian alacsonyabb költségekkel jár, mint a hagyományos katonai alternatívák.

Fogalommeghatározások

Sok, ha nem a legtöbb beavatkozásról szóló tudományos cikk nem határozza meg a témáját. A tudósok hajlamosak azt feltételezni, hogy a beavatkozás fogalma nyilvánvaló, hogy a beavatkozás a beavatkozás aktusa. Néhány kiemelkedő létező

definíció mindegyike fontos hibákkal küzd.

Martha Finnemore *A beavatkozás célja* című alapvető művében: *Changing Beliefs About the Use of Force című* munkájában a katonai beavatkozás definícióját adja meg, amely összefoglalja a hagyományos bölcsességet. Azt írja, hogy "a katonai beavatkozás a katonai személyzet elismert határokat átlépő bevetése a célállam politikai hatalmi struktúrájának meghatározása céljából".[12] Finnemore azonban elutasítja ezt a definíciót,

és a beavatkozás bármely meghatározását, mint túlságosan korlátozót. Ehelyett a beavatkozást az alapján határozza meg, hogy a beavatkozók beavatkozásnak nevezik-e azt. Finnemore beavatkozás-definíciójának van értelme egy olyan könyv kontextusában, amely a beavatkozások indoklásának változásait követi nyomon, de kevés útmutatást nyújt azoknak a tudósoknak, akik szeretnék kategorizálni, hogy pontosan mi számít beavatkozásnak, és mi nem.

Benjamin Miller a kinetikus oldalra összpontosít, és csak a katonai beavatkozást határozza meg. Az ő definíciója szerint "az egyik állam által egy másik állam szuverén területén történő különböző szintű csapatok telepítése olyan helyzetekben, amelyekben bizonyos valószínűséggel a telepítés ellenállásba ütközik, és a beavatkozó hatalomnak erőt kell alkalmaznia".[13] Miller definíciója azon túl, hogy kizárja a nem kinetikus beavatkozásokat, hibás:

a "terület" feltételezése annyira korlátozó, hogy vitathatóan kizárja a légierővel támogatott beavatkozások eseteit, mint például a NATO koszovói beavatkozása, amelyet Miller maga is elemez.

A beavatkozás kevés definíciója általában (a katonai beavatkozással szemben) gyakran túlságosan az ellenkező irányba tolódott el. Richard Little a beavatkozásról

szóló felmérésében megjegyzi, hogy "egy nem abszurd definíció szerint a beavatkozás egyenlővé tehető a következőkkel

[12] Martha Finnemore, *A beavatkozás célja*: *Changing Beliefs about the Use of Force* (Cornell University Press, 2013), 9.
[13] Miller, "Az amerikai katonai beavatkozások logikája a hidegháború utáni korszakban", 103.

a nemzetközi kapcsolatok egészét."[14] Hasonlóképpen, a beavatkozásról szóló egyik esszéjében, Stanley Hoffmann azzal nyitja, hogy "A téma gyakorlatilag ugyanaz, mint a

A [15]tág meghatározásoknak azonban éppoly kevés hasznuk van, mint a Túlságosan túlságosan szűkszavúaknak.

A beavatkozás jó meghatározásának ki kell zárnia minden olyan esetet, amely nem érdemel tudományos figyelmet, és be kell vonnia minden olyan esetet, amely igen - röviden, le kell fednie az ábrán bemutatott lehetőségek teljes terét, a használt eszközökre való 1,elfogultság nélkül. A beavatkozást a következőképpen határozom meg

> *egy vagy több állami szereplő arra irányuló kísérlete, hogy érdemben beavatkozzon egy másik állam belföldi műveleteibe egy olyan politikai cél elérése érdekében, amelyet sem a célzott lakosság, sem a célkormány nem kíván.*

Ez a meghatározás minden fontos esetet lefed, amelyet be kell vonni. A beavatkozókat az államokra korlátozza, és a beavatkozást az "értelmes" beavatkozásra korlátozza. Az "értelmes" egy gügye szó, de szükséges, és kizárja az olyan eseteket, mint például az USA csapatainak szövetséges nemzeteknél történő állomásoztatása. Az amerikai csapatok okinavai jelenlétét például bizonyára sok japán állampolgár nem kívánja, és van egy kívánt politikai célja, de az állomásoztatás nem éri el a japán belföldi műveletekbe való érdemi beavatkozás szintjét.

A beavatkozás korábbi meghatározásaihoz hasonlóan ez a meghatározás is csak olyan esetekre terjed ki, amikor a beavatkozás ellenzik vagy potenciálisan ellenzik, de eltér a korábbi meghatározásoktól, mivel lehetővé teszi, hogy az ellenállás a célállam kormányától származzon.

---

[14] Richard Little, "A beavatkozás felülvizsgálata: *Review of International Studies* no13,. 1 (1987): 49-60, 49.

[15] Stanley Hoffmann, *Janus és Minerva : Essays In The The Theory And Practice Of International Politics (Esszék a nemzetközi politika elméletéről és gyakorlatáról)*
(Routledge, 2019), 178.

vagy a népét. Erre a megkülönböztetésre azért van szükség, hogy az olyan eseteket, mint az amerikai drónháború Pakisztánban és a 2011-es szaúdi vezetésű bahreini beavatkozás, mindkettő a célország kormányának engedélyével történt.

Új beavatkozások

A fejlődő technológiák két új típusú beavatkozást tettek lehetővé, amelyek pontosan beleillenek az általam javasolt definícióba: a befolyásolási kampányok és a kibercsapások. Egyik beavatkozás sem "új" a céljait tekintve; mindkettő megfelel a nagyhatalmak azon történelmi vágyának, hogy beavatkozzanak riválisaik politikájába és korlátozzák ellenségeik aggasztó fegyverprogramjait. Mindkét új típusú beavatkozás azonban újszerű eszközökre támaszkodik, elsősorban az internet által lehetővé tett globális információs infrastruktúrára. Ez a szakasz áttekinti a befolyásolási kampányok és a kibercsapások első alkalmazására vonatkozó esettanulmányokat, hogy bemutassa, miért dönthetnek a vezetők racionálisan az ilyen beavatkozások indítása mellett. A fejezet egy folyamatban lévő befolyásolási kampány leírásával zárul.

A 2016-os orosz befolyásolási kampány

Az amerikai2016 elnökválasztás előtt az orosz állam "átfogó és rendszerszintű módon" beavatkozott.[16] Az amerikai hírszerző ügynökségek szerint Oroszország célja

hogy "aláássa a közvéleménynek az amerikai demokratikus folyamatba vetett hitét" és "segítse a megválasztott elnököt".

Trump választási esélyeit." Az orosz hadművelet korán kezdődött, majd 2014,nőtt

idővei [17]sokkal nagyobb.

[16] Robert Mueller, "Jelentés az elnökválasztásba2016 való orosz beavatkozással kapcsolatos vizsgálatról, I. kötet" (Washington, D.C.: Különleges ügyész, 2019. március).
[17] "Assessing Russian Activities and Intentions in Recent US Elections," Intelligence Community Assessment (Washington, D.C.: National Intelligence Council, 20176,. január), ii.

Az orosz befolyásolási kampánynak két fő ága volt. Először is, az orosz kormány a közösségi médiát használta a dezinformáció terjesztésére és az amerikai választókban való viszálykodásra fizetett trollok, az amerikai állampolgárokkal való közvetlen kapcsolatfelvétel és egy hatalmas bot-hálózat segítségével, amely képes volt felerősíteni a kiválasztott üzeneteket.[18] Másodszor, az orosz

a hírszerző ügynökségek hacker-műveleteket indítottak a Clinton-kampány és annak leányvállalatai ellen.[19] Ezután stratégiailag káros információkat terjesztett a Clinton-kampányról. több hónapon keresztül a nem főáramú médiával, a főáramú csatornákkal és a saját hazai propagandacsatornáival való kapcsolattartás révén. Oroszország tovább erősítette a káros információk közzétételét a közösségi médiában folytatott műveletével.

