

**TERVEZET FOLYAMATBAN: Grant W. Turnerrel a
turnergw@mail.uc.edu címen, ha érdekli a közzététel.**

5G és nemzetközi biztonság: Hogyan lehet az Egyesült Királyság élenjáró?

By: Turner

Összefoglaló/összefoglaló: Az 5G és a Huawei körül zajló jelenlegi viták és azok megoldása jól láthatóan jelzik a globális rend technológiai alapú változásait, amelyek meghatározzák a 21. század alaphangját. Jelenleg úgy tűnik, hogy az USA-ban és a Kínában sokan a hidegháborús és Thuküdidész-csapda paradigmákat használják, zéróösszegű mentalitással. Legalábbis az 5G technológia esetében az Egyesült Királyság, úgy tűnik, árnyaltabb megközelítést alkalmaz.

Ez a cikk az Egyesült Királyság új Nemzeti Kiberbiztonsági Stratégiájának előkészítéskor jelenik meg, és a Huawei-t körülvevő 5G és kiberbiztonsági vitákat tekinti át rendkívül interdiszciplináris módon, valamint az olvasókat számos forráshoz irányítja. A diskurzusból gyakran hiányzó kérdések és megoldások elemzése mellett a cikk legfőbb hozzájárulása az az érv, hogy az Egyesült Királyság több lehet, mint a középút példája. Konkrétan, ha az Egyesült Királyság megnöveli és nemzetközivé teszi a Huawei Kiberbiztonsági Értékelő Központját, esetleg egy Nemzetközi Kiberbiztonsági Értékelő Központ létrehozásával, akkor vezetheti szövetségeseit és a világot az 5G, 6G, kiberbiztonság és nemzetközi kapcsolatok terén, betöltve egy létfontosságú vezetői vákuumot.

-Russell Huang a University College London biztonsági és bűnügyi tudományok szakán szerez BSc diplomát. Gyakornoki gyakorlatot végzett a CybSafe és a Nanyang Technológiai Egyetem (NTU) S. Rajaratnam School of International Studies (RSIS) részlegéhez tartozó Centre of Excellence for National Security (CENS) munkatársainál.

-Grant W. Turner a Cincinnati Egyetemen szerzett diplomát neveléstudományokból, a társadalmi változásokra összpontosítva a részvételi akciókutatáson keresztül, valamint interdiszciplináris tanulmányok alapszakon, nagyrészt a nemzetközi kapcsolatokkal kapcsolatos témákra összpontosítva.

-A szerzők mindketten részt vettek a Cambridge Security Initiative Nemzetközi Biztonsági és Hírszerzési Kezdeményezés 2019-es nyári programján és konferenciáján.

Tartalomjegyzék

	3	Bevezetés
		Első rész - Háttér
7		A Huawei felemelkedése
8		5G és a Huawei
		Második rész - Öt alapvető fenyegetés
	15	Hátsó ajtók
	17	Gyengeforráskód
	19	Potenciális monopólium
	31	5G hatásai a teljesítményre
	34	Egyesült Királyság-USA kapcsolatok
		Harmadik rész - Lehetőségek, kihívások és megoldások
		Lehetőségek
	37	AHCSEC nemzetközivé tétele
	39	Legyen HCSEC ICSEC
39		A kiberbiztonsági politika központjának kihívásai
40		Ellátási láncok
	43	5G előrelépők
	48	Kormányok, vállalatok és jogok
50		A társadalmi réteg
51		Innovatív megoldások
52		Zéró bizalom
	54	jövedelemalapú biztonság
54		Vörös sejtek/Vörös csapatok
55		Előre látó intelligencia
56		Komplex rendszerek paradigmái
57		Általános erőforrások
57		Nemzetközi kapcsolatok és biztonság
58		A KNK
59		Sokszínűség
63		Akciókutatás
64		Következtetés
	72	Bibliográfia

FOLYTATANDÓ TERVEZET: 5G és a nemzetközi biztonság 3

Erős érvek szólnak amellett, hogy a feltörekvő (információs) technológiákat, például a mesterséges intelligenciát, a kvantumszámítást és az 5G technológiákat irányító szereplő(k) fogja(k) irányítani a világot¹. Az 5G a vezeték nélküli kommunikáció következő generációja. Lehetővé teszi a nagyobb adatátviteli sebességet és gyakorlatilag minden technológia, azaz a dolgok internetének (IoT) integrálását².

A Huawei³, a Kínai Népköztársaságban (KNK) székhellyel rendelkező távközlési vállalat 2020⁵. január 28-tól világelső az 5G infrastruktúra⁴ és a telefonyártás területén.

A globális infrastruktúrában⁶ betöltött egyre központibb szerepe és a KNK-val⁷ szembeni kötelezettségei azonban a gazdasági és biztonsági aggodalmak⁸ középpontjába helyezték, különösen a liberális demokráciák⁹ számára.

Egyszerűen fogalmazva, "az 5G lesz ... a 21. századi gazdaság központi idegrendszere - és ha a Huawei folytatja az emelkedést, akkor Peking"¹⁰, irányíthatja azt.

Az Egyesült Államok (USA) a Huawei korlátozásától a betiltásig jutott, a közelmúltban benyújtva egy

¹ Graham Allison, "Is China Beating America to AI Supremacy?", *The National Interest*, 2019. december 22., <https://nationalinterest.org/feature/china-beating-america-ai-supremacy-106861>; Theresa Hitchens, "US Risks Losing 5G Standard Setting Battle to China, Experts Say," *Networks/Cyber. Breaking Defense*, 2020. május 11., <https://breakingdefense.com/2020/05/us-risks-losing-5g-standard-setting-battle-to-china-experts-say/>.

² Tom Wheeler, "5G in Five (not so) Easy Pieces" jelentés, The Brookings Institution, 2019. július 9., <https://www.brookings.edu/research/5g-in-five-not-so-easy-pieces/>; Scott Fulton III, "What is 5G? The Business Guide to Next-Generation Wireless Technology," *How 5G Will Transform Business, ZDNet*, 2019. szeptember 19., <https://www.zdnet.com/article/what-is-5g-the-business-guide-to-next-generation-wireless-technology/>; Klint Finley, "The WIRED Guide to 5G". *WIRED*. December 18., h2019. <https://www.wired.com/story/wired-guide-5g/>.

³ Karishma Vaswani, "Huawei: Egy ellentmondásos vállalat története", *BBC News*, 2019. március 6., <https://www.bbc.co.uk/news/resources/idx-sh/Huawei>.

⁴ Will Townsend, "Who is 'Really' Leading in Mobile 5G, Part 6: Policy, Regulation and Consortia," *Forbes*, 2019. október 12., <https://www.forbes.com/sites/moorinsights/2019/10/12/who-is-really-leading-in-mobile-5g-part-6-policy-regulation-and-consortia/#6f08dffd2755>.

⁴ Abrar Al-Heeti, "Huawei is the World's Top 5G Phone Vendor, Analyst Says" *CNET*, 2020. január 28., <https://www.cnet.com/news/huawei-is-the-worlds-top-5g-phone-vendor-analyst-says/>.

⁶ Daniel Araya, "Huawei's 5G Dominance in the Post-American World", *Forbes*, 2019. április 5., <https://www.forbes.com/sites/danielaraya/2019/04/05/huaweis-5g-dominance-in-the-post-american-world/#47d130c748f7>.

⁷ Samantha Hoffman és Elsa Kania, "Huawei and the Ambiguity of China's Intelligence and Counter-Espionage Laws," *The Strategist*, 2018. szeptember 13., <https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/>.

⁸ Andrew Eversden, "China's 5G Tech is a National Security Issue ... or is it a Trade One?", *C4ISRNET*, 2020. február 28., <https://www.c4isrnet.com/show-reporters/rsa/2020/02/28/huaweis-a-national-security-issue-or-is-it-a-trade-issue/>.

⁹ Steven Feldstein, "When it Comes to Digital Authoritarianism, China is a Challenge - But Not the Only Challenge", *War on the Rocks*, 2020. február 12., <https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/>.

¹⁰ Keith Johnson és Elias Groll, "The Improbable Rise of Huawei: How did a Private Chinese Firm come to Dominate the World's Most Important Emerging Technology?", *Foreign Policy*, 2019. április 3., <https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/>.

új büntetőjogi vádak egész sora ellene¹¹. Másokat is nyomást gyakorol, hogy kövessék a példáját, vegyes, ha nem kontraproduktív eredményekkel¹². Miközben a nemzetek az USA vezette egypólusú világból a lehetséges kétpólusú¹⁵, többpólusú¹⁶, nem-pólusú¹⁷ vagy Kína vezette¹⁸világba való lehetséges elmozdulással¹³ foglalkoznak, minden szem¹⁹ a két szuperhatalomra szegeződik.

A nagyhatalmi verseny mag-periféria jellege tükrözi az 5G verseny mag-periféria jellegét. Így az 5G és a Huawei körül zajló viták, valamint azok megoldása jól láthatóan jelzik a globális rend technológiai alapú változásait, és megadják a 21. század alaphangját. Az USA-ban és a KNK-ban sokan a hidegháborús és Thuküdidész-csapda paradigmákat használják, zéróösszegű mentalitással²⁰. Ez szükségtelen, kontraproduktív és veszélyes²¹.

¹¹ Sean Keane, "Huawei Ban Timeline," *CNET*, Hozzáférés: 2020. április 17. (rendszeresen frissítve), <https://www.cnet.com/news/huawei-ban-full-timeline-us-government-china-trump-security-threat-5g-p40/>.

¹² Panettieri, Joe. "Huawei: Melyik országban tilos és melyikben engedélyezett? Lista és GYIK." ChannelE2E és After Nines Inc. Hozzáférés 2020. március 10. <https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/>; Thomas D. Lairson, David Skidmore, and Wu Xinbo, "Why the US Campaign Against Huawei Backfired," *Trans-Pacific View, The Diplomat*, 2020. május 13., <https://thediplomat.com/2020/05/why-the-us-campaign-against-huawei-backfired/>.

¹³ Peter Harris, "When Will the Unipolar World End?: Hegemony is Premises on Dominance in Asia and Europe", (Mikor ér véget az egypólusú világ?: A hegemonia az ázsiai és európai dominanciára épül). *The National Interest*, május 27, 2019, <https://nationalinterest.org/feature/when-will-unipolar-world-end-59202>.

¹⁴ Nathan A. Sears, "Kína, Oroszország és a hosszú "egypólusú pillanat": How Balancing Failures are Actually Extending US Hegemony," *The Diplomat*, 2016. április 27., <https://thediplomat.com/2016/04/china-russia-and-the-unipolar-moment/>.

¹⁵ Andrew A. Michta, "A globális átrendeződés: *The American Interest*, 2020. január 17., <https://www.the-american-interest.com/2020/01/17/bipolarity-is-back/>.

¹⁶ Mark Y. Rosenberg, "Experts Get Multipolarity All Wrong," *Foreign Policy*, 2019. június 24., <https://foreignpolicy.com/2019/06/24/experts-get-multipolarity-all-wrong/>.

¹⁷ Richard N. Haass, "A nem-polaritás kora: *Foreign Affairs*, május-június, 2008, <https://www.foreignaffairs.com/articles/united-states/2008-05-03/age-nonpolarity>.

¹⁸ Bradley A. Thayer és John M. Friend, "The World According to China: Understanding the World China Seeks to Create by 2049, When the PRC Turns 100," *The Diplomat*, 2018. október 3., <https://thediplomat.com/2018/10/the-world-according-to-china/>; Robert D. Kaplan, "America Must Prepare for the Coming Chinese Empire," *The National Interest*, 2019. június 17., <https://nationalinterest.org/print/feature/america-must-prepare-coming-chinese-empire-63102>.

¹⁹ Laura Silver, Kat Devlin és Christine Huang, "China's Economic Growth Mostly Welcomed in Emerging Markets, but Neighbors Wary of its Influence," Pew Research Center: Global Attitudes and Trends, The Pew Charitable Trusts, 2019. december 5., <https://www.pewresearch.org/global/2019/12/05/chinas-economic-growth-mostly-welcomed-in-emerging-markets-but-neighbors-wary-of-its-influence/>; Lindsey Ford, "Refocusing the China Debate: American Allies and the Question of US-China "Decoupling", Blog-Order from Chaos, The Brookings Institution, 2020. február 7., <https://www.brookings.edu/blog/order-from-chaos/2020/02/07/refocusing-the-china-debate-american-allies-and-the-question-of-us-china-decoupling/>.

²⁰ Robert D. Kaplan, "Why the U.S.-China Cold War Will Be Different," *The National Interest*, January 19, 2020, <https://nationalinterest.org/blog/buzz/why-us-china-cold-war-will-be-different-114986>; Catherine Wong, "Thucydides Trap Author Graham Allison says China and US Must Work Together and Not End Up on Path that Leads to War," *Diplomacy, South China Morning Post*, December 20, 2018, <https://www.scmp.com/news/china/diplomacy/article/2178905/thucydides-trap-author-says-china-and-us-must-work-together-together-and>; Ben Lowson, "Does

Henry Kissinger szerint a KNK és a Nyugat közötti konfliktus "választás, nem pedig szükségszerűség"²². A kölcsönös félreértések és előítéletek képezik konfliktusaik²³ alapját. Ezek nemcsak az együttműködést és a pozitív versenyt ássák alá, hanem a békét, az elrettentést és a de-eszkalációt is, különösen a kibertérben. Továbbá ezek a tényezők növelik a nem szándékos konfliktusok²⁴ kockázatát. Az első világháború lehetséges geopolitikai és technológiai megismétlődését el lehet és el is kell kerülni²⁵.

E kihívások kezelése részben megköveteli, hogy értékeljük és javítsuk az 5G kiberbiztonsági politika jelenlegi helyzetét. Dr. Myriam Dunn-Cavelty és Dr. Andreas Wenger szerint a kiberbiztonsági politika a tudomány, a politika és a technológia²⁶ szférájának függvénye. Russell Huang 2019-ben írt, még nem publikált esszéjére építve az 5G kiberbiztonsági politika minőségi feltárása az Egyesült Királyság Huawei-hez és a KNK-hoz való politikai hozzáállására összpontosít, a globális kiberbiztonsági politika kontextusában elhelyezve. A feltárást két kérdés vezérli:

- Engedélyezni kell-e a Huawei számára az 5G kommunikáció fejlesztését az Egyesült Királyságban?
- Vannak-e olyan kihívások, lehetőségek és megoldások, amelyeket az 5G és a kiberbiztonsági politika nagyrészt figyelmen kívül hagy vagy kihagy, akár az Egyesült Királyságról, akár a világról van szó?

Sino-US Competition Mean a Zero-Sum Game?: It May, but it Doesn't Have to," *The Diplomat*, 2019. január 3., <https://thediplomat.com/2019/01/does-sino-us-competition-mean-a-zero-sum-game/>.

²¹Dani Rodrik, "Az amerikai és kínai jellemzőkkel bíró kapitalizmus békésen együtt tud létezni - ha feladjuk a 'hiper-globalizmust'", Comment-Opinion, *South China Morning Post*, április 12, 2019, <https://www.scmp.com/comment/insight-opinion/article/3005674/capitalism-us-usand-chinese-characteristics-can-peacefully>; Taylor M. Fravel, J. Stapleton Roy, Michael D. Swaine, Susan A. Thornton, and Ezra Vogel, "China is not an Enemy," Opinions, *The Washington Post*, 2019. július 3., https://www.washingtonpost.com/opinions/making-china-a-us-enemy-is-counterproductive/2019/07/02/647d49d0-9bfa-11e9-b27f-ed2942f73d70_story.html.

²² Henry A. Kissinger, "Az amerikai-kínai kapcsolatok jövője: *Foreign Affairs*, 91, no. 2 (2012): <https://www.jstor.org/stable/23217220>.

²³ Josh Kerbel, "Thinking Straight: *Studies in Intelligence* 48, no. 3 (2004): 27-35, <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol48no3/pdf/v48i3a03p.pdf>; Eric C. Anderson, *China Restored: The Middle Kingdom Looks to 2020 and Beyond*, Santa Barbara, California: Praeger, 2010; Kenneth Lieberthal és Wang Jisi, "Addressing U.S.-China Strategic Distrust", in *John L. Thornton China Center Monograph Series*, no. 4 (Washington D.C.: The Brookings Institution, 2012), https://www.brookings.edu/wp-content/uploads/2016/06/0330_china_lieberthal.pdf.

²⁴ Eric C. Anderson, *Sinophobia: The Huawei Story*, CreateSpace Independent Publishing Platform, 2013; Clay Wilson és Nicole Drumhiller, "US-China Relations: Cyber Espionage and Cultural Bias," In *National Security and Counterintelligence in the Era of Cyber Espionage*, szerkesztette Eugénie de Silva, 28-47, Hershey, PA, US: Information Science Reference, 2016; Michael Kolton, "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence," *The Cyber Defense Review* no. 1 (2017): 119-54, www.jstor.org/stable/26267405.²⁵ Evan Osnos, "The Future of Americas Contest with China," A Reporter at Large, *The New Yorker*, január 6., 2020, <https://www.newyorker.com/magazine/2020/01/13/the-future-of-americas-contest-with-china>.