A befolyásolási2016 kampány rendkívül alacsony költségekkel járt Oroszország számára. Anyagi szempontból,

Oroszország becslések szerint havonta egymillió1.25 USD-t költött az internetkutatásra

Ügynökség, ami a nemzeti költségvetések birodalmában A művelet nem szenvedett jelentéktelen összeg.[20]

áldozatokkal és minimális hazai költségekkel járt. Geopolitikai szempontból Oroszország már elszigetelődött a Krím annektálása után, így a további amerikai szankcióknak nem volt sok hatása. Végül Oroszország megdöbbentően alacsony nemzetközi költséget fizetett. Tekintettel az alkalmazott technológiák újszerűségére, kevés konszenzus alakult ki arról, hogy a beavatkozás megsértette-e a nemzetközi jogot.[21] Ráadásul a beavatkozás haszonélvezője, Trump elnök.

[18] Mueller, "Jelentés az elnökválasztásba2016 való orosz beavatkozással kapcsolatos vizsgálatról, I. kötet".
[19] Mueller, "Jelentés az elnökválasztásba2016 való orosz beavatkozással kapcsolatos vizsgálatról, I.

kötet".
[20] "United States of America v. Internet Research Agency, et Al.," Indictment (Special Counsel, 201816,. február), https://www.justice.gov/file/1035477/download.
[21] Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law Symposium: Tallinn Manual on2.0 the International Law Applicable to Cyber Operations", *Texas Law Review* no95,. 7 (2017 2016): 1579-98.0

még azt sem szívesen ismerte el, hogy a Befolyásolási Kampány megtörtént, nemhogy erőteljes nemzetközi válaszlépéseket szervezzen.[22]

Nehéz meghatározni, milyen előnyökkel járt az oroszok számára a befolyásolási2016 kampány. Anyagilag, belpolitikailag vagy nemzetközi haszonból keveset nyert.

A kampány azonban előmozdította Oroszország "régóta fennálló" geopolitikai célját, hogy lejárassa a demokratikus Nyugat.[23] Ebben a tekintetben a művelet egyértelmű és átütő sikert aratott. siker: kevesen vitatják, hogy az amerikai demokrácia most erősebb, mint az orosz akció előtt volt. Trump elnök továbbá kézzelfogható orosz geopolitikai érdekeket támogatott, azt javasolva, hogy Oroszország csatlakozzon újra a G-8-hoz, és gratulált Putyinnak, miután újabb látszatválasztást nyert.[24]

A beavatkozás hatékonyságát is nehéz meghatározni. Putyin választása valóban megnyerte az elnökséget, de lehetetlen bizonyítani az ellenényt, hogy Trump elnök az orosz befolyásolási kampány nélkül is veszített volna. Trump elnök a három döntő közép-nyugati államot, Michigant, Pennsylvaniát és Wisconsint összesített77,744 szavazatokkal nyerte meg, és Oroszország ezeket az államokat különálló115 közösségi média kampányokkal célozta meg, amelyeket nagyrészt Clinton saját ellopott stratégiai feljegyzései alapján készítettek.[25] Ahogy azonban Nate Silver statisztikus rámutatott, lehetetlen elkülöníteni ezeknek a közösségi médiakampányoknak a hatását a nagyobb kampány erőfeszítéseihez képest, mert "az oroszok

[22] John Bowden, "Trump's Evolving Remarks on Russian Election Interference," Text, TheHill, június 1,2019, https://thehill.com/homenews/administration/446392-trumps-evolving-remarks-on-russian-election-interferencia.

[23] "Az orosz tevékenységek és szándékok értékelése a közelmúltbeli amerikai választásokon", ii.

[24] Amy Cheng Jilani Humza, "Trump on Putin: The U.S. President's Views, In His Own Words," *Foreign Policy* (blog), elérhető december14,ben. 2019, https://foreignpolicy.com/2018/07/18/trump-on-putin-the-u-s-president-in-his-own-words/.
[25] Philip Elliott, "The Mueller Report Doesn't Call Into Question Trump'2016s Win", *Time*, április h18,2019,ttps://time.com/5573537/mueller-report-russia-election-interference/.

a beavatkozási taktikák Orosz összhangban vannak azokkal az okokkal, amelyek miattClinton vesztett."[26]

a dezinformáció ugyanazokat a nyomásgyakorlási pontokat célozta meg, amelyeket Amerikában a Trump-párti választási ügynökök is megcéloztak.

Függetlenül a 2016-os befolyásolási kampány tényleges hatékonyságától, a nagyhatalmak által más kontextusban történő jövőbeni lehetséges elfogadása szempontjából a legfontosabb az *érzékelt* hatékonysága. Az a tény, hogy Oroszország továbbra is alkalmazza és finomítja a 2016-ban a világ más részein mutatott befolyásolási eszközeit, azt mutatja, hogy az orosz vezetők legalábbis úgy gondolják, hogy a művelet elég sikeres volt ahhoz, hogy megismétlődjön.[27]

A 2016-os orosz befolyásolási kampányt hagyományosan nem tekinthetjük beavatkozásnak, mivel Oroszországnak nem voltak életképes kinetikus lehetőségei. Mégis van haszna a racionális költség-haszon döntési keretrendszer alkalmazásának. A demokrácia aláásására és egy olyan jelölt támogatására irányuló céljának előmozdításában, akiről úgy vélte, hogy jobban megfelel az orosz érdekeknek, Putyinnak kevés alternatívája volt. Nem tehetett semmit, engedélyezhetett volna alacsony szintű dezinformációs kísérleteket, amelyek a szovjet korszak óta jellemzik az orosz politikát, vagy kombinálhatta volna a különböző új képességeket egy befolyásolási kampányban. Az utóbbi alternatíva nagyobb várható előnyökkel és nagyon kevés költséggel járt.

[26] Nate Silver, "How Much Did Russian Interference Affect The Election2016?", *FiveThirtyEight* (blog), február 16,2018, https://fivethirtyeight.com/features/how-much-did-russian-interference-affect-the-2016-election/.

[27] Laura Daniels, "How Russia Hacked the French Election", POLITICO, 2017. április 23., https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/; Davey Alba és Sheera Frenkel, "Russia Tests New Disinformation Tactics in Africa to Expand Influence," *The New York Times*, október sec30,2019,. Technológia, https://www.nytimes.com/2019/10/30/technology/russia-facebook-disinformation-africa.html.

A Stuxnet kibercsapás

2010 nyarán egy kis fehérorosz kiberbiztonsági cég furcsa e-mailt kapott egy iráni ügyféltől, amelyben részletezte, hogy egy számítógépe újraindítási hurokban ragadt. Az ezt követő hónapokban a világ kiberszakértői által végzett vizsgálat egy hihetetlenül kifinomult rosszindulatú programot tárt fel. A Stuxnet nevet kapta.[28]

A Stuxnet nagyságrendekkel bonyolultabb volt, mint bármelyik korábbi malware, és a célja nem volt azonnal nyilvánvaló a nyomozók számára, akik kezdetben attól tartottak, hogy a vírus általában ipari berendezéseket célzott A Stuxnet azonban meg.[29]

nem csak kifinomultságában különbözött elődeitől. Más vírusokkal ellentétben,

A Stuxnetnek volt egy meghatározott sor szükséges kiváltó feltétele, amely egy meghatározott építészet.[30] Ez vezetett Ralph Langner vezető kiberbiztonsági szakértőhöz, aki ezt úgy nevezte. "precíziós, katonai szintű kiberrakéta."[31]

Ma már tudjuk, hogy a Stuxnetet szinte biztosan az Egyesült Államok és Izrael hozta létre, hogy iráni nukleáris létesítményeket célozzon meg, és fizikailag elpusztítsa a fontos alkatrészeket.[32] A Symantec szakértői szerint a Stuxnet a dúsító centrifugák kimeneti frekvenciáját veszi célba több hónapon keresztül, megakadályozva a normál működést, amíg a

---

[28] Michael Joseph Gross, "A Declaration of Cyber-War", Vanity Fair, március h2,2011,ttps://www.vanityfair.com/news/2011/03/stuxnet-201104.

[29] Bruttó.

[30] T M Chen és S Abu-Nimeh, "Lessons from Stuxnet," *Computer* no44,. 4 (2011. április): 91-93, https://doi.org/10.1109/MC.2011.115, 91.

[31] Mark Clayton, "Stuxnet Malware Is 'weapon' out to Destroy Iran...'s Bushehr Nuclear Plant?," *Christian Science Monitor*, szeptember 21,2010, https://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nukleáris-üzem.

[32] Ralph Langner, "Stuxnet: *IEEE Security Privacy* 9, no. 3 (2011. május): 49-51, https://doi.org/10.1109/MSP.2011.67; Gross, "A Declaration of Cyber-War"; David E. Sanger, "Obama Ordered Wave of Cyberattacks Against Iran," *The New York Times*, June sec1,2012,. Közel-Kelet,

https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

centrifugák A Stuxnet vonzó voltamerikai végül szétrepülnek .[33] (és izraeli)

döntéshozók, mivel rendkívül alacsonyak a költségei. Anyagi szempontból a vírust a legtöbb magánszereplő nem tudta létrehozni, mivel kifinomult volt, és számos, rendkívül értékes exploitot tartalmazott.[34] A nemzeti költségvetésekhez képest azonban a vírus fillérekbe került - kevesebbe, mint egyetlen modern harci repülőgép.[35] Az USA nem szenvedett veszteségeket, sem

jelentős belpolitikai károkat okozhat. Geopolitikai szempontból Irán nagyrészt - bár nem teljesen - képtelen volt arra, hogy a támadásra természetben válaszoljon, és az amerikai kiberhadviselési kampány növelhette Irán ösztönzését arra, hogy tárgyalásokat folytasson a közös átfogó cselekvési tervről.[36] Nemzetközi szinten a kibertámadás burkolt jellege lehetővé tette az Egyesült Államok számára, hogy megússza a jelentős hírnévvesztést.[37]

A kibercsapás legfontosabb előnye közvetlenül kapcsolódik az iráni nukleáris program lassításának hatékonyságához. A Stuxnet több tízezer számítógépet fertőzött meg Iránban.

és évekig észrevétlen maradt.[38] Még a vírus nyilvános felismerése után is, Iránban

nem tudták megtisztítani a rendszerüket tőle, amíg a Irán eredetileg tagadta, hogy a korai 2012.[39]

---

[33] Eric Chien, "Stuxnet: Symantec Security Response, november h12,2010,ttp://www.symantec.com/connect/blogs/stuxnet-breakthrough.

[34] Thomas M. Chen, "Stuxnet, a kiberháború valódi kezdete? [Szerkesztői megjegyzés]," *IEEE Network* 24, no. 6 (November 2010): 2-3, A Stuxnet3. négy "nulladik napi" exploitot tartalmazott, amelyek elég értékesek ahhoz, hogy önmagukban több százezer dollárért eladják őket.

[35] James Farwell és Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival (*20111,. 53február): 23-40, 35.

[36] Wendy Sherman, "How We Got the Iran Deal", 2019. február 13., https://www.foreignaffairs.com/articles/2018-08-13/how-we-got-iran-deal; Ben Schaefer, "The Iran Nuclear Agreement as a Deterrent for Cyberattacks", Georgetown Security Studies Review,

augusztus. 18,2018,
https://georgetownsecuritystudiesreview.org/2018/08/18/the-iran-nuclear-agreement-as-a-deterrent-for-cyberattacks/.
[37] Farwell és Rohozinski, "Stuxnet és a kiberháború jövője". 31.
[38] Nicolas Falliere, Liam O'Murchu és Eric Chien, "W32.Stuxnet Dossier" (Symantec, 2011. február), 5. Thomas [39]Erdbrink és Ellen Nakashima, "Iran Struggling to Contain 'Foreign-Made' 'Stuxnet' Computer Virus," szeptember. 28,2010,
http://www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092706229.html; Mark

hogy a támadás a nukleáris program bármelyik elemét érintette volna, de Ahmadinezsád elnök később nyilvánosan elismerte, hogy centrifugákat semmisítettek meg.[40] Az Obama-kormányzat forrásai becslések szerint az iráni atomprogram másfél évvel visszavetette, és a nukleáris a Natanzban lévő ellenőrző kamerák néhány centrifuga roncsait és széles körű centrifugacsere.[41] Másrészt, a Stuxnet nem törölte el az iráni dúsulás, amely egy éven belül helyreállt.[42]

Végső soron a Stuxnet elsődleges hatása az volt, hogy drámaian megnövelte Irán nukleáris programjának költségeit. Nemcsak időt és energiát pazaroltak a hosszú és költséges tisztítási folyamatra, hanem az alkatrészek és szoftverek több éves teszteredményei is kétségessé váltak. A vírus felfedezése előtti években az iráni mérnökök az irányíthatatlanná vált centrifugákat hibás ellátmányra vagy emberi hibára fogták.[43]

A Stuxnet program története, amely része egy nagyobb kiberhadviselési erőfeszítésnek, amelyet a Egyesült Államok "olimpiai játékok", világosan mutatja, hogy a kibercsapás egy alternatíva a katonai beavatkozásra.[44] A program Bush elnök második feléből származik. a *New York Times* oknyomozó riportja szerint.[45] Az amerikai és szövetségesei évek óta próbálták szabotálni az Irán által importált alkatrészeket és készleteket, amelyeket az Irán

Hosenball, "Experts Say Iran Has 'Neutralized' Stuxnet Virus," *Reuters*, február h14,2012,ttps://www.reuters.com/article/us-iran-usa-stuxnet-idUSTRE81D24Q20120214.

[40] Mark Clayton, "Stuxnet: Ahmadinejad Admits Cyberweapon Hit Iran Nuclear Program," *Christian Science Monitor*, November 30,2010, https://www.csmonitor.com/USA/2010/1130/Stuxnet-Ahmadinejad-admits-cyberweapon-hit-Iran-nucle

ar-program.
[41] Sanger, "Obama elrendelte az Irán elleni kibertámadások hullámát".
[42] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies* no22,. 3 (20131,. július): 365-404, https://doi.org/10.1080/09636412.2013.816122.
[43] Sanger, "Obama elrendelte az Irán elleni kibertámadások hullámát". [44] Sanger, "Obama rendelte el az Irán elleni kibertámadások hullámát." [45] Sanger, "Obama rendelte el az Irán elleni kibertámadások hullámát".

nukleáris programot, kevés sikerrel.[46] Ezzel a kudarccal szembesülve, az elnök tagjai Bush belső köre, beleértve Cheney alelnököt is, katonai csapást sürgetett az iráni nukleáris létesítmények ellen. De a költségeket túl magasnak ítélték a bizonytalan haszonhoz képest.[47]

A racionális költség-haszon keretrendszerből nézve a kibercsapás kevésbé biztos hasznot, de drámaian alacsonyabb költségeket ígért. Bush elnök és később Obama elnök is a kibercsapás stratégiáját támogatta, mivel ez volt a legkevésbé költséges alternatíva.

A nagyhatalmakhoz intézett jövőbeli felhívás

Az iráni nukleáris program elleni Stuxnet-támadás egyértelműen olyan eset volt, amikor a katonai beavatkozás alternatívájaként a beavatkozás nem kinetikus eszközét választották. Az orosz2016 befolyásolási kampány abban különbözik, hogy Oroszországnak nem volt életképes katonai lehetősége arra, hogy beavatkozzon az amerikai belügyekbe. Mindkét eset azonban olyan képességeket mutat be, amelyek mostanra a nagyhatalmak vezetőinek beavatkozási lehetőségei közé kerültek.