²⁶ Myriam Dunn-Cavelty és Andreas Wenger, "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science," *Contemporary Security Policy* 41, no. 1 (2020): 5-32,

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 6**

<https://doi.org/10.1080/13523260.2019.1678855>.

Először is megvizsgáljuk a kiberbiztonsági politika, a nemzetközi kapcsolatok elméleteinek és a Kínai Népköztársaságnak a metszéspontját, áttekintjük a Huawei történetét, és elhelyezzük a Huawei-t a jelenlegi globális politikai környezetben. Ezután értékeljük a Huawei és az Egyesült Királyság (UK) 5G kapcsolatát. Ezt úgy tesszük, hogy foglalkozunk a Huawei öt fő fenyegetésével, ahogyan azt a szakirodalomban azonosítottuk:

- A Huawei potenciálisan hátsó ajtókat telepíthet a KNK számára
- Gyenge forráskód
- Annak kockázata, hogy a Huawei monopóliumot szerezhet az 5G felett
- Az 5G teljes körű kereskedelmi forgalomba kerülésének jövőbeli hatásai a villamosenergia-ellátásra
- Az Egyesült Királyság és az Egyesült Államok kapcsolataira, különösen a hírszerzési információk megosztására gyakorolt hatások

E veszélyek elemzése után feltárjuk és javasoljuk azokat a lehetőségeket, kihívásokat (különösen az alternatív szállítók által jelentett kockázatokat) és megoldásokat, amelyekkel az 5G-vitában nem vagy nem megfelelően foglalkoznak, ha egyáltalán foglalkoznak. Két elsődleges következtetésre jutunk.

Az első az, hogy Huang 2019-es esszéjének következtetése, miszerint az Egyesült Királyság számára a legjobb megoldás a kockázatsökkentő megközelítés, amely lehetővé teszi a Huawei számára, hogy felügyelet mellett, feltételesen fejlessze az 5G-t, úgy tűnik, hogy megállja a helyét. A Huawei-val való együttműködés mellőzése kontraproduktív. A Huawei-val való együttműködés lehetővé teszi az Egyesült Királyság számára, hogy a Huawei szolgáltatásainak előnyeit élvezze, miközben kezeli a kockázatokat. Továbbá a kockázatok elkerülése nem csökkenti az Egyesült Királyságot fenyegető veszélyt, és nem segíti elő annak helyzetét; a kockázatokkal való proaktív szembenézés a legjobb kockázatsökkentési stratégia²⁷.

Másodszor, mivel az Egyesült Királyság általánosságban és a Huawei-val kapcsolatban már elfogadott egy proaktív kultúrát, az 5G-vel kapcsolatos brit megközelítés mintául szolgálhat a világ Huawei-hez és a Kínai Népköztársasághoz fűződő kapcsolataira vonatkozó szélesebb körű stratégiák és taktikák számára. Különösen, ha az Egyesült Királyság növeli Huawei-jét Így, ahogy az Egyesült Királyság új nemzeti kiberbiztonsági stratégiáját készíti elő, mivel a jelenlegi stratégia 2021-ben²⁸ lejár, ez a cikk azt állítja, hogy az Egyesült Királyság jó helyzetben van ahhoz, hogy vezető szerepet vállaljon az 5G, a 6G²⁹, a kiberbiztonság és a nemzetközi kapcsolatok terén, különösen az USA megingó vezető szerepének összefüggésében.

²⁷ "5G Round-Up: A Round-Up of Published NCSC Content Following the UK Government's 5G Announcement," NCSC, január 31, 2020, <https://www.ncsc.gov.uk/information/5g-round-up>.

²⁸ "Nemzeti kiberbiztonsági stratégia 2016-2021", Policy Paper, HM Government, 2016. november 1., <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>; "National Cyber Security Strategy 2016-2021: Policy Paper, Cabinet Office, HM Government, május, h31,2019, <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021-progress>

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 8**

so-far; Conrad Prince és James Sullivan, "The UK Cyber Strategy: Challenges for the Next Phase," Briefing Papers, RUSI, 201927,. június, <https://rusi.org/publication/briefing-papers/uk-cyber-strategy-challenges-next-phase>.

²⁹ Andy Boxall, "Mi a 6G? It Could Make 5G Look Like 2G, but it's Not Even Close to Reality," Mobile, *Digital Trends*, 2020. február 3., <https://www.digitaltrends.com/mobile/what-is-6g/>; Iain Morris, "A 6G Arms Race May Define the 2020s," 6G, *Light Reading*, 2020. február 4., <https://www.lightreading.com/6g/a-6g-arms-race-may-define-the-2020s/a/d-id/757268>.

Első rész - Háttér

A Huawei felemelkedése

A Huawei 1987-ben alapította Ren Zhengei, aki 1984-ben hagyta ott a Kínai Népi Felszabadító Hadsereg (PLA) mérnöki és lehetséges hírszerzői pozícióját³⁰, alig néhány évvel azután, hogy a Kínai Népköztársaság 1978-ban³¹ Deng Xiaoping vezetésével megkezdte piaci reformjait. Ebben az összefüggésben kezdte meg vállalkozói útját, tanulmányozta a Nyugatot, és kisvállalkozói próbálkozásokkal próbálkozott³². Néhány társával (valószínűleg katonai és hírszerzési kapcsolatokkal) a Huawei a bimbózó technológiai központban, Sencsenben kezdte meg tevékenységét telefonkészülékek értékesítésével, majd fejlesztésével és gyártásával.

Ez végül egy jelentős P.L.A.-szerződéshez vezetett az 1990-es években. A Huawei 1995 belföldi értékesítése a jelentések szerint 220 millió USD körül volt. 1996-ban megkapta a "nemzeti bajnok" státuszt³³, ami megvédte a külföldi versenytől, és jelentősen növelte a sikerét. 2000-ben kezdett nemzetközi terjeszkedésbe, és 2005-re nemzetközi eladásai meghaladták a hazai eladásait.

A következő évtizedben a Huawei gyorsan terjeszkedett, különösen Európában, és számos jelentős nemzetközi távközlési és technológiai vállalattal³⁴ lépett partnerségre, illetve vásárolt be. A növekedés felkeltette a figyelmet. Legalább 2007-ig visszamenőleg az amerikai NSA elkezdte a Huawei hackelését, egyrészt azért, hogy kémkedjen a kínai tisztviselők után, másrészt azért, hogy hátsó ajtón keresztül hozzáférjen mindazokhoz, akik a Huawei termékeit³⁵ vásárolták. 2011-re már több mint 140 országban értékesített termékeket és szolgáltatásokat, 2012-re pedig "a világ legnagyobb távközlési berendezésgyártójává vált a bevételeket tekintve"³⁶. 2016 óta a 195-196³⁸ országból több mint 170-ben³⁷ képviselteti magát.

³⁰ Norman Pearlstine, David Pierson, Robyn Dixon, David S. Cloud, Alice Su és Max Hao Lu, "The Man Behind Huawei," *The Los Angeles Times*, 2019. április 10., <https://www.latimes.com/projects/la-fi-tn-huawei-5g-trade-war/>. ³¹ Yu Jie és Joseph Barnsley, "From Deng to Xi: Economic Reform, the Silk Road, and the Return of the Middle Kingdom," Special Report (023), LSE IDEAS, May, 2017, <http://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-From-Deng-to-Xi.pdf>.

³² Vaswani, "Huawei: A történet".

³³ Thomas A. Hemphill és George O. White III, "China's National Champions: *Thunderbird International Business Review* 55, no. 2 (2013. március/április), DOI: 10.1002/tie.21535.

³⁴ "Mérnökök - A Huawei-ről," Hozzáférés: 2020. február 20., <https://www.huawei.com/en/about-huawei/corporate-information/milestone>.

³⁵ David E. Sanger és Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," *Asia Pacific, The New York Times*, 2014. március 22., <https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?partner=rss&emc=rss&r=1>.

³⁶ Gong, Yeming. *Globális működési stratégia: Alapelvek és gyakorlat*. Berlin: Berlin: Springer-Verlag, pp2013., 62.

³⁷ "Mérnökök - A Huawei-ről".

³⁸ Attól függően, hogy hogyan számolod Tajvant, lásd: Matt Rosenberg, "The Number of Countries in the World," *Geography, ThoughtCo*, DotDash Publishing Company, February 27, 2020, <https://www.thoughtco.com/number-of-countries-in-the-world-1433445>.

5G és a Huawei

A Huawei felemelkedése azonban a valós és a várható viselkedés miatt riadalmat³⁹ keltett. Az 5G-ért folytatott csata csak fokozta a tétet⁴⁰. 2013 körül a Huawei elkezdett befektetni az 5G technológiába, és számos egyetemi, kormányzati és magánpartnerség társalapítója lett Európa-szerte⁴¹. 2018-ban a Huawei ígéretet tett arra, hogy 15-20 milliárd USD-t fektet be a kutatásba és fejlesztésbe, olyan feltörekvő 5G technológiákra összpontosítva, mint az autonóm autók, az intelligens városok és az IoT⁴². Ez a mai napig a tervek szerint halad: 2018-ban több mint 15 milliárd USD-t költött K+F-re, megelőzve⁴³ ezzel az Apple-t, 2019-ben⁴⁴ pedig több mint 17 milliárd USD-t fog költeni.

2019 közepére a Huawei legalább 50 nemzetközi szerződéssel rendelkezett 5G⁴⁵ fejlesztésére, 2020 februárjában pedig már 91 ilyen szerződésük⁴⁶ volt. Összehasonlításképpen, 2020 februárjában a legközelebbi versenytársak, az Ericsson és a Nokia 81, illetve⁴⁷ 65 5G-szerződéssel rendelkeznek, bár az Ericsson azt állítja, hogy más mérőszámok alapján az élen⁴⁸ áll. Az ilyen szerződések inkább a PR-hez használt mérőszámok, és ironikus módon a Huawei ezzel kapcsolatos kétes állításai, miszerint 18 hónapos előnyben van versenytársaival szemben, azokat szolgálják, akik alá akarnak menni a vállalatnak, mivel komoly fenyegetésként állítják be, különösen az Egyesült⁴⁹ Államokban.

Egyrészt 2013-as könyvében Dr. Eric C. Anderson⁵⁰ vezető amerikai hírszerzési elemző, északkelet-ázsiai szakértő és a National Intelligence University professzora több, a Huawei-re vonatkozó forrást 1,000⁵¹ elemez. Arra a következtetésre jut, hogy néhány szemölcs ellenére "a bizonyítékok ...

³⁹ Tripti Lahiri és Mary Hui, "Betiltva: *Quartz*, május 28., h2019, <https://qz.com/1627149/huaweis-journey-to-becoming-us-tech-enemy-no-1/>.

⁴⁰ Zen Soo, Zheping Huang, Sarah Dai és Li Tao, "SCMP sorozat: *South China Morning Post*, február-június, h2019, <https://series.scmp.com/5g/>.

⁴¹ "Mérőföldkövek - A Huawei-ről".

⁴² Sijia Jiang, "China's Huawei to Raise Annual R&D Budget to at Least \$15 Billion," *Technology News, Reuters*, 2018. július 26., <https://www.reuters.com/article/us-huawei-r-d/chinas-huawei-to-raise-annual-rd-budget-to-at-least-15-billion-idUSKBN1KG169>.

⁴³ "No Pay, No Gain: Huawei Outspends Apple on R&D for a 5G Edge," *New Economy, Bloomberg News*, április 25, 2019, <https://www.bloomberg.com/news/articles/2019-04-25/huawei-s-r-d-spending-balloons-as-u-s-tensions-flare-over-5g>.

⁴⁴ Yash Mishra, "A Huawei idén több mint 17 milliárd dollárt fektet K+F-be", *News, Huawei Central*, 2019. július 30., <https://www.huaweicentral.com/huawei-will-invest-over-17-billion-in-rd-this-year/>.

⁴⁵ Rita Liao, "Huawei Says Two-Thirds of 5G Networks Outside China Now Use its Gear," *TechCrunch*, június 25, h2019, <https://techcrunch.com/2019/06/25/huawei-wins-5g-contracts/>.

⁴⁶ Ray Le Maistre, "Huawei's Ding Gets Emotional About 5G, Boasts 91 Deals," *5G, Light Reading*, február 20, h2020, <https://www.lightreading.com/5g/huaweis-ding-gets-emotional-about-5g-boasts-91-deals/d/d-id/757629>.

⁴⁷ Ibid.

⁴⁸ Chris Nuttall, "Ericsson Claims 5G Leadership Over Huawei," *Technology Sector, Financial Times*, február 13, 2020, <https://www.ft.com/content/9cdf33f0-4e8e-11ea-95a0-43d18ec715f5>.

⁴⁹ Iain Morris, "Huawei's '18-Month Lead' in 5G is Telecom's Most Spurious Claim," *5G, Light Reading*, 2020. március 9., <https://www.lightreading.com/5g/huaweis-18-month-lead-in-5g-is-telecoms-most-spurious-claim/a/d-id/758064>.

⁵⁰ Anderson, *Sinophobia*.

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 11**

⁵¹ Sajnos Dr. Anderson meghalt, amit 2018-ban fedeztünk fel, amikor megpróbáltuk nyomon követni a Huawei-elemzését.

azt sugallja, hogy az amerikai kongresszus boszorkányüldözést folytat⁵². Továbbá nagyon meggyőzően érvel amellett, hogy az amerikai vádak szinte teljesen alaptalanok.

Inkább a rasszizmus, a különleges érdekek, a védelmi költségvetés indoklása, a fenyegetett hegemon stáusz, valamint a Nyugat és Kelet közötti kölcsönös gyanakvás és félreértés kombinációját tükrözik. Továbbá, a versengéstől való félelem aláássa a hagyományos amerikai és nyugati megfogalmazásokat arról, hogy hogyan lehet a legjobban megvédeni az érdekeiket, ami viszont önpusztító következményekkel jár. 2019 májusában a *ZDNet* egyik vezető technológiai szerkesztője hasonló érvet⁵³ fogalmazott meg.

Megjegyezi, hogy bár a Huawei és a KNK valóban fenyegetést jelent, a Huawei, a KNK, az USA és mások gazdasági és biztonsági érdekei általában visszatartják az ellenséges lépéseket. Továbbá rámutat arra, hogy nincsenek megalapozott jelentések az államilag támogatott rosszindulatú szoftverekről vagy más fenyegetésekről, amelyeket a Huawei állítólag képvisel. Ehelyett amellett érvel, hogy a nemzetközi figyelemnek a nagyobb kiberbiztonsági kockázatokra kellene összpontosítania, beleértve a más államok, például Észak-Korea és Irán, a bűnözők és az iparági/tervezési alapú kockázatokat. Ezekben az összefüggésekben még a Google is azt mondta, hogy a Huawei-jel való együttműködés megtiltása veszélyezteti a biztonságot az Egyesült Államokban és máshol⁵⁴.

Másrészt a Huawei legalább a Cisco szellemi tulajdonának⁵⁵ 2002-es "eltulajdonításáig" visszamenőleg már régóta törvénytelen és etikátlan magatartást tanúsít. Ez a minta magában foglalja a megvesztegetést⁵⁶, a korrupciót⁵⁷, az ipari kémkedést⁵⁸, a lopás⁵⁹ különböző formáit, az Iránnal⁶⁰ és Észak-Koreával⁶¹ szembeni szankciók megsértését, az ellene a közelmúltban a RICO-ügyben indított vádakot a

⁵² Anderson, *Sinophobia*, könyvösszefoglaló.

⁵³ Jason Perlow, "A paranoia elpusztít minket: Tech Broiler, *ZDNet*, 2019. május 20., <https://www.zdnet.com/article/paranoia-will-destroy-you-why-chinese-tech-isnt-spying-on-us/>.

⁵⁴ Dieter Bohn, "Google is Reportedly Arguingly that Cutting Huawei Off From Android Threatens US Security," *The Verge*, június 7, 2019, <https://www.theverge.com/2019/6/7/18656163/google-huawei-android-security-ban-claims>.

⁵⁵ Mark Chandler, "A Huawei és a Cisco forráskódja: Executive Platform, *Cisco Blogs*, 2012.11. október, <https://blogs.cisco.com/news/huawei-and-ciscos-source-code-correcting-the-record>.

⁵⁶ Masood Farivar, "Bribery, Corruption Charges Follow Huawei Around the World," East Asia Pacific, *VOA News*, 2019. február 11., <https://www.voanews.com/east-asia-pacific/bribery-corruption-charges-follow-huawei-around-vilag>.

⁵⁷ Ibid.

⁵⁸ Larry Chaffin, "A 60 Minutes percek alatt megtorpedózza a Huawei15: Putting Realism into Your Network, *Network World*, 2012. október 7., <https://www.networkworld.com/article/2223272/60-minutes-torpedoes-huawei-in-less-than-15-minutes.html>. ⁵⁹ Abrar Al-Heeti, "US Hammers Huawei with Indictments23 for Alleged Trade Secret Theft, Fraud," *CNET*, 2019. január 29., <https://www.cnet.com/news/us-hammers-huawei-with-23-indictments-for-alleged-trade-secret-theft-fraud/>; Chuin-Wei Yap, Dan Strumpf, Dustin Volz, Kate O'Keeffe és Aruna Viswanatha, "Huawei's Yearslong Rise is Littered With Accusations of Theft and Dubious Ethics," *Tech, The Wall Street Journal*, május 25, 2019, <https://www.wsj.com/articles/huaweis-yearslong-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858>.

⁶⁰ Steve Stecklow, "Exkluzív: Technology News, *Reuters*, március 2, 2020, <https://www.reuters.com/article/us-huawei-iran-sanctions->.

USA⁶², valamint számos más jogi és biztonsági kérdés⁶³(a *CNet* részletes és rendszeresen frissített idővonalat is közöl a Huawei nemzetközi fejleményeiről és problémáiról, egészen januárig 2018⁶⁴ visszamenőleg). *Nem is* beszélve a Huawei központi szerepéről a Kínai Népköztársaság belső elnyomási taktikájában, különösen Hszincsiangban⁶⁵.

Ezek az aggodalmak 2014-ben fokozódtak, amikor a KNK elfogadta a kémelhárítási törvényt, majd 2017-ben, amikor elfogadta a nemzeti hírszerzési törvényt⁶⁶. Különösen a 2017-es törvény készítetett számos országot arra, hogy különböző mértékben⁶⁷ betiltsa vagy korlátozza a Huawei-t, különösen az 5G hálózatoktól. Nyelvezete világossá teszi, hogy miért:

Minden szervezet és állampolgár köteles a törvénynek megfelelően támogatni, segítséget nyújtani és együttműködni a nemzeti hírszerzési munkában, és köteles a tudomására jutott nemzeti hírszerzési munka titkosságát megőrizni. Az állam védi a nemzeti hírszerzési munkát⁶⁸ támogató, azzal együttműködő és abban közreműködő személyeket és szervezeteket.

2020. február 3-ig azonban úgy tűnik, hogy nincs nyilvános bizonyíték az államilag támogatott kémkedésre a Huawei⁶⁹ révén.

Dr. James A. Lewis, a CSIS rangidős alelnöke és technológiapolitikai programjának igazgatója szerint a teljes tilalom a legjobb módja annak, hogy megvédjük magunkat a Huawei és a Kínai Népköztársaság által jelentett⁷⁰ kockázatoktól. Ennek oka az, hogy az 5G jellege miatt nehéz, ha nem is

[exclusive/exclusive/exclusive-newly-obtained-documents-show-huawei-role-in-shipping-prohibited-u-s-gear-to-iran-idUSKBN20P1VA](#).

⁶¹ Joseph Kim, "Huawei's Puzzling Wireless Project in North Korea," George W. Bush Presidential Center, szeptember 3, 2019, <https://www.bushcenter.org/publications/articles/2019/09/huawei-wireless-north-korea.html>. ⁶² "A Huawei kínai távközlési konglomerátum és leányvállalatai ellen vádak a zsarolással kapcsolatos összeesküvés és a

Conspiracy to Steal Trade Secrets," Justice News, US Department of Justice - Office of Public Affairs, 2020. február 3., <https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subidiaries-charged-racketeering>.

⁶³ "A Huawei tranzakciós kockázati profilja." RWR tanácsadó csoport. 2018. február 13. <https://www.rwradvisory.com/wp-content/uploads/2019/03/RWR-Huawei-Risk-Report-2-13-18.pdf>. ⁶⁴ Sean Keane, "A Huawei betiltásának idővonala".

⁶⁵ Zak Doffman, "A Huawei-t lopással és kétes etikával" vádolják - De nem ez a legrosszabb". *Innovation, Forbes*, 2019. május 25., <https://www.forbes.com/sites/zakdoffman/2019/05/25/huawei-accused-of-theft-and-dubious-ethics-why-it-should-come-as-no-surprise/#296527373f59>.

⁶⁶ Hoffman és Kania, "Kína törvényei".

⁶⁷ Panettieri, "Huawei Engedélyezett tiltott".

⁶⁸ Hoffman és Kania, "Kína törvényei".

⁶⁹ Brad Glosserman, "Huawei and the Realities of the 5G World", Commentary/World, *The Japan Times*, 2020. február 3., <https://www.japantimes.co.jp/opinion/2020/02/03/commentary/world-commentary/huawei-realities-5g-world/#.Xptzo-pKjIV>.

⁷⁰ James Andrew Lewis, "A Szenátus Kereskedelmi, Tudományos és Közlekedési Bizottsága - 5G ellátási lánc biztonsága: Lewis szóbeli tanúvallomása", tanúvallomás, CSIS, 2020. március 4., https://csis-prod.s3.amazonaws.com/s3fs-public/congressional_testimony/200304_Oral_Testimony.pdf?eMPCUCg_p48O8hSNQR7AgV_b3pYHpBeP.

lehetetlen, hogy a maghálózatokat, különösen a kritikus maghálózatokat elkülönítsük az úgynevezett "peremhálózatoktól", ahol a végfelhasználói eszközök kapcsolódnak a maghálózatokhoz⁷¹.

Simeon Gilding, az ASPI vezető munkatársa, aki 2019 decemberéig az Ausztrál Hírközlési Igazgatóság jelhírszerzési és offenzív kibermiszióinak vezetője volt, tagja volt annak a csapatnak, amely megállapította, hogy Ausztrália nem támaszkodhat a részleges 5G-tilalomra a core-edge probléma miatt, és nagyon szkeptikus a részleges tilalomra⁷² támaszkodó tervekkel szemben. Dr. Lewis nyitottabbnak tűnik a vitára a core-edge elválasztás hatékonyságáról, de kijelenti, hogy azok, akik úgy érzik, hogy mérsékelni tudják a Huawei kockázatait, csak akkor tehetik ezt meg, ha végigvizsgálják a biztonsági terveiket⁷³.

Az Öt Szem hírszerzési megosztási szövetség (amely az Egyesült Királyságból, az Egyesült Államokból, Kanadából, Ausztráliából és Új-Zélandból áll) közül Ausztrália⁷⁴ és Új-Zéland⁷⁵ volt az első, amely 2018-ban teljes mértékben kitiltotta a Huawei-t az 5G infrastruktúrájából. Az Egyesült Államok 2012⁷⁶ óta arra ösztönzi a vállalatokat, hogy ne használják a Huawei berendezéseit a hálózataikban. A közelmúltban számos import- és exportkorlátozást vezetett be a vállalatra, és 2019 májusában egy végrehajtási rendelet⁷⁷ révén gyakorlatilag kitiltotta a Huawei-t az összes amerikai távközlési hálózatból. A Huawei azonban többször is haladékot kapott a tilalom alól, részben azért, mert az amerikai vidéki hálózatoknak időre volt szükségük ahhoz, hogy alternatívákat⁷⁸ találjanak. E cikk írásakor a Huawei-t április 1-jéig nem tiltották be teljesen, és úgy tűnik, hogy még ez is változhat jóval az időpont⁷⁹ után.

Nemzetközi szinten az USA óriási nyomást gyakorolt mindenkire, akire csak tudott, hogy teljes mértékben betiltsa a

⁷¹ Rachel Falk, "Can the 'Core' and 'Edge' of a 5G Network Really be Separated?", Strategist Special Report, *The Strategist*, 2020. január 17., <https://www.aspistrategist.org.au/can-the-core-and-edge-of-a-5g-network-really-be-elkülönítve/>.

⁷² Gilding, Simeon. "5G választások: A világügyek sarkalatos pillanata." *The Strategist*, 2020. január 29. <https://www.aspistrategist.org.au/5g-choices-a-pivotal-moment-in-world-affairs/>.

⁷³ James Andrew Lewis, "What Did the United Kingdom Just Decide on Huawei and 5G?", Commentary, CSIS, január 28, 2020, <https://www.csis.org/analysis/what-did-united-kingdom-just-decide-huawei-and-5g>.

⁷⁴ Panettieri, "Huawei Permitted Banned", p. 1.

⁷⁵ Ibid, p. 2

⁷⁶ Jay Greene és Shara Tibken, "Lawmakers to U.S. Companies: CNET", október 8., 2012, <https://www.cnet.com/news/lawmakers-to-u-s-companies-dont-buy-huawei-zte/>.

⁷⁷ Panettieri, "Huawei Permitted Banned", 3. o.; Sean Keane, "Huawei Ban Timeline"; Donald J. Trump, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain", Executive Orders - Infrastructure and Technology, The White House, May 15, 2019, <https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/>.

⁷⁸ Corinne Reichert, "Huawei Gets Another 45-Day Reprieve from Commerce Department," *CNET*, február 14, 2020, <https://www.cnet.com/news/huawei-gets-another-45-day-reprieve-from-commerce-department/>.

⁷⁹ "Department of Commerce Renews Temporary General License for 45 Days," Press Releases - Trade Enforcement, *US Department of Commerce - Office of Public Affairs*, 2020. február 13., <https://www.commerce.gov/news/press-releases/2020/02/department-commerce-renews-temporary-general-license-45-days>; "Department of Commerce Extends Public Comment Period for Input on Huawei Temporary General License Extensions". Sajtóközlemények - Kereskedelmi végrehajtás. US Department of Commerce - Office of Public Affairs. March 25, 2020. <https://www.commerce.gov/news/press-releases/2020/03/department-commerce->

FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 15

[extends-public-comment-period-input-huawei.](#)

A Huawei, legalábbis az 5G infrastruktúrájukból, ha nem általánosabban a velük való üzletelésből⁸⁰. Amint azt rövidesen részletezni fogjuk, az Egyesült Királyságot nem hatotta meg ez a nyomás. Ennek eredményeképpen Kanada a partnerei⁸¹ között tételődik.

Annak ellenére, hogy az Európai Unió (EU) hírneve a jogok és a magánélet⁸² tiszteletben tartása mellett szól (ami a Huawei 5G-vel⁸³ szemben elnémult), az USA-val, a Huawei-jel és a KNK-val fenntartott bonyolult kapcsolatai azt eredményezték, hogy az EU lehetővé tette az államok számára, hogy saját döntéseket hozzanak a Huawei-jel⁸⁴ kapcsolatban. Az Egyesült Királyság európai stratégiai partnerei közül 2020. március 12-én csak Románia, Lengyelország és Észtország írt alá megállapodást az Egyesült Államokkal a Huawei tényleges betiltásáról. A tiltó döntéseik nyilvánvalóan annak köszönhetőek, hogy szükségük van az USA támogatására Oroszországgal szemben, nem pedig a Huawei-jel⁸⁵ kapcsolatos elsöprő aggodalmaknak.

Japán annyiban figyelemre méltó, hogy bár Öt Szem partnerévé kíván válni, csak a kormányzati infrastruktúrából és szerződésekből tiltotta ki a Huaweiit. Ennek azonban az lett az eredménye, hogy hazai vállalatai úgy döntöttek, hogy nem használják a Huaweiit az 5G-hálózatokban⁸⁶. Az Egyesült Királyság és az Egyesült Államok többi szövetségese és stratégiai partnere eddig saját megközelítéseket választott a Huawei kockázatainak mérséklésére, elsősorban arra összpontosítva, hogy a Huaweiit kitiltják a maghálózatokból, amelyeket figyelembe vesznek.

⁸⁰ Isobel Asher Hamilton, "The Trump Administration failed to Convince the UK to Ditch Huawei and Its Other Allies Aren't Listening Either," *Business Insider*, március <https://www.businessinsider.com/huawei-how-11-allies-are-reacting-to-us-calls-to-avoid-the-tech-firm-2019-2>2020,.

⁸¹ Kevin Carmichael, "Canada's Waffling on 5G is Just One of the Uncertainties Choking the Life Out of the Economy", *Business, Financial Post*, 2020. február 7., <https://business.financialpost.com/news/economy/canadas-waffling-on-5g-is-just-one-of-the-uncertainties-choking-the-life-out-of-the-economy>.

⁸² Marietje Schaake és Mathias Vermeulen, "Towards a Values-Based European Foreign Policy to Cybersecurity" (A kiberbiztonság értékalapú európai külpolitikája felé). *Journal of Cyber Policy* no1., 1 (2016): 75-84, <https://doi.org/10.1080/23738871.2016.1157617>.

⁸³ Carisa Nietzsche és Bolton Smith, "Why Europe Won't Combat Huawei's Trojan Tech," *National Security, The National Interest*, 2019. október 2., <https://nationalinterest.org/feature/why-europe-wont-combat-huaweis-trojan-tech-85041>.

⁸⁴ Erik Brattberg és Philipple Le Corre, "Huawei and Europe's 5G Conundrum," *The National Interest*, 2018. december 27., <https://nationalinterest.org/feature/huawei-and-europe%E2%80%99s-5g-conundrum-39972>; James Andrew Lewis, "5G To Ban or Not to Ban? It's Not Black or White," *Commentary, CSIS*, 2019. április 24., <https://www.csis.org/analysis/5g-ban-or-not-ban-its-not-black-or-white>; "EU Deals Another Blow to US, Allowing Members to Decide on Huawei's 5G role," *Europe News, CNBC via Reuters*, 2020. január 29., <https://www.cnbc.com/2020/01/29/eu-deals-blow-to-us-allowing-members-to-decide-on-huaweis-5g-role.html>; David E. Sanger and David McCabe, "Huawei is Winning the Argument in Europe, as the U.S. Fumbles to Develop Alternatives," *Politics, The New York Times*, február 17, 2020, <https://www.nytimes.com/2020/02/17/us/politics/us-huawei-5g.html>; Carisa Nietzsche és Martijn Rasser, "Washington's Anti-Huawei Tactics Need a Reboot in Europe," *Argument, Foreign Policy*, 2020. április 30., <https://foreignpolicy.com/2020/04/30/huawei-5g-europe-united-states-china/>.

⁸⁵ Andreea Brinza, "How Russia Helped the United States Fought Huawei in Central and Eastern Europe", *War on the Rocks*, 2020. március 12., <https://warontherocks.com/2020/03/how-russia-helped-the-united-states-fight-huawei-in-central-and-eastern-europe/>.

⁸⁶ Glosserman, "Huawei realitások".

kritikus a nemzetbiztonságuk⁸⁷ szempontjából.

Az Öt Szem Nemzet közül az Egyesült Királyság az egyetlen olyan nemzet, amely úttörő szerepet játszik a kockázatkezelési és kockázatsökkentési megközelítésben, és élen jár a Huawei-jel való partnerségben és annak felügyeletében. Az Egyesült Királyság 2003-ban kezdett el együttműködni a Huawei-jel, mint "magas kockázatú szállítóval", és kezdettől⁸⁸ fogva kockázatsökkentő megközelítést alkalmazott. 2010-ben, mivel az Egyesült Királyság kormányzati kommunikációs központja (GCHQ) szokatlan tevékenységet észlelt a Huawei hálózataiban, a Huawei és az Egyesült Királyság együttműködött a Huawei Kiberbiztonsági Értékelő Központ (HCSEC) létrehozásában⁸⁹. A HCSEC a GCHQ-val és a Nemzeti Kiberbiztonsági Központtal (NCSC) együttműködve értékeli, hogy a Huawei termékei megfelelnek-e a szabványoknak és biztonságosak-e a telepítéshez⁹⁰.

Ennek eredményeképpen a HCSEC hozzáféréssel rendelkezik a Huawei forráskódjához, termékeihez, és az átvilágítás részeként üzleti kérdésekben tanácsot adhat a Huawei-nek, hogy felmérje, hogy szándékai tisztán kereskedelmi jellegűek-e. Ez a partnerség lehetővé tette az Egyesült Királyság számára, hogy a Huawei-jel való együttműködés előnyeinek kihasználására összpontosítson, miközben proaktívan mérsékli a kockázatokat. Ez a korai partnerség tette lehetővé az 5G Innovációs Központ létrehozását a Surrey Egyetemen 2015-ben, amely hamarosan "az Egyesült Királyság legnagyobb akadémiai 5G vezeték nélküli kommunikációs infrastruktúra-kutató központjává" vált⁹¹.

Az Egyesült Királyság és a Huawei kapcsolata azonban még mindig kihívásokkal és aggodalmakkal jár. Először is, az Egyesült Királyságban a régebbi kritikus infrastruktúra már tartalmaz Huawei-alkatrészeket⁹². Aztán ott van a 2019-es HCSEC Felügyeleti Testület jelentése⁹³, amely a Huawei biztonságát érintő számos kritikája miatt került a címlapokra. A kritikák a munka rossz minősége és a korábbi HCSEC-jelentésekben azonosított problémák megfelelő orvoslásának elmulasztása körül forogtak, bár ezeket inkompetenciának és hanyagságnak tulajdonították, szemben a rosszindulatú szándékkal vagy a kínai beavatkozással. Végül pedig

⁸⁷ Hamilton, "A szövetségesek nem figyelnek"; Panettieri, "Huawei Permitted Banned".

⁸⁸ Ian Levy, "Security, Complexity and Huawei ; Protecting the UK's Telecoms Networks," People, *NCSC Blog*, 2019. február 22., <https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks>.

⁸⁹ Amit Katwala, "Here's How GCHQ Scours Huawei Hardware for Malicious Code," *WIRED UK*, február h22,2019, <https://www.wired.co.uk/article/huawei-gchq-security-evaluation-uk>.