Az orosz példa alapján a befolyásolási kampányokat két szükséges dimenzió jellemzi: először is a megosztó retorika és dezinformáció terjesztése a közösségi médián keresztül, hogy a lehető legszélesebb közönséghez jusson el; másodszor a kiberkémkedés, amelynek célja a káros politikai információk megszerzése és azok minél több csatornán keresztül történő terjesztése. A kibercsapásokat nem határozzák meg ilyen szigorúan, de a Stuxnet esetéből kiindulva a teljes mértékben digitális eszközökkel elért stratégiai hatások jellemzik. A Stuxnet azért volt eltérés a korábbi kiberhadviseléshez képest, mert

[46] Gross, "A kiberháborús nyilatkozat".

[47] Sanger, "Obama elrendelte az Irán elleni kibertámadások hullámát".

a kémkedésen túl, hogy elérjenek valamit, amit addig - egy újságíró szavaival élve - "csak úgy lehetett elérni, hogy lebombáztak egy országot, vagy ügynököket küldtek oda, hogy robbanóanyagokat helyezzenek el".[48]

Mindkét új beavatkozási mód drámaian alacsonyabb költségekkel jár, mint a hagyományos katonai alternatívák. Az egyik közös ok, amiért mindkettőnek ilyen alacsonyak a költségei, a titkosság és a tagadhatóság. Bár kevesen kételkednek abban, hogy Oroszország és az Egyesült Államok állt a befolyásolási kampány, illetve a vírus mögött, a nyílt felelősségvállalás hiánya lehetővé tette a két állam számára, hogy elkerüljék a nemzetközi visszhangot, amely a hagyományos beavatkozásokat követte volna. Ráadásul a műveletek nagyrészt rejtve maradtak mindkét ország belföldi közönsége előtt, így elkerülhetővé váltak a belföldi költségek. Természetesen az áldozatok hiánya lehetővé tette, hogy ezek a beavatkozások ne kerüljenek a figyelem középpontjába.

E beavatkozások vonzerejét mutatja, hogy az orosz befolyásolási kampánynak már van egy másolata: Kína éppen most folytatott befolyásolási kampányt Tajvanon a januári elnökválasztás előtt a hivatalban lévő

A Kínával szemben kritikusan nyilatkozó Tsai Ing-wen elnök és a kihívó Han Kuo-yu, aki

Kína-barátnak tekintik.[49]

Míg Kína esélyes jelöltje, Han Kuo-ju, vereséget szenvedett,

Kína fellépése a befolyásolási kampány mindkét kritériumát teljesítette. Először is, Kína

a közösségi média bőséges használata a megosztó retorika terjesztésére és Han Kuo-yu támogatására, annak

előnyben részesített jelölt.[50]

Kína korábban dezinformációt terjesztett a közösségi médián keresztül

[48] Sanger, "Obama elrendelte az Irán elleni kibertámadások hullámát".
[49] Joshua Kurlantzick, "How China Is Interfering in Taiwan's Election", Council on Foreign Relations, november h7,2019,ttps://www.cfr.org/in-brief/how-china-interfering-taiwans-election.
[50] Emily Feng, "Taiwan Gets Tough On Disinformation Suspected From China Ahead Of Elections," NPR.org, december 6,2019, https://www.npr.org/2019/12/06/784191852/taiwan-gets-tough-on-disinformation-suspected-from-china-ahead-of-elections; Kurlantzick, "How China Is Interfering in Taiwan's Election".

a helyi2018 választások során, több százezer alkalmazottat foglalkoztatva,

a tajvani tisztviselők szerint.[51] Az erőfeszítés legalább egy figyelemre méltó győzelmet hozott: Han

Kuo-yu saját meglepő megválasztása Kaohsiung polgármesterévé.[52]

Másodszor, Kína számos kibertámadást indított Tsai elnök pártja és a tajvani média ellen, bár nem ért el a DNC elleni orosz hackertámadással egyenértékű sikert.[53] Kína további intézkedéseket hozott, többek között hagyományos

a tajvani médiában, hogytovább terjesszék a Kína-barát üzeneteket és a katonai

erődemonstrációk a Tajvani-szorosban.[54] A V-Dem szerint a demokrácia

a svédországi Göteborgi Egyetem megfigyelési programja szerint Tajvanon minden más országnál több hamis információt terjesztenek külföldről.[55]

Az, hogy Kína befolyásolási kampányt indít Tajvan újraegyesítésének sürgetésére, racionális döntés. Egy invázió megindítása a sziget ellen hihetetlenül költséges lenne és

---

[51] Kuang-cheng Cheng és Yun Wang, "Democratic Taiwan Battling Disinformation From China Ahead of Elections", ford. Luisetta Mudie, Radio Free Asia, 2018. november 6., https://www.rfa.org/english/news/china/democratic-taiwan-battling-disinformation-11062018111310.html; Chris Horton, "Specter of Meddling by Beijing Looms Over Taiwan's Elections," *The New York Times*, november sec22,2018,. World, https://www.nytimes.com/2018/11/22/world/asia/taiwan-elections-meddling.html.

[52] Paul Huang, "Chinese Cyber-Operatives Boosted Taiwan's Insurgent Candidate," *Foreign Policy* (blog), elérhető december16,ben. 2019, https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/.

[53] Lawrence Chung, "Facebook Says It Will Target Fake News Ahead of Taiwan Election," South China Morning Post, 2019. november 5., https://www.scmp.com/news/china/politics/article/3036427/facebook-says-it-will-crack-down-fake-news-ahead-taiwan; "US and Taiwan Hold First Joint Cyber-War Exercise," *BBC News*, 2019. november 4., sec. Technology, https://www.bbc.com/news/technology-50289974.

[54] Aris Teon, "Taiwanese Government Says Some Local Media Work with China, Send Content to Beijing for Approval," *The Greater China Journal* (blog), május 6,2019, https://china-journal.org/2019/05/06/taiwanese-government-says-some-local-media-work-with-china-send-content-to-beijing-for-approval/; Bertil Lintner, "Asia Times | China's Influence Looms Darkly over Taiwan's Polls | Article," Asia Times, 2019. november 22., https://www.asiatimes.com/2019/11/article/chinas-influence-looms-darkly-over-taiwans-polls/.

[55] Anna Luhrmann et al., "Democracy Facing Global Challenges: V-Dem Annual Democracy Report 2019" (V-Dem, Göteborgi Egyetem, 2019. május),

https://www.v-dem.net/en/news-publications/democracy-reports/.

katasztrofális vereséggel végződhet, feltételezve az amerikai katonai ellenállást. A status quo elfogadása, ahogy Tajvan tovább halad a függetlenség felé, szintén ellenszenves a kínai vezetők számára. Ezzel szemben egy befolyásolási kampány alacsony költséggel járó potenciális előnyöket ígért.

Hipotetikus szemléltető esetek

Mivel a beavatkozás mindkét új típusa bizonyított némi olcsó hatékonyságot a való életben, a nagyhatalmak racionális vezetői minden bizonnyal fontolóra veszik majd az ilyen típusú beavatkozások elindítását a jövőbeli válságok esetén. Ez a szakasz az új beavatkozási eszközök két hipotetikus jövőbeli alkalmazását részletezi. Egyik eset sem tekinthető jóslatnak; mindkettő annak illusztrációja, hogy *a* nagyhatalmak hogyan reagálhatnának azokra a válságtípusokra, amelyek hagyományosan katonai beavatkozást váltottak ki.

Egy hipotetikus befolyásolási kampány

Ez a hipotetikus eset 2023-ban, a következő zimbabwei általános választások előtt következik be. Emmerson Mnangagwa kormánya inog, mivel a zimbabwei gazdaság továbbra is döcög. Az ellenzéki pártok egy népszerű elnökjelölt körül egyesültek, aki drámai reformokat ígér a nyolcvanéves hivatalban lévő elnökkel szemben, és a külföldi, elsősorban kínai befolyás csökkentését. A jelenlegi közvélemény-kutatások, bár hiányosak, elég nagy előnyt jeleznek az ellenzék számára ahhoz, hogy a korábbi szavazat-hamisítási gyakorlatok valószínűleg nem lennének elegendőek, és a nagyvárosokban zajló nagy utcai tüntetések tovább ássák alá a kormánypárt legitimitását. Nemzetközi nem kormányzati szervezetek szerint a tüntetők elleni

erőszakos fellépés valószínűvé válik, és egy esetleges polgárháborúra figyelmeztetnek.