⁹⁰ A HCSEC éves jelentései itt találhatóak: "Keresés: Huawei Cyber Security Evaluation Centre Oversight Board". Gov.uk. Hozzáférés: 2020. március 30. <https://www.gov.uk/search/all?keywords=%22Huawei+Cyber+Security+Evaluation+Centre+Oversight+Board%22&order=relevance>.

⁹¹ "5G Innovation Centre (5GIC) - University of Surrey," UK Research Partnership Initiative Fund, Hozzáférés: 2020. március 10., <https://re.ukri.org/funding/our-funds-overview/uk-research-partnership-initiative-fund/case-studies/5g-innovation-centre-5gic-university-of-surrey/>.

⁹² Juliet Samuel, "Sorry Boris, France Shows There is an Alternative to Huawei After All", News, *The Telegraph*,

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 19**

február h2020, <https://www.telegraph.co.uk/news/2020/02/01/sorry-boris-france-shows-alternative-huawei/>.

⁹³ Huawei Kiberbiztonsági Értékelő Központ (HCSEC) Felügyeleti Testület, "Éves jelentés: 2019," HCSEC, március 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

a Huawei teljes⁹⁴ betiltására irányuló, évek óta növekvő amerikai nyomás.

Amikor e cikk nagy részei először készültek 2019-ben, az Egyesült Királyságban éppen miniszterelnök-választás zajlott, és bizonytalanság volt abban, hogy betiltja-e a Huawei-t, akár ~~esetben~~ akár csak az 5G tekintetében. Még 2019 decemberéig úgy tűnt, hogy Boris Johnson miniszterelnök végigviszi a tilalmat⁹⁵. 2020. január végén Johnson és a parlament úgy döntött, hogy nem tiltja be teljesen a Huawei-t és a nagy kockázatot jelentő gyártókat, ehelyett úgy szavazott, hogy távol tartja őket a kritikus alapvető hálózatoktól, és 35%-ban korlátozza piaci részesedésüket.⁹⁶

Márciusban Johnson saját pártjának tagjai megkísérelték a teljes betiltást, de végül ez is elbukott⁹⁷. Azóta úgy tűnik, hogy az Egyesült Királyság megközelítése lehetővé tette, hogy az ország magabiztosan lépjen előre a Huawei és a nagy kockázatú szállítókkal, ami mind a gazdasága, mind a biztonsága⁹⁸ egyensúlyát és előnyeit szolgálja. A koronavírus-járvány azonban hatással lehet az Egyesült Királyság kapcsolataira mind a KNK-val, mind az USA-val, ami kihatással lehet az 5G-re és az Egyesült Királyság következő nemzeti kiberbiztonsági stratégiájára⁹⁹.

Johnson pártjának tagjai a koronavírust a Huawei betiltásának és a Five-Eyes és a Kínai¹⁰⁰ Népköztársaság szétválasztásának eszközének tekintik. A Henry Jackson Society április közepén végzett felmérése szerint a brit felnőttek 62%-a támogatja, hogy a Huawei építse ki az Egyesült Királyság 5G-jét, 12% ellenzi, 19% "Egyik sem", 6% pedig "Nem tudom"¹⁰¹. Ugyanez a felmérés szerint 63% támogatja, hogy "szigorúbb kereskedelmi, befektetési és biztonsági politikát folytassanak Kínával szemben, mint amelyet az USA az elmúlt években folytatott", míg 12% ellenzi, 19% "Egyik sem", 8% pedig "Nem tudom"¹⁰².

⁹⁴ Garrett M. Graff, "The US is Losing Its Fight Against Huawei," Business, *WIRED*, 2020. január 29., <https://www.wired.com/story/uk-huawei-5g-networks-us/>.

⁹⁵ Gordon Rayner, "Boris Johnson Gives Clearest Indication Yet He Will Ban Huawei After Election," Politics, *The Telegraph*, 2019. december 4., <https://www.telegraph.co.uk/politics/2019/12/04/boris-johnson-gives-clearest-indication-yet-will-ban-huawei/>.

⁹⁶ Paul Sandle és Jack Stubbs, "Defying Trump, UK's Johnson Refuses to Ban Huawei from 5G," Technology News, *Reuters*, 2020. január 27., <https://www.reuters.com/article/us-britain-usa-huawei/defying-trump-uks-johnson-refuses-to-ban-huawei-from-5g-idUSKBN1ZR02G>.

⁹⁷ Norman Smith, "Huawei: Government Wins Vote After Backbench Rebellion," Politics, *BBC News*, március 10., h2020, <https://www.bbc.com/news/uk-politics-51806704>.

⁹⁸ "Johnson: Huawei 5G Decision Will Balance Innovation and Security," AJ Impact/China, *Al Jazeera*, 2020. január 27., <https://www.aljazeera.com/ajimpact/johnson-huawei-5g-decision-balance-innovation-security-200127181107270.html>; Ian Levy, "The Future of Telecoms in the UK," NCSC Publications, *NCSC Blog*, 2020. január 28., <https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk>; Matthew Field, "Why Britain's Spooks 'Think They Know Better' Than the US on Huawei," Technology Intelligence, *The Telegraph*, január 29., h2020, <https://www.telegraph.co.uk/technology/2020/01/29/britains-spooks-think-know-better-us-huawei/>.

⁹⁹ "National Cyber", HM kormány; "National Progress", HM kormány.

¹⁰⁰ James Rogers, Andrew Foxall, Matthew Henderson, Sam Armstrong, Gisela Stuart, Michael Danby, Andrew Hastie, Peter Mackay, Marco Rubio és Bob Seely, "Breaking the China Supply Chain: How the 'Five Eyes' Can Decouple from Strategic Dependency," White Paper, Henry Jackson Society, 2020. május, <https://henryjacksonsociety.org/wp-content/uploads/2020/05/Breaking-the-China-Chain.pdf>.

¹⁰¹ Ibid, p. 14.

¹⁰² Ibid.

Ebben az összefüggésben most megvizsgáljuk azt az öt fő veszélyt, amelyet a Huawei állítólag az Egyesült Királyságra jelent. Ezután megvizsgálunk néhány egyedi 5G és kiberbiztonsági lehetőséget, amelyekkel az Egyesült Királyság rendelkezik, mielőtt feltárnánk az 5G biztonságáról szóló vitában figyelmen kívül hagyott kihívásokat és innovatív megoldásokat, amelyeket az Egyesült Királyságnak és más szereplőknek figyelembe kellene vennie.

Második rész - Öt fő fenyegetés

Hátsó ajtók

A hátsó ajtó távoli hozzáférést tesz lehetővé az információkhoz, és általában láthatatlan az azt telepítő személyen kívül minden fél számára. A hátsó ajtók jelen lehetnek hardverben vagy szoftverben; egy kulcsfontosságú komponens megváltoztatásával vagy egy olyan javítás telepítésével, amely távoli hozzáférést¹⁰³ tesz lehetővé. Az a kockázat, hogy a Huawei ezt megteheti az 5G készülékével, a leggyakoribb érv a Huawei iránti bizalmatlanság mellett. Ez a bizalmatlanság nem magából a Huawei-ből ered, hanem inkább a KNK és annak tekintélyelvű jellege¹⁰⁴ által jelentett potenciális fenyegetésből.

Nem csak elméleti aggályok merülnek fel azzal kapcsolatban, hogy a Kínai Népköztársaság a Huawei erőforrásként használhatja fel arra, hogy politikai programját egyénekkal vagy más államokkal szemben előmozdítsa. A *The Wall Street Journal* februári jelentése^{12,2020} amerikai kormányzati forrásokra hivatkozva azt állítja, hogy a Huawei által világszerte kiépített 4G hálózatok legalább 2009 óta hátsó ajtós képességeket biztosítanak a Huawei számára, de nem állítja, hogy a Kínai Népköztársaság kihasználta volna ezeket. A cikk szerint az Egyesült Államok 2019 végén osztotta meg ezt az információt az Egyesült Királysággal és Németországgal, mivel a végső fázisban voltak annak eldöntésében, hogy bevonják-e a Huawei az 5G¹⁰⁵ fejlesztésébe.

Ez az ütemterv azt jelzi, hogy az Egyesült Királyság úgy véli, hogy a hátsó ajtók által jelentett kockázatok enyhítési stratégiákkal¹⁰⁶ kezelhetők, amint azt a 2019-es tervezet is megállapította. A HCSEC hozzáféréssel rendelkezik a forráskódhoz, és rutinszerűen teszteli az egyenértékűséget megismételhető buildek során azzal, amit a patch-frissítéseken keresztül telepítenek. A HCSEC erőforrásait a GCHQ és az NCSC egészíti ki. Ezek együttes képessége a hátsó ajtók azonosítására csökkenti annak kockázatát, hogy azok észrevétlenül maradjanak, és biztosítja a felhasználókat arról, hogy a Huawei termékei átvilágítottak és biztonságosak.

A hardveres kockázatok kezelését korlátozza, hogy a kínai gyárak milyen mértékben függetlenek az alkatrészek gyártásától. Felmerül a kérdés, hogy vannak-e életképes alternatívák az 5G távközlési szolgáltatók számára? A kínai székhelyű vállalatok egyes alkatrészeket szállítanak a Nokia és az Ericsson számára, amelyek az Egyesült¹⁰⁷ Királyság két potenciális 5G-pótlója. Aztán ott van az a tény, hogy a Huawei jelen van a Nokia és az Ericsson egyes 4G és 5G hálózataiban¹⁰⁸. A hardveres fenyegetés azonban

¹⁰³ Aviva Zacks, "Mi az a hátsó ajtó és hogyan védekezzünk ellene", Blog, Safety Detectives, szeptember 2, 2018, <https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/>.

¹⁰⁴ "5G biztonság: Policy, US Department of State, november 2019, <https://policystatic.state.gov/uploads/2019/11/5G-What-is-Trust.pdf>.

¹⁰⁵ Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks", World, *The Wall Street Journal*, 2020. február 12., <https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256>.

¹⁰⁶ Levy, "Future Telecoms"; Lewis, "United Kingdom".

¹⁰⁷ Stu Woo és Dustin Volz. "U.S. Considers Requiring 5G Equipment for Domestic Use Be Made Outside China," Tech, *The Wall Street Journal*, 2019. június 23., <https://www.wsj.com/articles/u-s-considers-requiring-5g-equipment-for-domestic-use-be-made-outside-china-11561313072>.

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 23**

¹⁰⁸ Z. X., (szerkesztő), "A norvég Telenor azt mondja, hogy továbbra is Huawei berendezéseket használ az 5G-hez", *XinHuaNet*, december 14, 2019, http://www.xinhuanet.com/english/2019-12/14/c_138631613.htm.

talán nem is olyan vészes, és úgy tűnik, van lehetőség arra, hogy az érdekelt felekkel együttműködve csökkentjük a kockázatokat.

Francis Dinha, az OpenVP nevű biztonsági szoftvercég vezérigazgatója jelezte, hogy a vezeték nélküli szolgáltatók különböző hardvergyártókat használnak, és végső soron az ő kötelességük, hogy biztosítsák hálózataikat, mivel ostobaság lenne a gyártókra hagyatkozni a biztonságot illetően. Dinha szerint már iparági szabvány, hogy extra biztonsági rétegeket adnak hozzá. Ez nem jelenti azt, hogy a KNK és az ottani székhelyű vállalatok nem jelentenek fenyegetést. Dinha inkább úgy véli, hogy a magánszektorbeli partnerek és más szakértők képesek kezelni és csökkenteni azokat a kockázatokat, amelyeket a Huawei-hez hasonló gyártók jelentenek az 5G számára, de legalábbis az Egyesült Államokban úgy érzi, hogy még nem konzultáltak¹⁰⁹ velük megfelelően.

Ha a KNK befolyását, sőt, az ottani székhelyű vállalatok feletti ellenőrzést teljes mértékben rosszindulatúnak ismerjük el, akkor nem marad gazdaságilag életképes út az 5G megszerzéséhez és előnyeinek kiaknázásához. A fenyegetés elkerülése nem életképes biztonsági megközelítés. A KNK által jelentett fenyegetések többet igényelnek az elkerülésnél, az elrettentésnél vagy más passzív, reaktív megközelítéseknél.

A hátsó ajtók és egyéb kockázatok által jelentett veszélyek felismerése jelentősen csökkenti azokat. Azáltal, hogy továbbra is éberren figyelik a fenyegetést, az ügynökségek és az érdekelt felek elkötelezhetik magukat a kiberbiztonság mellett, hogy a Huawei jóindulatúan viselkedjen. Úgy tűnik, a HCSEC jó helyzetben van ahhoz, hogy ezt tegye, belföldön és - ahogyan azt a későbbiekben érvelni fogjuk - nemzetközi szinten is.

¹⁰⁹ Corinne Reichert és Marguerite Reardon, "Huawei Says US Ban Will 'Significantly Harm' American Jobs, Companies," *CNET*, május <https://www.cnet.com/news/huawei-says-blacklisting-will-significantly-harm-16-american-companies-jobs/2019>,.

Gyenge forráskód

A HCSEC 2019. évi jelentése szerint csak "korlátozott biztosítékot tud nyújtani arra vonatkozóan, hogy a Huawei brit *kritikus fontosságú hálózatokban* való részvételéből eredő, az Egyesült Királyság nemzetbiztonságát fenyegető valamennyi kockázatot [kiemelés hozzáadva] hosszú távon kellőképpen mérsékelni lehet"¹¹⁰. Hasonlóképpen, a Huawei termékei tekintetében a HCSEC általánosságban "*csak korlátozott biztosítékot* tud nyújtani [kiemelés eredeti] arra vonatkozóan, hogy a hosszú távú biztonsági kockázatok kezelhetők"¹¹¹. Amíg a Huawei szoftver- és kiberbiztonsági hibáit nem javítják, "*nehéz lesz a jövőbeli termékek megfelelő kockázatkezelése* [kiemelés eredeti]"¹¹².

A felvázolt kockázatok közül a gyenge forráskód a legkézzelfoghatóbb biztonsági kockázat az 5G hálózatra nézve. A HCSEC 2019-es jelentése szerint jelenleg három olyan probléma van, amely a gyenge forráskódból¹¹³ ered:

- Az ismételhető buildekben talált rossz forráskódok
- Az épített termékek és a ténylegesen telepített termékek egyenértékűségének ellentmondásossága
- Korlátozott bizonyítékok a rossz folyamatok és a kódolás kijavításáról

Az Egyesült Királyság azóta úgy döntött, hogy a Huawei 5G-partnereként lép tovább. A Huawei azonban nem nyújthat majd alkatrészeket és szolgáltatásokat az Egyesült Királyság biztonsági apparátusai számára kritikus hálózatokhoz. Ennek ellenére a rossz forráskód továbbra is általános aggodalomra ad okot.

A rossz forráskód jelentette kockázat abból ered, hogy harmadik felek, például államok, magánszemélyek vagy szervezett bűnözés behatolhatnak a hálózatba, és lopást, kémkedést, szabotázszt vagy váltságdíjat követelhetnek el. Az építmények egyenértékűségének következtelensége azt jelenti, hogy a Huawei által a HCSEC-nek átadott forráskód nem azonos azzal, amit a Huawei egyes vagy valamennyi termékében használ. Ez a következtelenség korlátozza azt a mértéket, ameddig a HCSEC azt állíthatja, hogy a Huawei termékei biztonságosak.

A jelentésben felvázolták a Huawei "átalakítási tervét" a gyártás szabványosítására és a biztonság garantálására. Konkrétan olyan eljárásokat kell követniük, amelyek biztosítják a forráskód megfelelő replikációját (vagyis azt, hogy a HCSEC-nek átadott adatok megegyeznek a telepített hardverrel és szoftverrel), valamint javítják a mérnöki munkát és a biztonságot. Bár 8 milliárd USD-t különítenek el ennek végrehajtására, a javasolt kezdeti költségvetés nem határoz meg semmilyen tevékenységet¹¹⁴.

A HCSEC szabványainak betartatása olyan szükségszerűség, amelyet az Egyesült Királyságnak követnie kell a kockázatok¹¹⁵ csökkentése érdekében. Ha ezt megteszi, akkor az Egyesült Királyság - mivel már hozzáfér a Huawei forráskódjához, és a Huawei-jel való látható partnerségének súlya miatt - egyedülálló helyzetben lesz ahhoz, hogy megszilárdítsa szerepét.

¹¹⁰ HCSEC, "2019", p. 4.

¹¹¹ Ibid.

¹¹² Ibid.

¹¹³ Ibid., 12-29. o.

¹¹⁴ Ibid, p. 17.

¹¹⁵ Ibid; Levy, "Future Telecoms"; Lewis, "United Kingdom".

a kiberbiztonság globális vezetőjévé váljon, és nagyobb kontrollt gyakoroljon fenyegetettségi előrejelzései felett. Továbbra is van okunk megkérdőjelezni a forráskód-ellenőrzés¹¹⁶ hatékonyságát. Biztonsági és gazdasági szempontból azonban eredményesebbnek tűnik a Huawei bevonása, miközben proaktívan kezeli kockázatait¹¹⁷, esetleg a jelenlegi kockázatcsökkentési erőfeszítések többoldalúvá tételével.

A biztonsági kérdések természetüknél fogva politikai jellegűvé válnak, ha olyan mértékűek, mint a Huawei gyenge forráskódja. A gyenge forráskód nem csak a kormányzati behatolás szempontjából aggályos. Sok szempontból nagyobb, kölcsönös aggodalomra ad okot a kiberbűnözés, mint transznacionális kérdés¹¹⁸. A nagyobb figyelem és finanszírozás - akár az Egyesült Királyság, akár egy többoldalú erőfeszítés révén - nagyobb technikai szakértelmet és politikai tőkét mozgósíthatna a Huawei által jelentett kockázatokkal szemben, függetlenül attól, hogy azok kormányzati vagy nem állami szereplőkből származnak.

Ennél is fontosabb, hogy az ilyen intézkedések megkönnyítsék a Huawei felelősségrevonását a biztonsági előírások betartásáért nemcsak az Egyesült Királyságban, hanem világszerte. Az Egyesült Királyság számára az elkerülés mint enyhítő stratégia nem szünteti meg a Huawei forráskódja által jelentett veszélyt. A Huaweivel való együttműködés és a Huawei megtartása az Egyesült Királyság piacán mindenki számára előnyösebb.

¹¹⁶ Gilding, "5G választások".

¹¹⁷ Levy, "Future Telecoms"; Lewis, "United Kingdom".

¹¹⁸ "Cyber Crime," United Nations - Office on Drugs and Crime, Accessed March 25, 2020, <https://www.unodc.org/unodc/en/cybercrime/index.html>.

Potenciális monopólium

Dr. Lewis szerint "a Huawei monopóliumot akar, és a kínai kormány támogatja ezt, mert ezáltal globális hírszerző hálózatot kapnak"¹¹⁹, hasonlóan az évtizedek óta tartó amerikai-német Crypto AG művelethez¹²⁰, és a Huawei¹²¹ 2007-es amerikai hackeléséhez. Bár a monopóliumok nem kívánatosak sem a biztonság, sem a gazdaság szempontjából, a Huawei növekvő monopóliumának fenyegető veszélye nem egyszerűen önmagában jelent fenyegetést. Inkább felerősíti a korábban tárgyalt kockázatokat, és súlyosbítja a KNK ragadozó gazdasági gyakorlatával¹²² kapcsolatos kérdéseket és kockázatokat.

Azzal, hogy az európai és más nemzetek részleges tilalmak révén beengedik a Huawei-t, egyensúlyt próbálnak teremteni a Huawei és a Kínai Népköztársaság költségei, előnyei és kockázatai között¹²³. A Huawei által létrehozott globális monopólium koncentrálna a hatalmat a szoftverek és hardverek forgalmazása és gyártása felett, általában és az 5G-ben is. Ez növeli a hátsó ajtó telepítésének kapacitását, miközben a rossz forráskód potenciálisan javítás nélkül folytatódnak, ami a szervezeteket és a kormányokat sebezhetőbbé teszi. Továbbá, ha a Huawei-t a Kínai Népköztársaság kötelezné arra, hogy a Kínai Népköztársaság törvényeinek részeként ne nyújtson több szolgáltatást egy ügyfélországnak, a monopólium hihetetlen befolyást biztosít a Huawei-nek és a Kínai Népköztársaságnak a függő nemzetek felett.

Feltételezve, hogy a koronavírus nem választja el a KNK-t a Nyugattól¹²⁴, ez a kockázat túlnyomórészt előre jelzett kockázatnak tűnik, mivel a globális gazdasági integráció hatékonyan akadályozza a Huawei-t abban, hogy egy tipikus monopolista¹²⁵ szabadságával cselekedjen. A Huawei például jelenleg az Android operációs rendszert (OS) használja, amely a Google¹²⁶ tulajdonában van. Miközben saját operációs rendszerüket, a Harmony-t (más néven Hongmeng) fejlesztik arra az esetre, ha egy amerikai tilalom leállítaná a Google-partnerségüket¹²⁷, a

¹¹⁹ Lewis, "5G betiltása vagy sem".

¹²⁰ Greg Miller, "'Az évszázad hírszerzési puccsa': National Security, *The Washington Post*, 2020. február 11., <https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/>.

¹²¹ Sanger és Perloth, "N.S.A. Breached".

¹²² Matthew P. Goodman, "Predatory Economics and the China Challenge", *Global Economics Monthly* 6, no. 11 (November 2017): 1-2, <https://www.csis.org/analysis/predatory-economics-and-china-challenge>.

¹²³ Brinza, "Hogyan Oroszország".

¹²⁴ Ford, "Refocusing Decoupling"; Erica Pandey, "U.S. Bans Could Make Huawei Stronger," *Technology, Axios*, 2020. március 5., <https://www.axios.com/huawei-cybersecurity-china-decoupling-5g-11034740-797b-4f00-a17e-7b3265d8bbcd.html>; Kurt M. Campbell és Rush Doshi, "The Coronavirus Could Reshape Global Order," *Foreign Affairs*, 2020. március 18., <https://www.foreignaffairs.com/articles/china/2020-03-18/coronavirus-could-reshape-global-order>.

¹²⁵ Morris, "Huawei's '18-Month'"; James Andrew Lewis, "Statement Before the Senate Committee on the Judiciary - '5G: The Impact on National Security, Intellectual Property, and Competition' - A Testimony by: James A. Lewis," Tanúvallomás, CSIS, május 14, 2019, https://csis-prod.s3.amazonaws.com/s3fs-public/congressional_testimony/Jim%20Lewis%20Written%20Statement_%203-4-20.pdf?j.NdIo307mKlOlZ7sobLj5o088GC53m.¹²⁶ Tom Bedford és Basil Kronfli, "Harmony OS: What You Need to Know About Huawei's New Operating System," *News, TechRadar*, január 17, 2020, <https://www.techradar.com/news/harmonyos>.

¹²⁷ Ibid.

Az USA továbbra is ellenőrzi a félvezetők és a kulcsfontosságú chipkomponensek¹²⁸ gyártását. Ahogy Ren Zhengfei, a Huawei vezérigazgatója elismeri, "ha ezer kulcsfontosságú alkatrész közül egy hiányzik, egy távközlési berendezés nem fog működni"¹²⁹.

Továbbá, miközben a Kínai Népköztársaság gyártási kapacitása az áruk előállításához folyamatosan növekszik¹³⁰ (2011-ben¹³¹ a világ PC-inek mintegy 90%-át és a telefonok 70%-át gyártotta), hiányoznak a szabad piaci struktúrák, amelyek lehetővé teszik az 5G jövőjébe vezető út előkészítéséhez szükséges innovációt¹³². Még ha az innovációs képességük meg is változik, a globális versenytársak minden bizonnyal méltó ellenfelek vagy akár együttműködők¹³³ maradnak. Ebben az értelemben a kisebb 5G-s vállalkozások, például az Ericsson és a Nokia számára sikeres üzleti stratégia lehet, ha olyan speciális szolgáltatásokat nyújtanak, amelyeket a Huawei nem. Akárhogy is, még ha a Huawei a piaci részesedés alapján potenciálisan monopolhelyzetet is teremthet, nem viselkedhet tipikus monopóliumként. Ennek oka, hogy a berendezések és szolgáltatások tekintetében külső beszállítóktól függ, ami viszont korlátozza a Huawei büntetlen fellépési képességét.

Most gondoljunk arra az alternatívára, hogy a Huawei-t kivonják az Egyesült Királyság piacáról. Eltekintve a KNK esetleges megtorlásától az Egyesült Királysággal szemben, ha az Ericsson és a Nokia marad az 5G versenytárs, a kiadások és az alternatív költségek megnőnek. Mindkét beszállító berendezései többre kerülnek, elsősorban a KNK-n¹³⁴ kívüli magasabb gyártási költségek miatt.

A Covid-19-járvány előtt az Ericsson és a Nokia elkezdte az 5G-gyártás egy részét a KNK-n kívülre, különösen Indiába¹³⁵ helyezni. A Covid-19 politikai és gazdasági következményei számos országot arra készítettek, hogy átgondolja a Kínával való kapcsolatait, különösen az orvosi és technológiai ellátási láncok tekintetében. Ennek egyik eredménye az Indiával folytatott kereskedelem iránti fokozott érdeklődés, különösen az Egyesült Királyságot illetően¹³⁶.

¹²⁸ Lewis, "Statement Judiciary", p. 7.

¹²⁹ James Kynge, Yuan Yang és Sue-Lin Wong, "Huawei: Still Fighting for Survival Despite Trump Truce," The Big Read - Huawei Technologies, *Financial Times*, 2019. július 3., <https://www.ft.com/content/a6db14d8-9993-11e9-9573-ee5cbb98ed36>.

¹³⁰ Gordon Orr, "What Can We Expect in China in 2020?," Featured Insights - Commentary, McKinsey and Company, 2019. december, [h2020https://www.mckinsey.com/featured-insights/china/what-can-we-expect-in-china-in-](https://www.mckinsey.com/featured-insights/china/what-can-we-expect-in-china-in-).

¹³¹ Matt Schiavenza, "China's Dominance in Manufacturing-in One Chart," China, *The Atlantic*, August 5, 2013, <https://www.theatlantic.com/china/archive/2013/08/chinas-dominance-in-manufacturing-in-one-chart/278366/>. Ben

¹³² Blanchard és Perry Michael, "Lack of Innovation is 'Achilles Heel' for China's Economy, Xi Says," World News, *Reuters*, May 15 2019, <https://www.reuters.com/article/us-china-politics-xi/lack-of-innovation-is-achilles-heel-for-chinas-economy-xi-says-idUSKCN1SM08G>.

¹³³ Scott Kennedy, "Kína egyenlőtlen csúcstechnológiai hajtása: Implications for the United States", jelentés, CSIS, február h27,2020, <https://www.csis.org/analysis/chinas-uneven-high-tech-drive-implications-united-states>.

¹³⁴ Anirban Ghoshal, "Nokia, Ericsson to Soon Export 5G Equipment Made in India," Technology, *TechCircle*, October 26, 2018, <https://www.techcircle.in/2018/10/26/nokia-ericsson-to-soon-export-5g-equipment-made-in-india>.

¹³⁵ Ibid.

¹³⁶ George Parker és Daniel Thomas, "UK Looks to Wean Itself Off Chinese Imports," UK Trade, *Financial*

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 30**

Times, 2020. június 9., <https://www.ft.com/content/dc22913c-4abd-4258-89fb-e45a4342e2a6>.

Míg a diverzifikáció számos okból okos dolog, nem olyan egyértelmű, hogy a termelés Indiába való áthelyezése javítja a biztonságot vagy megakadályozza a magasabb költségeket. Az India és a Kínai Népköztársaság között az elmúlt években egyre nagyobb feszültségek alakultak ki, és úgy tűnik, hogy az 1975 óta tartó első halálos kimenetelű összecsapásuk 2020¹³⁷. június 15-én történt. A Covid-19 és a halálos kimenetelű összecsapás előtt és különösen után India már vizsgálta a kínai székhelyű vállalatok, köztük a Huawei és a ZTE¹³⁸ korlátozását vagy betiltását.

Az eszkalálódó gazdasági és politikai harcok mindkét ország¹³⁹ számára növelték a költségeket. Továbbá India protekcionista megközelítése nem csak a Kínával való kapcsolatára van hatással. Ahelyett, hogy lehetőséget teremtett volna a Nyugat és olyan országok számára, mint Japán, Dél-Korea és Ausztrália, India protekcionista politikája olyan széleskörűen fogalmazódott meg, hogy gyakorlatilag minden partnere¹⁴⁰ számára növelte a költségeket. Tekintettel arra, hogy India és a Nyugat a KNK-tól való elszakadás irányába mutat, ezek a költségek valószínűleg csak növekedni fognak.

Ezeket a magasabb költségeket öt probléma tovább súlyosbíthatja. Először is, a Huawei vitathatóan arra ösztönzi az 5G-szolgáltatókat, hogy versenyképesek maradjanak a költségek, a minőség és az innováció¹⁴¹ tekintetében. Másodsor, 2018 végén iparági szakértők, sőt, még a vállalat bennfentesei is úgy vélték, hogy a Nokia és az Ericsson nehezen tudná "helyettesíteni a Huawei egy üzemeltetői hálózat magjában", nem is beszélve "az összes rádiós helyszínen", bár mindkét vállalat vegyes eredményekkel¹⁴² próbálta cáfolni ezeket az állításokat. A képességekkel, a költségekkel és a késedelmekkel kapcsolatos ilyen aggodalmak februárban 2020¹⁴³ is fennállnak.

Harmadszor, a Nokia és az Ericsson közelmúltbeli, az USA¹⁴⁴ és Franciaország¹⁴⁵ által a Huawei alternatívájaként kínált ajánlatai, amelyeket az USA és Kína közötti kereskedelmi háború súlyosbított, arra készítette őket, hogy még inkább áthelyezzék a

¹³⁷ Helen Davidson és Ben Doherty, "Explainer: World-India, *The Guardian*, 2020. június 16., <https://www.theguardian.com/world/2020/jun/17/explainer-what-is-the-deadly-india-china-border-dispute-about>.

¹³⁸ Akhil Bery és Clarise Brown, "India és Kína digitális válása", Eurasia Live, Eurasia Group, júliusi videó 1, 2020., 11m:35s, <https://www.eurasiagroup.net/live-post/india-china-digital-divorce>.

¹³⁹ Ibid.

¹⁴⁰ Ibid.

¹⁴¹ Iain Morris, "Where Huawei Fears to Tread," *5G, Light Reading*, 2018. december 13., <https://www.lightreading.com/mobile/5g/where-huawei-fears-to-tread/d/d-id/748266>; Gordan Corera, "Eric Schmidt: Huawei has Engaged in Unacceptable Practices," *Technology, BBC News*, 2020. június 18., <https://www.bbc.com/news/technology-53080113>.

¹⁴² Iain Morris, "Huawei Muscle Puts Ericsson, Nokia on 5G Back Foot in Europe - Sources," *5G, Light Reading*, 2019. február 14., <https://www.lightreading.com/mobile/5g/huawei-muscle-puts-ericsson-nokia-on-5g-back-foot-in-europe---sources/d/d-id/749474>.

¹⁴³ Johannes Ledel és Sam Kingsley, "Can Nokia, Ericsson Compete With Huawei?", Kína. *Asia Times*, február 3, 2020, <https://asiatimes.com/2020/02/can-nokia-ericsson-compete-with-huawei/>.

¹⁴⁴ Marguerite Reardon, "Nokia and Ericsson Pitch Themselves as Huawei 5G Alternative," *CNET*, 2020. március 4., <https://www.cnet.com/news/nokia-and-ericsson-pitch-themselves-as-huawei-5g-alternative/>.

¹⁴⁵ Zak Doffman, "China Just Issued Stark New Threats Over Huawei: This Time Nokia and Ericsson are in Its Sights," *Innovation, Forbes*, 2020. február 9., <https://www.forbes.com/sites/zakdoffman/2020/02/09/china-just-issued-stark-new-threats-over-huawei-this-time-nokia-and-ericsson-are-in-its-sights/#57f21d2119d7>.

a gyártást a KNK-ból, ami valószínűleg tovább növeli a költségeket¹⁴⁶. Negyedszer, versenyben vannak a szerződésekért a KNK-ban, amely a "globális 4G infrastruktúra piac 60%-át"¹⁴⁷ teszi ki, ami a Nokia és az Ericsson ellen hathat, ami potenciálisan növelheti a költségeket. Ötödször, ha az Egyesült Királyság, az USA, Európa és mások kiszorítják a Huawei-t az Ericsson és a Nokia javára, az a verseny¹⁴⁸ mintegy 40 százalékát szüntetné meg. Mivel az Apple, a Samsung, a Dell vagy a Microsoft amerikai reményei valószínűtlenek¹⁴⁹ tűnnek, egy ilyen helyzet kényelmes duopóliumot hoz létre.

A hatalom koncentrációja önmagában is biztonsági fenyegetést jelent, és a modern technológia példátlan¹⁵⁰ teszi az ilyen koncentrációt. Kiberbiztonsági szempontból maga a piaci koncentráció növeli, "a rendszerszintű kiberkockázat volumenét"¹⁵¹. Emellett korlátozza a fenyegetések¹⁵² reaktív, nem is beszélve a proaktív kezelésének képességét. Ebben az összefüggésben a kockázatsökkentés "jobb mérést, a rendszerek sokféleségét ... a piaci koncentrációra való odafigyelést igényel a kiberbiztosítások árazásában, valamint a kritikus rendszerek mindenütt jelenlévő összekapcsolásának tudatos elkerülését"¹⁵³.

Ezek a kockázatok súlyosbodnak Európa és az Egyesült Királyság esetében. Európában mindössze négy rádió-hozzáférési hálózat (RAN) hardverszállítója van: a ZTE, a Huawei, a Nokia és az Ericsson. Az Egyesült Királyságban csak három RAN-beszállító van: a Huawei, a Nokia és az Ericsson¹⁵⁴.

Gazdasági szempontból a duopóliumok nem jelentenek¹⁵⁵ ugyanolyan mértékű veszélyt, mint a duopóliumok.

¹⁴⁶ Iain Morris, "Ericsson, Nokia Prepared for Any US Ban on China-Made Gear," 5G, *Light Reading*, június 24., <https://www.lightreading.com/mobile/5g/ericsson-nokia-prepared-for-any-us-ban-on-china-made-gear/d/d-2019,id/752342>.