A zimbabwei politikai válság dilemmát jelent a kínai vezetők számára. Zimbabwe nem közvetlen szövetséges, de fontos résztvevője az Övezet és Út kezdeményezésnek, és központi szereplője Kína afrikai geopolitikai ambícióinak, amelyek az elmúlt négy évben csak növekedtek.[56] Kína vezetői több alternatívát is mérlegelnek: nem tesznek semmit, és hagyják, hogy a

válságot, légi eszközöket küldjön Zimbabwébe, hogy segítsen a kormánynak elnyomni a tüntetéseket, küldjön szárazföldi erőket, hogy segítsen a kormánynak elnyomni a tüntetéseket, vagy indítson befolyásoló kampányt, hogy a választási egyensúlyt visszafordítsa a hivatalban lévő kormány javára.

A racionális költség-haszon döntés szemszögéből nézve minden lehetőség más-más várható értéket képvisel. Az egyes döntések dimenzióit az alábbi táblázat foglalja össze.

[56] Egyes jelentések szerint Kínának szerepe lehetett a 2017-es puccsban, amely Mnangagwa elnököt hatalomra juttatta. Ettől függetlenül a kínai érdekek Zimbabwében kiterjedtek. Lásd Nyshka Chandran, "China, Alleged to Have Influenced Zimbabwe Coup, Is Set to Benefit from Mugabe's Replacement," CNBC, november. 29,2017,

https://www.cnbc.com/2017/11/28/zimbabwe-coup-china-benefits-from-president-emmerson-mnangagwa-post-mugabe.html; Vasabjit Banerjee és Rich, "Diamonds and the Crocodile: Kína szerepe a zimbabwei puccsban," hozzáférés december 16,2019, https://thediplomat.com/2017/11/diamonds-and-the-crocodile-chinas-role-in-the-zimbabwe-coup/.

1. táblázat: Kínai lehetőségek a zimbabwei válsággal kapcsolatban

Alternatív	**Elsődleges előnyök**	**Elsődleges költségek**	**A siker valószínűsége**
Ne csinálj semmit	Geopolitikai: nincs Anyagi: nincs Belföldi: nincs Nemzetközi: nincs	Geopolitikai: közepes Anyagi: nincs Belföldi: nincs Nemzetközi: alacsony Emberi: nincs	Nagyon alacsony (Mnangagwa beavatkozás nélkül megtarthatja a hatalmat)
Légi beavatkozás	Geopolitikai: közepes Anyagi: alacsony Belföldi: nincs Nemzetközi: alacsony	Geopolitikai: alacsony Anyagi: közepes Belföldi: nincs Nemzetközi: közepes Emberi: alacsony	Közepes vagy magas
Földi beavatkozás	Geopolitikai: közepes Anyagi: alacsony Belföldi: nincs Nemzetközi: alacsony	Geopolitikai: alacsony Anyagi: magas Belföldi: alacsony Nemzetközi: magas Emberi: közepes	Magas
Befolyásolási kampány	Geopolitikai: közepes Anyagi: alacsony Belföldi: nincs Nemzetközi: nincs	Geopolitikai: nincs Anyagi: alacsony Belföldi: nincs Nemzetközi: alacsony Emberi: nincs	Alacsony vagy közepes

Ha Kína nem tesz semmit, azt kockáztatja, hogy elveszíti jelentős zimbabwei befektetéseit, és meggyengül a pozíciója Afrikában. Azonban egyik katonai opció sem vonzó. Mind a légi, mind a szárazföldi beavatkozás, különösen az utóbbi, nagyon magas anyagi és nemzetközi költségekkel jár, különösen azért, mert Kína korábban még nem hajtott végre ilyen műveleteket. Mindkettő akár amerikai válaszlépéseket is kiválthat. A jelentős, de nem elsöprő geopolitikai előnyök nem érnek fel ilyen következményekkel. Ezzel szemben egy befolyásolási kampány rendkívül alacsony költségekkel jár. Annak ellenére, hogy a siker valószínűsége csekély, a lehetséges nyereség vonzó alternatívává

teszi.

A hipotetikus forgatókönyv szerint a kínai vezetők könnyen dönthetnek úgy, hogy befolyásolási kampányt indítanak Zimbabwében, különösen a tajvani befolyásolási kampány kínai tapasztalatai és a közösségi média kínai felhasználása miatt, amellyel a hongkongi tiltakozásokat igyekeztek elhomályosítani.[57]

Egy hipotetikus kibercsapás

Ez a feltételezett eset valamikor a 2020-as években következik be, amikor a venezuelai politikai helyzet ismét rosszabbra fordul. Néhány év viszonylagos stabilitás után a venezuelai gazdaság ismét zuhanórepülésbe kezd, ami újabb menekülthullámot és heves utcai tüntetéseket indít el. A szomszédos országok küzdenek a menekültek befogadásáért, és nyíltan követelni kezdik Maduro elnök lemondását. Maduro úgy dönt, hogy erőszakot alkalmaz a menekültek és a tüntetők ellen, és a leghatékonyabb fegyvere a vidéki menekültoszlopok ellen az oroszok által szállított forgószárnyas repülőgépek.[58]

Ez a humanitárius válság Washingtonban vitát indít a lehetséges válaszlépésekről. Az Egyesült Államok régóta elítéli a venezuelai kormány cselekedeteit, és ahogy az Egyesült Államok az Öböl-háború után kötelességének érezte, hogy megvédje az iraki kurdokat Husszein fosztogatásaitól, úgy az amerikai vezetők is felelősnek érzik magukat azért, hogy megvédjék a venezuelai kormányt.

---

[57] Emily Stewart, "How China Used Facebook, Twitter, and YouTube to Spread Disinformation about the Hong Kong Protests," Vox, augusztus 20,2019, https://www.vox.com/recode/2019/8/20/20813660/china-facebook-twitter-hong-kong-protests-social-media; Emily Feng, "How China Uses Twitter And Facebook To Share Disinformation About Hong Kong," NPR.org, augusztus. 20,2019, https://www.npr.org/2019/08/20/752668835/how-china-uses-twitter-and-facebook-to-share-disinformation-about-hong-kong; Brenda Goh, "'All the Forces': Kína globális közösségi médiás nyomulása a hongkongi tüntetések miatt", *Reuters*, augusztus. 22,2019, https://www.reuters.com/article/us-hongkong-protests-china-socialmedia-idUSKCN1VC0NF.

[58] Oroszország már szállított helikoptereket és pilótaképzést Venezuelának. Lásd Alec Luhn és Harriet Alexander, "Russia Opens Military Helicopter Training Centre in Venezuela", *The Telegraph*, április. 2,2019, https://www.telegraph.co.uk/news/2019/04/02/russia-opens-military-helicopter-training-centre-venezu

ela/.

Venezuelai civilek. Az Egyesült Államoknak hat lehetséges lehetősége van: nem tesz semmit; légi erőket küld a repüléstilalmi zóna bevezetésére; szárazföldi erőket küld a menekültek és a tüntetők védelmére; különleges erőket küld a venezuelai helikopterek szabotálására; fokozza a szankciókat; vagy kibercsapást indít Venezuela légiereje ellen.[59] Ezeket a lehetőségeket a következő dokumentum foglalja össze
az alábbi táblázatban.