¹⁴⁷ Iain Morris, "Nokia in Line for 5G Contracts Worth Up to \$2.2B With Chinese Telcos," Asia, *Light Reading*, November 11, 2019, [https://www.lightreading.com/asia-pacific/nokia-in-line-for-5g-contracts-worth-up-to-\\$22b-with-chinese-telcos/d/d-id/755523](https://www.lightreading.com/asia-pacific/nokia-in-line-for-5g-contracts-worth-up-to-$22b-with-chinese-telcos/d/d-id/755523).

¹⁴⁸ Valentin Weber, "Making Sense of Technological Spheres of Influence", Strategic Updates, LSE IDEAS, március 31, 2020, <http://www.lse.ac.uk/ideas/publications/updates/technological-spheres-of-influence>.

¹⁴⁹ Jeremy Horwitz, "U.S. 5G Security is Imperiled by Trump Administration Infighting and Fantasies," Security - Opinion, *Venture Beat*, 2020. február 6., <https://venturebeat.com/2020/02/06/u-s-5g-security-is-imperiled-by-trump-administration-infighting-and-fantasies/>.

¹⁵⁰ Adam Garfinkle, "Hatalomkoncentrációk: The Net Effect," *The American Interest*, 2020. április 7., <https://www.the-american-interest.com/2020/04/07/the-net-effect/>.

¹⁵¹ Dan Geer, Eric Jardine és Eireann Leverett, "On Market Concentration and Cybersecurity Risk", *Journal of Cyber Policy* (online megjelent 2020. február), <https://doi.org/10.1080/23738871.2020.1728355>.

¹⁵² Tom Wheeler és David Simpson, "Why 5G Requires New Approaches to Cybersecurity: Jelentés, The Brookings Institution, 2019. szeptember 3., <https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/>.st

¹⁵³ Ibid.

¹⁵⁴ James Sullivan és Rebecca Lucas, "5G kiberbiztonság: The Globalisation of Technology Occasional Paper, RUSI, 2020. február 14., 16-17. o., <https://rusi.org/publication/occasional-papers/5g-cyber-security-risk-management-approach>.

¹⁵⁵ Erwin A. Blackstone, Larry F. Darby és Joseph P. Fuhr Jr., "The Case of Duopoly: Industry Structure is not a Sufficient Basis for Imposing Regulation," *Regulation* (Winter 2011-2012): 12-17, <https://www.cato.org/sites/cato.org/files/serials/files/regulation/2012/6/v34n4-3.pdf>.

az ármeghatározási, versenyellenes és egyéb problémák, amelyeket a monopóliumok általában garantálnak¹⁵⁶, a két vállalat közötti összejátszás révén lehetőséget nyújtanak az ilyen gyakorlatokra. Az összejátszás illegális az Egyesült Államokban és máshol is. Úgy tűnik azonban, hogy ez nem tartja vissza az iparágakat és a vállalatokat az összejátszástól¹⁵⁷. Ez különösen akkor igaz, ha elég nagyok vagy fontosak ahhoz, hogy lobbizzanak a figyelem ellen, lobbizzanak a törvények megváltoztatásáért, vagy egyszerűen csak bírságot fizessenek és továbblépjenek.

A távközlési és az informatikai iparágak már most is kiváló példái az ilyen tendenciáknak, amelyek megbénítják az innovációt és növelik a költségeket¹⁵⁸.

Továbbá a duopóliumok, valamint azok rokonai, a kartellek és az oligopóliumok "hallgatólagos összejátszást"¹⁵⁹ hozhatnak létre. A hallgatólagos összejátszás azt jelenti, hogy a vállalatok és a piacok passzívan (vagy éppen nem teljesen aktívan) összejátszóként és monopóliumként viselkedhetnek, ami árt az innovációnak és a fogyasztóknak. Bizonyos körülmények ösztönzik vagy elriasztják a hallgatólagos összejátszást. Bár további elemzésekre lenne szükség, úgy tűnik, hogy a Nokia és az Ericsson duopóliumának nem szándékolt negatív következményei - beleértve a hallgatólagos összejátszást és ezáltal a magasabb árakat - mindenképpen megalapozottan aggályosak.

Ezek a tényezők külön-külön vagy összességében korlátoznák az 5G-hálózatok bevezetésének sebességét, általános minőségét és lefedettségét, valamint a későbbi innovációt. Az ilyen piaci dinamikára való támaszkodás jelentős költségvetési és alternatív költségekkel járna azok számára, akik megpróbálnának felzárkózni azokhoz az országokhoz, amelyek már beléptek a Huawei által megfizethetővé tett, teljesen kereskedelmi forgalomba hozott 5G korszakába. Akárhogy is, az Egyesült Királyság és a Nyugat válasza a Kínai Népköztársaság protekcionizmusára, a Huawei monopóliumára és a hozzájuk kapcsolódó ragadozó gazdasági gyakorlatokra nem lehet az, hogy saját protekcionista monopóliumot, duopóliumot vagy oligopóliumot hozzanak létre.

A szabad piacok és a gazdasági integráció ösztönzése történelmileg megakadályozta a negatív versenyt és a konfliktusokat¹⁶⁰. Az Egyesült Királyság és az Egyesült Államok szabadságra, biztonságra és jólétre vonatkozó értékei és stratégiái mintegy egy évszázada a piaci verseny ösztönzését és az érdekelt felek részvételén¹⁶¹ keresztül történő integrációjának fokozását célozzák. A KNK elzárkózása ettől a

¹⁵⁶ James A. Schmitz Jr., "The Cost of Monopoly: A New View", cikk, Federal Reserve Bank of Minneapolis, július 12, 2016, <https://www.minneapolisfed.org/article/2016/the-costs-of-monopoly-a-new-view>.

¹⁵⁷ Joseph E. Harrington Jr., *The Theory of Collusion and Competition Policy*, Cambridge, Massachusetts: Massachusetts Institute of Technology, 2017.

¹⁵⁸ Susan P. Crawford, *Foglyul ejtett közönség: The Telecom Industry and Monopoly Power in the New Gilded Age*, New Haven, Connecticut, US: Yale University Press, 2013; Tim Wu, "The Oligopoly Problem", *Annals of Technology*, *The New Yorker*, április 15, 2013, <https://www.newyorker.com/tech/annals-of-technology/the-oligopoly-problem>.

¹⁵⁹ Marc Ivaldi, Bruno Jullien, Patrick Rey, Paul Seabright és Jean Tirole, "The Economics of Tacit Collusion", zárójelentés a Versenypolitikai Főigazgatóság számára, Európai Bizottság, 2013. március, https://ec.europa.eu/competition/mergers/studies_reports/the_economics_of_tacit_collusion_en.pdf.

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 34**

¹⁶⁰ Wu Xinbo, "Az Egyesült Államok biztonságpolitikája Ázsiában: Implications for China-U.S. Relations," Report, The Brookings Institution, September 1, 2000, <https://www.brookings.edu/research/u-s-security-policy-in-asia-implications-for-china-u-s-relations/>; Jong-Wha Lee és Ju Hyun Pyun. "Does Trade Integration Contribute to Peace?", *Review of Development Economics* no20,. 1 (2016. február): 327-344, <https://doi.org/10.1111/rode.12222>.

¹⁶¹ Dani Rodrik, "Globalization's Wrong Turn and How it Hurt America", *Foreign Affairs* no98,. 4 (2019. július/augusztus): 26-33, https://drodrik.scholar.harvard.edu/files/dani-rodrik/files/globalizations_wrong_turn.pdf.

piaci és egyéb területeken ellentétes ezekkel az elvekkel, és kockázatokat¹⁶² rejt magában. Továbbá, ahogy Dr. Lewis rámutat, a KNK elleni vádak ellenére a közelmúlt történelmében az USA az egyetlen ország, amely következetesen gazdasági háborút folytat, és egy globalizált világban az ilyen akciók visszaütnek¹⁶³.

A Huawei jogfosztása ezáltal arra ösztönzi mind a Huawei-t, mind a P.R.C.-t, hogy még önállóbban, sőt rosszindulatúan lépjen fel azokkal szemben, akik megakadályozták őket az új piacokra való belépésben¹⁶⁴. Továbbá gyengítheti az Egyesült Királyság és az USA gazdasági, biztonsági és ideológiai érdekeit.¹⁶⁵ Ez azonban **nem** a hidegháború, és az ilyen ideológiai vagy egyéb összehasonlításokat kritikusan kell értékelni¹⁶⁶. Mindkét esetben jobb, ha az Egyesült Királyság és az USA ösztönzi a nagyobb és egészségesebb részvételt az általuk létrehozott globális rendszerben, segítve értékeik eladását a KNK és a világ népeinek és hivatalnokainak, mintha mindent elveszítenének.

A Huawei egyesült királyságbeli engedélyezése növelné a regionális és globális versenyt és az innovációt az 5G és minden ezzel járó tényező terén. A Huawei betiltása negatív versenyre ösztönöz, mivel azt jelzi a politikai döntéshozók és a magánvállalkozások számára, hogy az Egyesült Királyság és a Kínai Népköztársaság kapcsolata ellenséges jellegű. A verseny és a kereskedelem előnyei viszont elvesznek, nemcsak az 5G, hanem más iparágakban is.

Az 5G-vel összefüggésben az Egyesült Királyság mint piac elvesztése nem lesz jelentős hatással a KNK-ra. Míg az Egyesült Királyság elveszíti a Huawei által nyújtott, versenyképes árú 5G távközlési szolgáltatásokhoz való hozzáférést, valamint a már meglévő és a jövőbeni egyéb informatikai előnyöket. Aztán ott vannak a Kínai Népköztársaságnak az Egyesült Királyság hálózataiba¹⁶⁷ való meglévő, meglehetősen átható behatolásából adódó esetleges következmények, amelyeket jobb lenne enyhíteni, mint súlyosbítani.

¹⁶² Kolton, "China's Cyber Sovereignty"; Michael D. Swaine, "A Relationship Under Extreme Duress: USA-Kína kapcsolatok válaszüton", The Carter Center, január16,2019, <https://www.cartercenter.org/resources/pdfs/peace> <https://www.cartercenter.org/resources/pdfs/peace/china/china-program-2019/swaine.pdf>; Robert B. Zoellick, "Can American and China be Stakeholders?", Transcript - U.S.-China Business Council, The Carnegie Endowment for International Peace, december h4,2019, <https://carnegieendowment.org/2019/12/04/can-america-and-china-be-stakeholders-pub-80510>.

¹⁶³ James Andrew Lewis, "ZTE, the Telecom Wars, and Cyber Spies," Report - CSIS Briefs, CSIS, 2018. június 25., <https://www.csis.org/analysis/zte-telecom-wars-and-cyber-spies>.

¹⁶⁴ Zak Doffman, "China Just Crossed a Dangerous New Line for Huawei: 'There Will be Consequences'," Innovation, *Forbes*, 2019. december 16., <https://www.forbes.com/sites/zakdoffman/2019/12/16/china-just-crossed-a-dangerous-new-line-for-huawei-there-will-be-consequences/#1d3effb575a3>.

¹⁶⁵ Kolton, "China's Cyber Sovereignty"; Zhang Lin, "US-China Trade War is Really a Clash of Civilizations and Ideologies", Economy-Opinion, *South China Morning Post*, 201815., október, <https://www.scmp.com/economy/china-economy/article/2168492/us-china-trade-war-really-clash-civilisations-and-ideologies>; Osnos, "America's Contest China"; Pandey, "Bans Huawei Stronger".

¹⁶⁶ Tarun Chhabra, Rush Doshi, Ryan Hass és Mira Rapp-Hooper, "Rethinking US-China Competition: Next Generation Perspectives - A Brookings Interview," By Bruce Jones, Edited by Bruce Jones and Will Moreland, Foreign Policy at Brookings, The Brookings Institution, June 2019, https://www.brookings.edu/wp-content/uploads/2019/06/FP_20190625_global_china.pdf; Melvyn P. Leffler, "China isn't the Society Union. Confusing the Two is

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 36**

Dangerous," Ideas, *The Atlantic*, 2019. december 2., <https://www.theatlantic.com/ideas/archive/2019/12/cold-war-china-purely-optional/601969/>.

¹⁶⁷ Lewis, "Egyesült Királyság".

Mindkét esetben a Huawei és a KNK elutasítása esetén a relatív kockázatok és az előnyök megvonása sokkal nagyobb az Egyesült Királyság számára, mint a KNK számára. Tekintettel a KNK és a Huawei szerepére a jelenlegi gazdasági rendben, előnyösnek tűnik, hogy kihasználják gyártási kapacitásukat és viszonylagos műszaki szakértelmüket a jövő néhány legnagyobb iparágában (azaz az 5G és a 6G területén). Ez különösen igaz akkor, ha a Huawei csak egy a sok elfogadott versenytárs közül az IoT-aránban.

A szabad piacok mellett szóló érvek nem nélkülözhetik a jól átgondolt, a versenyt és az innovációt¹⁶⁸ elősegítő köz- és magánszféra közötti szabályozás, valamint a kormány által irányított kutatás-fejlesztési finanszírozás¹⁶⁹ fontosságának elismerését. Bár az Egyesült Királyság és a nyugati világ nagy része általában a piaci erőkre támaszkodott a kiberbiztonság terén, a piaci *kudarok*, köztük az imént említettek, jelentős problémákat¹⁷⁰ okoztak. Az Egyesült Királyság esetében a piaci kudarok, köztük "a folyamatos adatszegések, a nem megfelelő magánkiberbiztonsági beruházások és a folyamatos digitális készséghiány", "inkább államilag irányított köz- és magánszféra közötti partnerséget" eredményeztek¹⁷¹. Az, hogy ez hogyan történik, különösen az 5G¹⁷² esetében számít.

A szabad piacok és a kormányzati beavatkozás egyensúlyának megteremtése azon múlik, hogy ne játsszuk ki a kedvenceket, és ne engedjük meg jelentős piaci torzulásokat és koncentrációkat¹⁷³. Az 5G és a kiberbiztonság esetében ez az egyensúly még inkább kulcsfontosságú¹⁷⁴. A trösztellenes törvények érvényesítése a Huawei ellen nehéz, ha nem lehetetlen, és a jelenlegi amerikai megközelítés "az általunk ismert trösztellenes jogérvényesítés végét jelentheti" ¹⁷⁵világszerte. Továbbá az amerikai megközelítést akár ki is lehet használni a

¹⁶⁸ Crawford, "Captive Audience"; Ivaldi et al., "Tacit Collusion"; Harrington Jr., "Collusion Competition"; Mihail Danov, "Global Competition Law Framework: A Private International Law Solution Needed," *Journal of Private International Law* no12., 1 (2016): 77-105, <https://doi.org/10.1080/17441048.2016.1150103>; Wolfgang Kerber és Heike Schweitzer, "Interoperabilitás a digitális gazdaságban", *Journal of Intellectual Property, Information Technology and E-Commerce Law* no8., 1 (2017): 39-58, <https://nbn-resolving.org/urn:nbn:de:0009-29-45317>.

¹⁶⁹ Sheila Campbell és Chad Shirley, "Estimating the Long-Term Effects of Federal R&D Spending: CBO's Current Approach and Research Needs," Blog, Congressional Budget Office, 2018. június 21., <https://www.cbo.gov/publication/54089>.

¹⁷⁰ "Különszám: Különszám: Összehasonlító iparpolitika és kiberbiztonság." *Journal of Cyber Policy* no3., 3 (2018): 287-

469. <https://www.tandfonline.com/toc/rcyb20/3/3>; Wheeler és Simpson, "5G igényli".

¹⁷¹ Madeline Carr és Leonie Maria Tanczer, "UK Cybersecurity Industrial Policy: *Journal of Cyber Policy* 3, no. 3 (2018): 430. o., <https://doi.org/10.1080/23738871.2018.1550523>.

¹⁷² Wheeler és Simpson, "5G igényli".

¹⁷³ Ivaldi et al., "Tacit Collusion"; Kerber és Schweitzer, "Interoperability Economy"; Carr és Tanczer, "UK Cybersecurity"; Geer, Jardine és Leverett, "Market Cybersecurity"; "Why Competition and Consumer Protection Matter", Department of International Trade and Commodities-Competition Law, United Nations Conference on Trade and Development, Accessed April 17, 2020, <https://unctad.org/en/Pages/DITC/CompetitionLaw/why-competition-matters.aspx>.

¹⁷⁴ "Special Issue", *Journal of Cyber Policy*; Wheeler és Simpson, "5G Requires".

¹⁷⁵ Christian Peeters, "Huawei Ban Creates Challenge for Int'l Antitrust Enforcement," Expert Analysis-Opinion, *Law360*, May 30, 2019, <https://www.law360.com/articles/1164251/huawei-ban-creates-challenge-for-int-l-antitrust-enforcement>.

Huawei javára, ami az amerikai nemzetbiztonságra nézve¹⁷⁶ következményekkel jár.