Ha nem teszünk semmit a válságra válaszul, az jelentős költségekkel jár, és potenciálisan lehetővé teszi, hogy az orosz és kínai befolyás még inkább beszivárogjon Latin-Amerikába. Ugyanakkor a katonai lehetőségek, még a repüléstilalmi zóna bevezetése is jelentős költségekkel jár. Ez részben az orosz katonai felszereléssel ellátott ellenféllel szembeni műveletek anyagi és emberi költségeiből adódik, de bármilyen amerikai katonai beavatkozás valószínűleg jelentős visszahatást váltana ki más latin-amerikai nemzetekből is, még azokból is, amelyek ellenzik a Maduro-rezsimet, tekintettel az USA latin-amerikai katonai kalandvágyának történetére.[60]

[59] Nem rendelkezem olyan technikai szakértelemmel, hogy bármilyen mértékben megbízhatóan meg tudnám mondani, hogy az Egyesült Államok jelenleg rendelkezik-e olyan kiberkészséggel, amely lehetővé tenné a venezuelai légierő földre kényszerítését, vagy hogy a venezuelai helikopterek sebezhetőek-e egy ilyen támadással szemben. E hipotetikus eset szempontjából feltételezem, hogy egy ilyen támadás lehetséges, ami hihetőnek tűnik.

[60] Karen DeYoung, "Trump latin-amerikai szövetségesei változást akarnak Venezuelában, de nem amerikai beavatkozást", *The Washington Post*, május. 9,2019, https://www.washingtonpost.com/world/national-security/trumps-latin-american-allies-want-change-in-venezuela-but-not-us-military-intervention/2019/05/08/d61b21e4-7106-11e9-9eb4-0828f5389013_story.html; Ciara Nugent, "Why Venezuela Revives Historical Tensions Over U.S. Intervention in Latin

America," *Time*, január. 25,2019,
https://time.com/5512005/venezuela-us-intervention-history-latin-america/.

2. táblázat: Az USA lehetőségei a venezuelai válsággal kapcsolatban

Alternatív	**Elsődleges előnyök**	**Elsődleges költségek**	**A siker valószínűsége**
Ne csinálj semmit	Geopolitikai: nincs Anyagi: nincs Belföldi: nincs Nemzetközi: nincs	Geopolitikai: közepes Anyagi: nincs Belföldi: alacsony Nemzetközi: alacsony Emberi: nincs	Nagyon alacsony (Maduro kormánya összeomolhat, és a helyzet stabilizálódhat).
Repülési tilalmi övezetek	Geopolitikai: közepes Anyagi: nincs Belföldi: alacsony Nemzetközi: közepes	Geopolitikai: nincs Anyagi: közepes Belföldi: alacsony Nemzetközi: közepes Emberi: alacsony	Magas
Földi beavatkozás	Geopolitikai: közepes Anyagi: alacsony Belföldi: alacsony Nemzetközi: alacsony	Geopolitikai: alacsony Anyagi: magas Belföldi: közepes Nemzetközi: magas Emberi: közepes	Magas
Különleges erők	Geopolitikai: közepes Anyagi: nincs Belföldi: nincs Nemzetközi: nincs	Geopolitikai: nincs Anyagi: alacsony Belföldi: alacsony (katasztrófa esetén magas) Nemzetközi: alacsony-közepes Emberi: alacsony (magas, ha katasztrofális)	Alacsony
Szankciók eszkalálása	Geopolitikai: közepes Anyagi: nincs Belföldi: nincs Nemzetközi: nincs	Geopolitikai: nincs Anyagi: alacsony Belföldi: nincs Nemzetközi: alacsony Emberi: nincs	Nagyon alacsony
Cyber Strike	Geopolitikai: közepes Anyagi: nincs Belföldi: nincs Nemzetközi: nincs	Geopolitikai: nincs Anyagi: alacsony Belföldi: nincs Nemzetközi: alacsony Emberi: nincs	Alacsony vagy közepes

A különleges erők bevetése többnyire elkerüli a nemzetközi visszahatást; ennek az alternatívának azonban magasak a katasztrofális kudarcok költségei, amint azt a Jemenben elszúrt rajtaütés2017 utóhatásai is mutatják.[61] A további szankcióknak valószínűleg kevés hatása lesz, mivel

súlyos szankciókat már kiszabtak, bár ez a lehetőség kevés költséggel jár. A kibercsapás ezzel szemben nagyon kevés költséggel jár, és nagyobb az esélye a sikerre, mint a szankcióknak. A költségek kulcsfontosságú meghatározója ennél az alternatívánál az, hogy az Egyesült Államok habozna-e a kulcsfontosságú nulladik napi sebezhetőségek kihasználásától, hogy azokat fontosabb küldetésekre mentse.

Az Egyesült Államok könnyen dönthet úgy, hogy katonai erőt alkalmaz, vagy elutasítja a választ egy jövőbeli venezuelai humanitárius válsághelyzetre. A kibercsapás indítása azonban a megfontolt alternatívák egyike lenne, és alacsony költségei miatt vonzó.

Jövőbeni tendenciák és következmények az amerikai politikai döntéshozók számára

Az elmúlt évtizedekben megjelent új technológiák új típusú beavatkozásokat tettek lehetővé. A jövőbeni technológiai fejlődés valószínűleg tovább javítja majd e beavatkozások hatékonyságát, miközben csökkenti a költségeket, elsősorban a mesterséges intelligencia területén bekövetkező lehetséges áttöréseknek köszönhetően. Bár még nem világos, hogy a mesterséges intelligencia milyen konkrét képességeket fog lehetővé tenni, a befolyásolási kampányokban használt chatbotok kis mértékű fejlesztése is drámaian hatékonyabb dezinformációs kampányokhoz fog vezetni.

anélkül, hogy egy embernek kellene fizetnie a Jelenleg azonban nem világos, hogy trollkodásért.[62]

[61] Eric Schmitt és David E. Sanger, "Rajtaütés Jemenben: *The New York Times*, 2017. február 1., sec. World, https://www.nytimes.com/2017/02/01/world/middleeast/donald-trump-yemen-commando-raid-questi ons.html.
[62] A MADCOM-ok, azaz a gépvezérelt kommunikációs eszközök kockázatairól lásd: Matt Chessen, *The MADCOM Future: Reprogramozás: Hogyan fogja a mesterséges intelligencia fokozni a számítógépes propagandát?*

A mesterséges intelligencia több képességet ad a támadónak vagy a védekezőnek, különösen a kibertérben, így a beavatkozásra való ösztönzésre gyakorolt általános hatása bizonytalan.[63]

Ezek az új beavatkozások egyszerre jelentenek kihívásokat és lehetőségeket az Egyesült Államok számára, amint azt a két első alkalmazásra vonatkozó esettanulmány is mutatja. Az amerikai politikai döntéshozóknak nagyobb eszköztár áll majd rendelkezésükre a nemzetközi válságokkal való szembenézéshez, de e válságok terjedelmét és súlyosságát negatívan befolyásolhatja, ha az ellenfelek ugyanezeket az új eszközöket használják. Amerika demokratikus szövetségesei, mint nyitott társadalmak, sebezhetőek a befolyásolási kampányokkal szemben. Ezzel szemben az USA többet nyerhet a kibercsapásokból, mivel kiberhadviselési képességei eltörpülnek azon kisebb nemzetek képességei mellett, amelyekben valószínűleg beavatkozik.[64]

Az itt bemutatott racionális költség-haszon döntési keretrendszer két fő következményt hordoz magában. Az első az, hogy ha a beavatkozás költségei elhanyagolhatóvá válnak egy nagyhatalom számára, akkor a beavatkozás folyamatos lehet. Amerika kibertámadásai az iráni atomprogram ellen valószínűleg a mai napig fennmaradnak, és Kína tajvani befolyásolási kampánya a januári választási kudarc ellenére szinte biztosan folytatódik a belátható jövőben.

A második következmény az, hogy minden racionális költség-haszon döntéstől el lehet téríteni. Ha az Egyesült Államok képes megemelni az ellenséges befolyásolási kampányok és kibercsapások költségeit és csökkenteni azok előnyeit, akkor ugyanúgy elrettentheti őket, mint a hagyományos katonai műveleteket.

Human Culture, and Threaten Democracy… and What Can Be Done About It (Atlantic Council, 2017),

http://www.atlanticcouncil.org/images/publications/The_MADCOM_Future_RW_0926.pdf.
[63] Az Emberiség Jövője Intézet jelentése szerint a mesterséges intelligencia kezdetben a támadó képességeket fogja előnyben részesíteni alacsony szintű beruházások esetén, de a nagyobb beruházásoknál a védekezést fogja előnyben részesíteni. Lásd Ben Garfinkel és Allan Dafoe, "How Does the Offense-Defense Balance Scale?", *Journal of Strategic Studies* 42, no. 6 (September 201919,): 736-63, https://doi.org/10.1080/01402390.2019.1631810.
[64] Lindsay, "Stuxnet és a kiberhadviselés határai".

A kibercsapások és a befolyásolási kampányok nem próbálnak meg semmi olyat elérni, amit a nagyhatalmak a történelem során ne próbáltak volna megtenni. Ehelyett ezek újszerű eszközök e célok elérésére, olyan eszközök, amelyek olcsóbbak, mint a katonai alternatívák. Az Egyesült Államok és más nagyhatalmak vezetőinek ma több lehetőség áll a rendelkezésükre, mint valaha.

Alba, Davey és Sheera Frenkel. "Oroszország új dezinformációs taktikákat tesztel Afrikában, hogy kiterjessze befolyását". *The New York Times*, 2019. október 30., sec. Technology. https://www.nytimes.com/2019/10/30/technology/russia-facebook-disinformat ion-africa.html.

"Az orosz tevékenységek és szándékok értékelése a közelmúltbeli amerikai választásokon". Intelligence Community Assessment. Washington, D.C.: National Intelligence Council, január h6,2017.ttps://www.dni.gov/files/documents/ICA_2017_01.pdf.

Bowden, John. "Trump változó megjegyzései az orosz választási beavatkozásról". Szöveg. TheHill, 2019. június 1. https://thehill.com/homenews/administration/446392-trumps-evolving-remarks-az-orosz-választási beavatkozásról.

Chen, T M és S Abu-Nimeh. "A Stuxnet tanulságai." *Computer* 44, no. 4 (2011. április): 91-93. https://doi.org/10.1109/MC.2011.115.

Chen, Thomas M. "Stuxnet, a kiberháború valódi kezdete? [A szerkesztő megjegyzése]." *IEEE Network* 24, no. 6 (2010. november): 2-3. https://doi.org/10.1109/MNET.2010.5634434.

Cheng, Kuang-cheng és Yun Wang. "A demokratikus Tajvan küzd a Kínából érkező dezinformációval a választások előtt". Fordította Luisetta Mudie. Radio Free Asia, 2018. november 6. https://www.rfa.org/english/news/china/democratic-taiwan-battling-disinformation-11062018111310.html.

Chessen, Matt. *A MADCOM jövője: Hogyan fokozza a mesterséges intelligencia a számítógépes propagandát, hogyan programozza át az emberi kultúrát és hogyan fenyegeti a demokráciát... és mit lehet tenni ellene*. Atlantic Council, 2017. http://www.atlanticcouncil.org/images/publications/The_MADCOM_Future_RW_0926.pdf.

Chien, Eric. "Stuxnet: A Breakthrough." Symantec Security Response, 2010. november 12. http://www.symantec.com/connect/blogs/stuxnet-breakthrough.

Chung, Lawrence. "Facebook Says It Will Target Fake News Ahead of Taiwan Election". South China Morning Post, 2019. november 5. https://www.scmp.com/news/china/politics/article/3036427/facebook-says-it-will-crack-down-fake-news-ahead-taiwan.

Clayton, Mark. "Stuxnet: Ahmadinezsád elismeri, hogy a kiberfegyver eltalálta az iráni nukleáris programot." *Christian Science Monitor*, 2010. november 30. https://www.csmonitor.com/USA/2010/1130/Stuxnet-Ahmadinejad-admits-cyberweapon-hit-Iran-nuclear-program.

---. "Stuxnet malware "fegyver" ki, hogy elpusztítsa ... Irán Bushehr atomerőművét?" *Christian Science Monitor*, 2010. szeptember 21.

https://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.

Daniels, Laura. "Hogyan hackelte meg Oroszország a francia választásokat." POLITICO, 2017. április 23. https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks.
/.

Danning, Gordon. "Vajon az RTLM rádió valóban érdemben hozzájárult-e a ruandai népirtáshoz? Using Qualitative Information to Improve Causal Inference from Measures of Media Availability." (Minőségi információk felhasználása a média elérhetőségének méréséből származó oksági következtetések javítására)." *Civil Wars* 20, no. 4 (2018. október 2.): 529-54. https://doi.org/10.1080/13698249.2018.1525677.

Destexhe, Alain. "A harmadik népirtás." *Foreign Policy*, no. 97 (1994): 3. https://doi.org/10.2307/1149436.

Elliott, Philip. "A Mueller-jelentés nem kérdőjelezi meg Trump 2016-os győzelmét". *Időpont*, 2019. április 18. https://time.com/5573537/mueller-report-russia-election-interference/.

Erdbrink, Thomas és Ellen Nakashima. "Iran Struggling to Contain 'Foreign-Made' 'Stuxnet' Computer Virus," 2010. szeptember 28. http://www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092706229.html.

Evans, Gareth, Ramesh Thakur és Robert A. Pape. "Levelezés: Humanitárius beavatkozás és a védelem iránti felelősség". *International Security* 37, no. 4 (2013. április): 199-214. https://doi.org/10.1162/ISEC_c_00119.

Falliere, Nicolas, Liam O'Murchu és Eric Chien. "W32.Stuxnet dosszié." Symantec, 2011. február. https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-044.pdf.

Farwell, James és Rafal Rohozinski. "A Stuxnet és a kiberháború jövője". *Survival* 53 (2011. február 1.): 23-40. https://doi.org/10.1080/00396338.2011.555586.

Feng, Emily. "Hogyan használja Kína a Twittert és a Facebookot a Hongkongról szóló dezinformációk megosztására". NPR.org, 2019. augusztus 20. https://www.npr.org/2019/08/20/752668835/how-china-uses-twitter-and-facebook-to-share-disinformation-about-hong-kong.

---. "Tajvan keményen fellép a Kínából feltételezett dezinformációval szemben a választások előtt." NPR.org, 2019. december 6. https://www.npr.org/2019/12/06/784191852/taiwan-gets-tough-on-disinformation-suspected-from-china-ahead-of-elections.

Forges, Alison De. "'Ne hagyj senkit, hogy elmesélje a történetet': Genocide in

Rwanda." New York: Human Rights Watch, 1999.

https://www.hrw.org/reports/1999/rwanda/Geno1-3-10.htm#P408_170340.

Garfinkel, Ben és Allan Dafoe. "Hogyan alakul a támadás-védelem mérleg?" *Journal of Strategic Studies* 42, no. 6 (2019. szeptember 19.): 736-63. https://doi.org/10.1080/01402390.2019.1631810.

Goh, Brenda. "'Minden erő': China's Global Social Media Push over Hong Kong Protests". *Reuters*, 2019. augusztus 22. https://www.reuters.com/article/us-hongkong-protests-china-socialmedia-idUSKCN1VC0NF.

Gross, Michael Joseph. "A kiberháborús nyilatkozat." Vanity Fair, 2011. március 2. https://www.vanityfair.com/news/2011/03/stuxnet-201104.

Habimana, Kantano. "Adás 1994. április 12-én." Fordította Fabien Nsengiyumva. RTLM, 1994. április 12. Concordia MIGS. http://migs.concordia.ca/links/documents/RTLM_16-17May94_eng_tape0002.pdf.

Hitimana, Noël. "Április 6-i adás." Fordította: UN. RTLM, 1994. április 6. http://migs.concordia.ca/links/documents/RTLM_06Apr94_eng_tape0122x.pdf.

Hoffmann, Stanley. *Janus és Minerva : Essays In The Theory And Practice Of International Politics*. Routledge, 2019. https://doi.org/10.4324/9780429036606.