Más botalapú megközelítések is nehéznek tűnnek. A Huawei elleni számos gazdasági panasz és tiltás ellenére az Egyesült Államok általában úgy döntött, hogy kereskedelmi háborújában nem lép fel ellene, valószínűleg a politikai vagy gazdasági¹⁷⁷ kockázatok miatt. Ez nem jelenti azt, hogy a globális trösztellenes jogérvényesítés¹⁷⁸ megszüntetését javasolnánk. Ahelyett azonban, hogy a Huawei és ezáltal saját¹⁷⁹ maguk megbüntetésére összpontosítanak, az Egyesült Királyságnak és másoknak többet kellene tenniük az állami és magánszektorbeli 5G és IoT innováció ösztönzése érdekében a sokszínű verseny¹⁸⁰ finanszírozásával.

Összehasonlítva a Kína által a Huawei-nek 20 év¹⁸¹ alatt nyújtott 75 milliárd dolláros támogatással és a Huawei 17 milliárd dolláros K+F költségvetésével, az 2018Egyesült Királyságban alig több mint 6,41 milliárd dollárt tartottak fenn...

¹⁷⁶ Loren Thompson, "Qualcomm Antitrust Case Raises Far-Reaching National Security Concerns", Business, *Forbes*, 2020. január 28., <https://www.forbes.com/sites/lorenthompson/2020/01/28/qualcomm-antitrust-case-raises-far-reaching-national-security-concerns/#1d9399f669ea>.

¹⁷⁷ Robert Clark, "No One Wants to Talk About Huawei's State Subsidies", News Analysis, *Light Reading*, 2020. január 9., <https://www.lightreading.com/asia-pacific/no-one-wants-to-talk-about-huaweis-state-subsidies/d/d-id/756697>.

¹⁷⁸ Danov, "Globális verseny".

¹⁷⁹ Will Knight, "The Newest US Sanctions on China's Huawei Could Backfire", Business, *WIRED*, 2020. március 31., <https://www.wired.com/story/newest-us-sanctions-chinas-huawei-backfire/>; Elsa B. Kania és Lindsay Gorman, "The United States Can't Afford to Turn Away Chinese Talent", Argument, *Foreign Policy*, május 13., 2020, <https://foreignpolicy.com/2020/05/13/united-states-cant-afford-turn-away-chinese-talent/>; Lairson, Skidmore és Xinbo, "US Backfired".

¹⁸⁰ Carr és Tanczer, "UK Cybersecurity"; Milo Medin, Gilman Louie, Kurt DelBene, Michael McQuade, Richard Murray és Mark Sirangelo, "The 5G Ecosystem: Risks & Opportunities for DoD," Report, Defense Innovation Board, 2019. április 3., https://media.defense.gov/2019/Apr/04/2002109654/-1/-1/0/DIB_5G_STUDY_04.04.19.PDF; Phil Budden és Fiona Murray, "Defense Innovation Report: Applying MIT's Innovation Ecosystem & Stakeholder Approach to Innovation in Defense on a Country-by-Country Basis," Working Paper, MIT LAB for Innovation Science and Policy, 2019. május, <https://innovation.mit.edu/assets/Defense-Innovation-Report.pdf>; Wheeler, "5G Five"; James Andrew Lewis, Clete Johnson és Denise E. Zheng. "5G innováció és biztonság: Perspectives from Industry and Government Leadership (Az iparági és kormányzati vezetés perspektívái)". Christopher Krebs, Kim Hart, Jason Boswell, John Godfrey, Susie Armstrong, Peter Lord, Robert Strayer, Eric Wagner, Kevin Linehan, Chris Boyer, Valerie J. Parker, Geoffrey Starks és Jennifer Lane. Rendezvény. CSIS. 2019. július 31. Audio, 2h:57m:40s. <https://www.csis.org/events/5g-innovation-and-security>; Elsa B. Kania, "Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy," Reports, Center for a New American Security, november 07, 2019, <https://www.cnas.org/publications/reports/securing-our-5g-future>; Kathleen H. Hicks, Joseph Federici, Seamus P. Daniels, Rhys McCormick, and Lindsey R. Sheppard. "Getting to Less? Az innovációs fölény stratégiája." Jelentés. CSIS. 2020. január 23. <https://www.csis.org/analysis/getting-less-innovation-superiority-strategy>; Elsa B. Kania, "Why Doesn't the U.S. Haven't the U.S. Have Its Own Huawei?", The 5G Future-Opinion. *Politico*, 2020. február 25., <https://www.politico.com/news/agenda/2020/02/25/five-g-failures-future-american-innovation-strategy-106378>; Daniel Kliman, Ben FitzGerald, Kristine Lee és Joshua Fitt, "Forging an Alliance Innovation Base," Report-America Competes 2020, CNAS, 2020. március 29., <https://www.cnas.org/publications/reports/forging-an-alliance-innovation-base>.

¹⁸¹ Chuin-Wei Yap, "State Support Helped Fueled Huawei's Global Rise," Tech, *The Wall Street Journal*, december

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 39**

h25,2019,ttps://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

USD-t az 5G beruházásokra a közel 743 milliárd dolláros infrastrukturális költségvetéséből¹⁸². Ehhez képest a Cisco (6,37 milliárd USD), a Qualcomm (5,48 milliárd USD), a Nokia (5,46 milliárd USD) és az Ericsson (4,4,8 milliárd USD) 2018-as kutatás-fejlesztési adatai, valamint az USA által 2020-ban¹⁸³ az 5G kutatás-fejlesztésre elkülöníthető 1 milliárd USD potenciális összege. Ami azt illeti, 2019 októberében az amerikai kormányzat K+F-kiadásai a GDP arányában a legalacsonyabb szinten vannak, mióta 1955¹⁸⁴.

Függetlenül a befektetések nagyságától, legalábbis az Egyesült Királyság és az Egyesült Államok befektetési jogosan összpontosítanak az 5G-vel kapcsolatos tudományos és üzleti vállalkozások támogatására. Továbbra is fennáll azonban annak a veszélye, hogy az összes hálózati beruházást csak néhány cégbe fektetik. Ideális esetben példát mutatnának, növelve a sokszínű verseny és az innováció támogatását, ahelyett, hogy saját, államilag támogatott óriásvállalatukat (óriásvállalataikat) támogatnák.

Ha a Nyugat saját "nemzeti bajnok(oka)t" hoz létre, akkor nemcsak hogy kapitulálna a KNK megközelítése előtt, hanem a nemzetközi versenyjog alapján a KNK jogi lépéseknek is kitenné magát. Az ilyen piaci koncentrációk azonban az eddig említettekénél nagyobb és költségesebb kockázatot jelentenek: az innovatívabb, versenyképesebb és biztonságosabb jövő készletetését vagy akár elmaradását¹⁸⁵. A nyílt hálózati architektúra szinte biztosan ezt a jövőt jelenti.

A nyílt hálózati architektúra lényegében a jelenlegi hardveralapú hálózati megközelítés szoftveres felváltása. Tom Wheeler, az amerikai FCC korábbi elnöke és a hírszerzési tanácsadó testület tagja szerint, míg "maga az 5G szabvány nyitott és interoperábilis"¹⁸⁶, az infrastruktúratársaságok a saját hardverüket használják a fogyasztók bezárására. Ez megakadályozza, hogy az 5G elérje valódi és tervezett potenciálját¹⁸⁷.

A nyílt hálózati architektúra célja, hogy "a hagyományos hálózati szállítók saját technológiáját olyan szoftvervezérelt technológiával váltsa fel, amely bármilyen, a polcra beszerezhető hardveren futtatható"¹⁸⁸. Ez nagyobb innovációt, versenyt és biztonságot tesz lehetővé a hardver, a szoftver és a tárgyak internetének területén. A nyílt hálózatok előnyeitől a Huawei nagyon tart¹⁸⁹, és a megközelítés vitathatatlanul

¹⁸² Jamie Davies, "UK Gov Reserves £ 6,8bn to Realise 5G dream by 2027," News. *Telecoms*, 2018. november 27., <https://telecoms.com/493818/uk-gov-reserves-6-8bn-to-realise-5g-dream-by-2027/>.

¹⁸³ Klint Finley, "A szenátorok 1 milliárd dollárt javasolnak a Huawei megelőzésére az 5G-ben. That's Small Change," Business, *WIRED*, január 14, 2020, <https://www.wired.com/story/billion-outpace-huawei-5g-small-change/>.

¹⁸⁴ Michael T. Nietzel, "The U.S. Loses Ground to the Rest of the World in R and D Funding", Leadership, *Forbes*, 2019. október 22., <https://www.forbes.com/sites/michaelt Nietzel/2019/10/22/the-us-loses-ground-to-the-rest-of-the-world-in-r-and-d-funding/#637c3864202d>.

¹⁸⁵ Kerber és Schweitzer, "Interoperabilitási gazdaság".

¹⁸⁶ Tom Wheeler, "Moving from 'Secret Sauce' to Open Standards for 5G", TechTank, The Brookings Institution, 2020. február 18., <https://www.brookings.edu/blog/techtank/2020/02/18/moving-from-secret-sauce-to-open-standards-for-5g/>.

¹⁸⁷ Ibid.

¹⁸⁸ Ibid.

¹⁸⁹ Ibid.

sokkal hatékonyabb, mint a szankciók.¹⁹⁰

Elemzők elismerik, hogy az Egyesült Államoknak az európai Huawei-kapcsolatokkal kapcsolatos egyméretű megközelítése kudarcot vallott. Ezért arra bátorítják, hogy árnyaltabb megközelítést alkalmazzon, miközben a Nokia és az Ericsson technológiáival¹⁹¹ elősegíti mind a nyílt hálózatok fejlesztését, mind az 5G-s sikereiket. Furcsa módon annak ellenére, hogy az Ericsson és a Nokia már csatlakozott¹⁹² a nyílt hálózati jövőt célzó O-RAN Alliance-hoz¹⁹³, és annak ellenére, hogy a nyílt hálózatok kétpárti támogatása ellenére a Trump-kormányzat lenézi a nyílt hálózatokat¹⁹⁴.

Úgy tűnik, hogy a kormányzat nem fog árnyaltan közelíteni, vagy nyílt hálózatokra törekedni. Ehelyett a kormányzat megpróbál bizonyos rádiófrekvenciákat az 5G számára megnyitni, szemben az amerikai védelmi miniszter, a légierő, a képviselőház és a szenátus fegyveres szolgálatokkal foglalkozó bizottságainak kétpárti tagjai, a magánipar és sokan mások biztonsági aggályaival. Szakértők rámutattak, hogy a vitatott frekvenciasáv nem is hatékony közeg az 5G számára, a kormányzat mégis tovább erőlteti. Mindkét esetben a megoldás ismét a nyílt hálózati technológia, de van okunk feltételezni, hogy ezt figyelmen kívül¹⁹⁵ hagyják.

Az O-RAN szövetség 2020. április közepén levelet küldött az Egyesült Királyságnak, amelyben arra ösztönözte, hogy ne csak biztonsági okokból, hanem a karbantartási és a lehetőségekkel kapcsolatos költségek miatt is kerülje a Huawei-t a nyílt hálózatok javára. A nyílt hálózatok azonban még nem valósultak meg, és időbe telik, amíg kialakulnak, ezért az Egyesült Királyságnak mérlegelnie kell, hogyan tudja a legjobban egyensúlyba hozni rövid és hosszú távú érdekeit. Ez az egyensúly egyedülálló gazdasági, biztonsági és politikai lehetőségeket biztosíthat az Egyesült Királyság számára.

Azzal, hogy a Huawei és a Kínai Népköztársaság részesedést kap a globális gazdasági rendben, tovább ösztönzi a HCSEC-vel és más, a biztonsággal foglalkozó partnerekkel való együttműködést, és visszatartja a hátsó ajtók telepítését. Az alternatíva, a Huawei kizárása az Egyesült Királyság piacáról, nem ösztönzi az Egyesült Királyság hazai piacának fejlődését, és nem kínál olyan lehetőségeket, amelyeket a biztonságérzetten túlmenően ki lehetne használni. A Huawei által az Egyesült Királyságba hozott partnerségek és verseny ösztönözheti egy nagyobb kiberbiztonsági iparág azonnali fejlődését és a jövőbeli IoT-hez kapcsolódó vállalkozások - mindkettő nagy potenciállal rendelkező növekedési piac.

Így a Huawei-jel és a KNK-val folytatott verseny és együttműködés ösztönzése, miközben a

¹⁹⁰ "Open standards, not sanctions, are America's Best Weapon Against Huawei," Leaders-5Geopolitics, *The Economist*, 2020. április 8., <https://www.economist.com/leaders/2020/04/08/open-standards-not-sanctions-are-americas-best-weapon-against-huawei>.

¹⁹¹ Nietzsche és Rasser, "Washington újraindítása".

¹⁹² "Amerika nem akarja, hogy Kína uralja az 5G mobilhálózatokat.: It is Going About it the Wrong Way," Business-5Geopolitics, *The Economist*, 2020. április 8., <https://www.economist.com/business/2020/04/08/america-does-not-want-china-to-dominate-5g-mobile-networks>.

¹⁹³ "Az O-RAN szövetség áttekintése." O-RAN Szövetség. Hozzáférés április 2, 2020. <https://www.o-ran.org/>.

¹⁹⁴ Wheeler, "Titkos szósz".

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 43**

¹⁹⁵ Mackenzie Eaglen, "Mi lenne, ha a Pentagon kihagyná az 5G-t?", Ideas. *Defense One*, 2020. május 11., <https://www.defenseone.com/ideas/2020/05/what-if-pentagon-skipped-5g/165277/>; Hitchens, "US Risks".

a "bizalmatlanság, de ellenőrizze"¹⁹⁶, a mérséklési stratégia lehetőséget biztosít, ugyanakkor visszatartja és proaktívan védekezik az ellenséges lépések¹⁹⁷ ellen. A Huawei kizárása a piacról viszont nem csökkenti az általa és a KNK által jelentett kockázatokat, sőt, vitathatatlanul felerősíti azokat. Bizonyára van olyan lehetőség, amely mindkét fél számára előnyös, és az Egyesült Királyság eddig úgy tűnik, hogy ezt hatékonyan követi. Van azonban még hova fejlődni.

¹⁹⁶ Cliff Kupchan és Paul Triolo, "Distrust but Verify: How the U.S. and China Can Work Together on Advanced Technology," Business and Tech-Opinion, *SupChina*, 2019. november 26., <https://supchina.com/2019/11/26/distrust-but-verify-the-us-china-advanced-technology/>.

¹⁹⁷ Julia Voo és Cindy Gao, "U.S.-China Cyber Competition and Cooperation with Julia Voo," By Joanna Chiu, Podcasts-NuVoices, *SupChina*, April 3, 2020, Audio, 54m:33s. <https://supchina.com/podcast/u-s-china-cyber-competition-and-cooperation-with-julia-voo/>.

Az 5G hatásai a teljesítményre

Az 5G állítólag kulcsszerepet játszik az információs technológia uralmában, ami viszont a 21st. század uralmának kulcsa¹⁹⁸. Az 5G hálózatok kulcsfontosságúak a Digitális Selyemút¹⁹⁹ szempontjából, amely összeköti a Kínai Népköztársaság Övezet és Út kezdeményezését²⁰⁰. Az 5G hálózatok lehetővé teszik majd új technológiák sokaságának széles körű kereskedelmi hasznosítását, többek között a kvantumszámítástechnikát, a mesterséges intelligenciát (AI), az automatizált gyárakat, az autonóm autókat, az intelligens városokat, a kiterjesztett/virtuális valóságot és az egészségügyi folyamatok optimalizálását. Ezeknek az egyes technológiáknak a társadalomra gyakorolt teljes hatása még nem ismert. Gazdasági hatásuk az előrejelzések szerint nagy lesz. Taktikai²⁰¹ (bár talán nem stratégiai²⁰²) hatásaik azonban forradalmiak²⁰³ lehetnek (néhány fenntartással²⁰⁴).

Az 5G maga is számos katonai alkalmazással²⁰⁵ rendelkezik. Ezeket az alkalmazásokat a közbeszédben²⁰⁶ gyakran figyelmen kívül hagyják. A kémkedés mellett ez is része annak, hogy az 5G biztonsága továbbra is vitatott terület.

Az Egyesült Királyságban a kritikus maghálózatoktól való eltiltáson és a magas kockázatú hálózati szállítókra vonatkozó 35%-os piaci részesedési korláton kívül a Huawei által az ilyen technológiák fejlesztésére vonatkozóan még nem határozták meg a korlátokat. Megalapozottak azonban az aggodalmak, hogy a Huawei 5G hálózatok fejlesztése

¹⁹⁸ Allison, "AI Supremacy"; Hitchens, "US Risks".

¹⁹⁹ Clayton Cheney, "Kína digitális selyemútja: Stratégiai technológiai verseny és a politikai illiberalizmus exportálása", Blog-Net Politics, Council on Foreign Relations, 2019. szeptember 26., <https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political>.

²⁰⁰ Andrew Chatzky és James McBride, "China's Massive Belt and Road Initiative," Backgrounder, Council on Foreign Relations, Hozzáférés 2020. március 24., <https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-kezdemenyezés>.

²⁰¹ Mark Esper, "Globális Biztonsági Fórum: H. Hicks, Transcript, CSIS, 2020. január 24., <https://www.csis.org/analysis/global-security-forum-emerging-technologies-governance>. ²⁰² James Andrew Lewis, "Can Artificial Intelligence Compensate for Strategic Shortcomings?", Commentary, CSIS, 2020. január 29., <https://www.csis.org/analysis/can-artificial-intelligence-compensate-strategic-hianyossagok>.