Horton, Chris. "A pekingi beavatkozás kísértete a tajvani választások felett." *The New York Times*, 2018. november 22., sec. World. https://www.nytimes.com/2018/11/22/world/asia/taiwan-elections-meddling.html.

Hosenball, Mark. "Szakértők szerint Irán "semlegesítette" a Stuxnet vírust." *Reuters*, 2012. február 14. https://www.reuters.com/article/us-iran-usa-stuxnet-idUSTRE81D24Q20120214.

Huang, Paul. "Kínai kiber-műveletek erősítették Tajvan lázadó jelöltjét". *Foreign Policy* (blog). Accessed December 16, 2019. https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/.

Jilani, Amy Cheng, Humza. "Trump Putyinról: Az amerikai elnök nézetei saját szavaival". *Foreign Policy* (blog). Accessed December 14, 2019. https://foreignpolicy.com/2018/07/18/trump-on-putin-the-u-s-president-in-his.
-saját szavak/.

Kuperman, Alan J. *A humanitárius beavatkozás határai: Genocide in Rwanda*.

Brookings Institution Press, 2004.

Kurlantzick, Joshua. "Hogyan avatkozik be Kína a tajvani választásokba". Council on Foreign Relations, 2019. november 7. https://www.cfr.org/in-brief/how-china-interfering-taiwans-election.

Langner, Ralph. "Stuxnet: Dissecting a Cyberwarfare Weapon." *IEEE Security Privacy* 9, no. 3 (2011. május): 49-51. https://doi.org/10.1109/MSP.2011.67.

Lindsay, Jon R. "Stuxnet és a kiberhadviselés határai". *Security Studies* 22, no. 3 (2013. július 1.): 365-404. https://doi.org/10.1080/09636412.2013.816122.

Lintner, Bertil. "Asia Times | Kína befolyása sötéten árnyékolja be a tajvani választásokat | cikk." Asia Times, 2019. november 22. https://www.asiatimes.com/2019/11/article/chinas-influence-looms-darkly-over.
-taiwans-polls/.

Little, Richard. "A beavatkozás felülvizsgálata: A Survey of Recent Developments." *Review of International Studies* 13, no. 1 (1987): 49-60.

Luhn, Alec és Harriet Alexander. "Oroszország katonai helikopter kiképzőközpontot nyit Venezuelában." *The Telegraph*, 2019. április 2. https://www.telegraph.co.uk/news/2019/04/02/russia-opens-military-helicopter-training-centre-venezuela/.

Luhrmann, Anna, Lisa Gastaldi, Sandra Grahn, Staffan I. Lindberg, Laura Maxwell, Valeriya Mechkova, Richard Morgan, Natalia Stepanova és Shreeya Pillai. "A demokrácia a globális kihívásokkal szemben: V-Dem éves demokráciajelentés 2019." V-Dem, Göteborgi Egyetem, 2019. május. https://www.v-dem.net/en/news-publications/democracy-reports/.

Miller, Benjamin. "Az amerikai katonai beavatkozások logikája a hidegháború utáni korszakban". *Contemporary Security Policy* 19, no. 3 (1998. december 1.): 72-109. https://doi.org/10.1080/13523269808404202.

Mueller, Robert. "Jelentés a 2016-os elnökválasztásba való orosz beavatkozással kapcsolatos vizsgálatról, I. kötet". Washington, D.C.: Special Counsel, 2019. március. https://relayto.com/cdn/media/files/6hE5LFPORw2TKnEf8TkK_mueller-report%20(2).pdf.

Ndahiro, Kennedy. "Ruandában mindent tudunk a dehumanizáló nyelvről". The Atlantic, 2019. április 13. https://www.theatlantic.com/ideas/archive/2019/04/rwanda-shows-how-hateful-speech-leads-violence/587041/.

Ohlin, Jens David. "Megsértette-e a nemzetközi jogot az orosz kiberbeavatkozás a 2016-os választásokon?" Szimpózium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Tallinni kézikönyv 2.0 a

kiberműveletekre alkalmazandó nemzetközi jogról)". *Texas Law Review* 95, no. 7 (2017 2016):

1579-98.

Power, Samantha. "A népirtás bámulói". The Atlantic, 2001. szeptember 1. https://www.theatlantic.com/magazine/archive/2001/09/bystanders-to-genocide/304571/.

Russett, Bruce M. "Pearl Harbor: Pearl Harbor: Az elrettentés elmélete és a döntéselmélet." *Journal of Peace Research* 4, no. 2 (June 1, 1967): 89-105. https://doi.org/10.1177/002234336700400201.

Sagan, Scott D. "A csendes-óceáni háború eredete". *The Journal of Interdisciplinary History* 18, no. 4 (1988): 893-922. https://doi.org/10.2307/204828.

Sanger, David E. "Obama rendelte el az Irán elleni kibertámadások hullámát." *The New York Times*, 2012. június 1., sec. Közel-Kelet. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

Schaefer, Ben. "Az iráni nukleáris megállapodás mint a kibertámadások elrettentő ereje". Georgetown Security Studies Review, 2018. augusztus 18. https://georgetownsecuritystudiesreview.org/2018/08/18/the-iran-nuclear-agreement-as-a-deterrent-for-cyberattacks/.

Schmitt, Eric és David E. Sanger. "Rajtaütés Jemenben: Kockázatos a kezdetektől fogva és költséges a végén". *The New York Times*, 2017. február 1., sec. World. https://www.nytimes.com/2017/02/01/world/middleeast/donald-trump-yemen.
-commando-raid-questions.html.

Sherman, Wendy. "How We Got the Iran Deal", 2019. február 13. https://www.foreignaffairs.com/articles/2018-08-13/how-we-got-iran-deal.

Silver, Nate. "Mennyire befolyásolta az orosz beavatkozás a 2016-os választásokat?" *FiveThirtyEight* (blog), 2018. február 16. https://fivethirtyeight.com/features/how-much-did-russian-interference-affect-the-2016-election/.

Stewart, Emily. "Hogyan használta Kína a Facebookot, a Twittert és a YouTube-ot a hongkongi tüntetésekkel kapcsolatos dezinformáció terjesztésére". Vox, 2019. augusztus 20. https://www.vox.com/recode/2019/8/20/20813660/china-facebook-twitter-ho ng-kong-protests-social-media.

Straus, Scott. "Mi a kapcsolat a gyűlöletrádió és az erőszak között? A ruandai 'Radio Machete' újragondolása." *Politics & Society* 35, no. 4 (2007. december 1.): 609–37. https://doi.org/10.1177/0032329207308181.

Teon, Aris. "A tajvani kormány szerint egyes helyi médiumok Kínával dolgoznak együtt, tartalmukat Pekingbe küldik jóváhagyásra." *The Greater China Journal* (blog),

2019. május 6. https://china-journal.org/2019/05/06/taiwanese-government-says-some-local-.

media-work-with-china-send-content-to-beijing-for-approval/.

Thompson, Allan. *Média és tömeges atrocitás: A ruandai népirtás és azon túl*. McGill-Queen's Press - MQUP, 2019.

"Amerikai Egyesült Államok kontra Internet Research Agency, et Al." Vádirat. Különleges ügyész, február h16,2018.ttps://www.justice.gov/file/1035477/download.

"Az USA és Tajvan megtartotta első közös kiberháborús gyakorlatát." *BBC News*, 2019. november 4., sec. Technology. https://www.bbc.com/news/technology-50289974.

Wisner, Frank G. "Memorandum az elnök nemzetbiztonsági ügyekért felelős helyettes asszisztense számára, Nemzetbiztonsági Tanács. Ruanda: Zavarás a polgári rádióadásokban." Védelmi Minisztérium, 1994. május 5. https://nsarchive2.gwu.edu//NSAEBB/NSAEBB53/rw050594.pdf.

Yanagizawa-Drott, David. "Propaganda és konfliktus: Evidence from the Rwandan Genocide." *The Quarterly Journal of Economics* no129,. 4 (20141,. november): 1947–94. https://doi.org/10.1093/qje/qju020.