²⁰³ Michael E. O'Hanlon, "Forecasting Change in Military Technology, 2020-2040", Research-Report, The Brookings Institution, 2018. szeptember, <https://www.brookings.edu/research/forecasting-change-in-military-technology-2020-2040/>.

²⁰⁴ Laura Schousboe, "The Pitfalls of Writing About Revolutionary Defense Technology," Commentary, *War on the Rocks*, 2019. július 15., <https://warontherocks.com/2019/07/the-pitfalls-of-writing-about-revolutionary-defense-technology/>.

²⁰⁵ William Schneider Jr, "Why 5G is a Big Deal for Militaries Throughout the World", Opinion, *C4ISRNET*, 2019. február 5., <https://www.c4isrnet.com/opinion/2019/02/05/why-5g-is-a-big-deal-for-militaries-throughout-the-world/>.

²⁰⁶ Erica D. Borghard és Shawn W. Lonergan. "The Overlooked Military Implications of the 5G Debate," Blog-Net Politics, Council on Foreign Relations, 2019. április 25., <https://www.cfr.org/blog/overlooked-military-implications-5g-debate>.

példátlan mértékű hatalmat összpontosítanak ezen új technológiák²⁰⁷ felett. Ez a hatalom az Egyesült Királyságot és másokat is kiszolgáltatottá tehet a Huawei és ezen keresztül a Kínai Népköztársaság szeszélyeinek. Bár alig tárgyalják, az IoT-eszközök fegyverre tétele konfliktusok során, szemben a konfliktusokkal vagy konfliktusok nélküli megfigyeléssel, ez az, ami valóban az 5G-vita²⁰⁸ középpontjában áll.

Ez a kockázat azonban egy olyan félelemből fakad, amely még nem nyilvánult meg. A Huawei jelenlegi sikere az 5G-piacon nem jelenti azt, hogy a jövőben uralni fogja az IoT-piacot. Bár a Huawei talán előnyben van, a viszonylag közelmúlt történelmében a Nyugat a liberálisabb értékek és intézmények²⁰⁹ miatt sikeresebb volt az új technológiák létrehozásában és az innovációs eljárásokban. A KNK ezzel szemben nagyrészt a későn érkező előnyét²¹⁰ élvezte.

Most, az 5G és 6G technológiába való betörésükkel a Huawei és a Kínai Népköztársaság azt remélik, hogy "elsőként lépnek a piacra"²¹¹. Az elsőként lépő státusz önmagában még nem jelent előnyt²¹². Ez valóban kétélű kard²¹³. Az 5G és a 6G esetében azonban, különösen, ha az AI-val kapcsolódik (lásd még), a tét sokkal nagyobb lesz, és valószínűleg lehetővé teszi, sőt tartósan meg is szilárdítja az egypólusú hegemonia²¹⁴ következő korszakát. Ennek ismeretében az EU, az Egyesült Királyság, az Egyesült Államok és Kína már most versenyben van a 6G-ért a 2030²¹⁵.

Amint azt az Egyesült Államok Védelmi Innovációs Testületének (DIB) 2019-es, az 5G-ről szóló jelentése tárgyalja, az első lépcsőfok státusznak "kereskedelmi, versenyképességi és biztonsági vonatkozásai"²¹⁶ vannak, és az előnyök közé tartozik az infrastruktúra és más termékek szabványainak és specifikációinak meghatározása. Ugyanakkor a jelentés megjegyzi, hogy ha az első lépésben haladók nem tudnak innoválni, akkor jelentősen lemaradnak²¹⁷. Az 5G és a

²⁰⁷ Bob Seely, Peter Varnish Obe és John Hemmings, "Defending Our Data: Huawei, 5G, and the Five Eyes," Ázsiai Tanulmányok Központja. Henry Jackson Society, 2019. május, <https://henryjacksonsociety.org/wp-content/uploads/2019/05/HJS-Huawei-Report-A1.pdf>.

²⁰⁸ "Amerika nem akarja, hogy Kína uralja az 5G-t", *The Economist*.

²⁰⁹ Regina M. Abrami, William C. Kirby és F. Warren McFarlan, "Why China Can't Innovate", *Innovation, Harvard Business Review*, 2014. március, <https://hbr.org/2014/03/why-china-cant-innovate>; Blanchard és Michael, "Innovation is 'Achilles Heel'".

²¹⁰ Justin Yifu Lin, "Advantage of Being a Latecomer," *Opinion, China Daily*, 2013. augusztus 7., http://www.china.org.cn/opinion/2013-08/07/content_29646629.htm.

²¹¹ Kennedy, "Kína egyenetlen".

²¹² William Boulding és Markus Christen, "First-Mover Disadvantage", *Financial Management, Harvard Business Review*, október h2001, <https://hbr.org/2001/10/first-mover-disadvantage>.

²¹³ Ronald Klingebiel és John Joseph, "When First Movers are Rewarded, and When They are Not," *Innovation, Harvard Business Review*, 2015. augusztus 11., https://hbr.org/2015/08/when-first-movers-are-rewarded-and-when-theyre-not?referral=03759&cm_vc=rr_item_page.bottom.

²¹⁴ Allison, "AI Supremacy"; Indermit Gill, "Whoever Leads in Artificial Intelligence in Will 2030 Rule the World Until 2100", *Blog-Future Development, The Brookings Institution*, 2020. január 17., <https://www.brookings.edu/blog/future-development/2020/01/17/whoever-leads-in-artificial-intelligence-in-2030-will-rule-the-world-until-2100/>.

²¹⁵ Martijn Rasser, "Setting the Stage for U.S. Leadership in 6G", *Cyber & Technology, Lawfare*, 2019. augusztus 13., <https://www.lawfareblog.com/setting-stage-us-leadership-6g>.

²¹⁶ Medin et al., "5G Ecosystem", p. 6.

²¹⁷ Ibid., 6-7. o.

6G, ez a Nyugatot kényes, de talán előnyös helyzetbe²¹⁸ hozza.

Dr. Lewis ugyanis, miközben kijelenti, hogy a teljes betiltás a legbiztonságosabb megközelítés, elismeri az Egyesült Királyság és Európa gazdasági érdekeit is a Huawei-jel és a KNK-val való együttműködésben. Míg az öt szem partner, Európa, Japán és Dél-Korea mind versenyképesebbek az 5G területén, mint azt a diskurzus gyakran sugallja, és az előnyben részesített nyugati 5G vállalatok, a Nokia, az Ericsson és a Samsung jobb minőségűek, mint a Huawei, mindegyikük egymásra²¹⁹ van utalva. Ha a nyugati országok és szövetségeseik együtt tudnak működni gazdasági, biztonsági, jogi és polgári aggodalmaikban, rövid távon előnyükre válhat a Huawei és a KNK együttműködésével, miközben hosszú távon is átvehetik a vezetést. Dr. Lewis azonban arra figyelmeztet, hogy míg az Egyesült Államok különösen az 5G piacvezető szerepére van felkészülve, addig a globális vezető szerep általában és az 5G és a kiberbiztonság tekintetében hiányzik²²⁰.

Ez összességében megerősíti az Egyesült Királyság gazdasági integrációját A KNK és a Huawei által biztosított ipari erő kihasználása lehetővé teszi a Nyugat számára, hogy olyan módon fejlessze ki az innovációhoz és a specializációhoz szükséges ipart, ahogyan a KNK modellje nem teszi lehetővé. Ez a szimbiózis a Kínai Népköztársaságot is visszatarthatja attól, hogy rosszindulatúan használja a Huaweiit, mivel fennáll annak a veszélye, hogy megfosztják őket attól, amit a gazdasági modelljük jellemzően nem tudott produkálni - a találékonyságtól.

A Huawei hazai piacra gyakorolt hatása lehetővé teszi az alternatív távközlési versenytársak számára, hogy a saját szakterületükön versenyezzenek, miközben a Huawei biztosítja a berendezések nagy részét. Ez csökkentené a Huawei hatalomkoncentrációját azáltal, hogy olyan piaci résszerepeket határoz meg, amelyeket a Huawei nem biztosít. A Huawei termelési kapacitása viszont ösztönözheti a növekedést ezekben a résárgazatokban.

A Huawei brit piacra lépésének megakadályozása csökkenti a jövőbeni versenyképes IoT-piac kilátásait. A drágább távközlési szolgáltatóktól való függés növeli az indulási költségeket, csökkenti a kutatási és fejlesztési projektekhez rendelkezésre álló tőkét, és akadályozza az innovációt. Az Egyesült Királyság szabad piaci struktúrája a Huawei termelési árréséből profitál, mivel a piaci körülményekre reagál. Az 5G lehetővé tétele elhozza a szükséges kreativitási hullámot, amely arra készíti az ipart, hogy reagáljon a keresletre, ahol a Huawei nem tud teljesíteni. Így a kockázatok, lehetőségek, költségek és előnyök mérlegelése során a Huawei számára az 5G fejlesztésének engedélyezése az Egyesült Királyságban jobb választásnak tűnik, mint a piacról való kitiltás.

²¹⁸ Medin et al. "5G Ecosystem"; Budden és Murray, "Defense Innovation"; Morgan Dwyer, "An Alternative to the Defense Department's New, Technology-Focused Organizations", Commentary, CSIS, January 22, 2020, <https://www.csis.org/analysis/alternative-defense-departments-new-technology-focused-organizations>; Hicks et al. "Getting Less".

²¹⁹ Lewis, "Nyilatkozat 5G"; "Szenátus 5G".

²²⁰ James Andrew Lewis, "Cyber Solarium and the Sunset of Cybersecurity", Commentary, CSIS, március 13, 2020, <https://www.csis.org/analysis/cyber-solarium-and-sunset-cybersecurity>.

Egyesült Királyság-USA kapcsolatok

Részben a Huawei-t érintő 5G-politikák miatt az angol-amerikai védelmi és hírszerzési kapcsolatok egyre feszültebbé váltak. Májusban Trump amerikai 2019. elnök azzal fenyegetőzött, hogy korlátozza a hírszerzési információk megosztását, amennyiben a Huawei számára engedélyezik az 5G fejlesztését az Egyesült²²¹ Királyságban. 2020. január 27-én amerikai szenátorok törvényjavaslatot terjesztettek elő, hogy korlátozzák a hírszerzési információmegosztást minden olyan országgal, amely lehetővé teszi a Huawei számára, hogy 5G-hálózatot fejlesszen. Egyes szenátorok kifejezetten megfenyegették az Egyesült Királyság és az Egyesült Államok hírszerzési kapcsolatát²²². Ez drasztikusnak, sőt kontraproduktívnek tűnik, tekintettel az amerikai külföldi hírszerzési megosztás²²³ előnyeire és kockázataira, valamint arra, hogy az USA nem tudott alternatív megoldást kínálni.

Az ilyen fenyegetések politikai kimenetelét nehéz volt megjósolni, amikor ez az esszé először készült 2019 nyarán, Johnson brit miniszterelnök megválasztása miatt. Azóta több fejlemény is megszüntette a kétértelműséget. Mások megerősítették a 2019-es tervezetben szereplő, a mérséklési stratégia és a részleges tilalom melletti érvek relevanciáját.

Megdöböntő módon brit tisztviselők kijelentették, hogy átgondolják az Egyesült Államokkal való hírszerzési és védelmi partnerségüket. Úgy tűnik, hogy ez Trump elszigetelődési politikájának, a Huawei-jel kapcsolatos fenyegetéseknek és különösen az amerikai Soleimani-gyilkosságnak²²⁴ az eredménye. Egy 2020. január 12-i interjúban Wallace brit védelmi miniszter kijelentette, hogy aggódik az USA globális vezetésből való kivonulása miatt. Wallace azt is kijelentette, hogy az Egyesült Királyság túlzottan függ az USA "légi fedezetétől ... hírszerzési, megfigyelési és felderítési eszközeitől"²²⁵, és hogy az Egyesült Királyságnak el kell kezdenie az ilyen partnerségek diverzifikálását.

Valószínűleg az ilyen fejleményekre való tekintettel Boris Johnson miniszterelnök és a Nemzetbiztonsági Tanács 2020. január 28-án úgy döntött, hogy engedélyezi a "magas kockázatú szállítók", köztük a Huawei számára, hogy az Egyesült Királyság vezeték nélküli és 5G infrastruktúrájához alkatrészeket szállítsanak. Az ilyen szállítók

²²¹ Telegraph Reporters, "Donald Trump Could 'Limit Sharing of US Intelligence With the UK 'if Britain ' Fails to Ban Huawei,'" Technology Intelligence, *The Telegraph*, May 31, 2019,

<https://www.telegraph.co.uk/technology/2019/05/31/donald-trump-could-limit-sharing-us-intelligence-uk-britain/>.

²²² Joe Gould, "Key Republicans Seek Ban on Intel Sharing with Countries that Use Huawei," 5G, *C4ISRNET*, 2020. január 27., <https://www.c4isrnet.com/congress/2020/01/27/key-republicans-seek-ban-on-intel-sharing-with-countries-that-use-huawei/>.

²²³ Michael E. DeVine, "Az Egyesült Államok külföldi hírszerzési kapcsolatai: Report, Congressional Research Service, 2019. május 15., <https://fas.org/sgp/crs/intel/R45720.pdf>.

²²⁴ Adam Bienkov, "The UK is Abandoning Its Alliance with Trump as the United States 'Withdraws from Its Leadership Around the World'", Analysis, *Business Insider*, 2020. január 12., <https://www.businessinsider.com/uk-abandoning-trump-iran-us-withdraw-leadership-world-qassem-soleiman2020-1>.

²²⁵ Tim Shipman, "Ben Wallace interjú: News, *The Sunday Times*, 2020. január 12., https://www.thetimes.co.uk/edition/news/ben-wallace-interview-we-cant-rely-on-us-pmwcv398?wgu=270525_54264_15817040629028_276d8c4cf9&wgexpiry=1589480062&utm_source=planit&utm_medium=affiliate&utm_content=22278.

olyan komponensek biztosítására korlátozódnak, amelyek "nem veszélyeztetik a rendszer(ek) integritását"²²⁶.

2020. május elején az amerikai kongresszus tagjai olyan módosítást javasoltak a közelgő védelmi költségvetéshez, amely megakadályozná, hogy az amerikai F-35 Joint Strike Fighter (JSF) vadászgépeket olyan nemzetek vásárolják meg, amelyek lehetővé teszik a magas kockázatú szállítók 5G és 6G hálózataikban való részvételét. A JSF-programban kilenc nemzet vesz részt: az Egyesült Államok, az Egyesült Királyság, Hollandia, Olaszország, Ausztrália, Norvégia, Dánia, Kanada és Törökország. További ügyfelek közé tartozik Izrael, Dél-Korea, Belgium, Japán, Lengyelország és Szingapúr. Kanada még nem kötelezte el magát az F-35 beszerzése mellett, Törökországot pedig az új orosz rakétarendszerek²²⁷ beszerzése miatt tiltották el.

Az Egyesült Királyság ezt megdöbbentő fejleménynek tekintette, különösen a jelenlegi globális instabilitás és az amerikai fenyegetések fényében, és igyekszik biztosítani, hogy ez a módosítás ne kerüljön elfogadásra. Mindennél inkább úgy tűnik, hogy ez egy újabb példa az USA kontraproduktív diplomáciai nyomására. A JSF-programban vásárolni kívánt, és ami még fontosabb, abban részt venni kívánó nemzetek közül sokan már most is a Huawei általánosságban és az 5G számára is biztosítanak hálózati komponenseket.

Mindazonáltal nem valószínű, hogy a "különleges" amerikai-brit hírszerzési kapcsolat megszűnne²²⁸. Bár rövid távon politikai visszahatás érheti, az amerikai Nemzetbiztonsági Ügynökség továbbra is a GCHQ tengerentúli lehallgatóállomásokból álló hálózatára támaszkodik az adatgyűjtés során. Emellett az Egyesült Államok és az Egyesült Királyság közötti hírszerzési információcsere korlátozása nemcsak az Egyesült Államok és az Egyesült Királyság közötti partnerség átalakítását tenné szükségessé, hanem hatással lenne a többi Five Eyes-partnerre is, mivel jelenleg az összes hírszerzési információ mintegy 80%-át megosztják²²⁹ egymással.

Az ilyen változások minden érdekelt fél számára károsan hatnának a hírszerzési műveletekre. Ahogyan az is, hogy az 5G kifejlesztésében nem működünk együtt a Huawei-jel, sok országot öt-tíz évvel vetne vissza, miközben az USA még nem kínál életképes alternatívát²³⁰. Ezeket a tényeket mérlegelni kell azzal a kockázattal szemben, hogy a Huawei képes lesz a különböző kommunikációk megfigyelésére.

Az Egyesült Királyság és az Egyesült Államok kapcsolatát összetartó kötelékek egyelőre erősebbek, mint

²²⁶ Adam Satariano, "Britain Defies Trump Plea to Ban Huawei from 5G Network," *Technology, The New York Times*, január 28, 2020, <https://www.nytimes.com/2020/01/28/technology/britain-huawei-5g.html>.

²²⁷ Peter Suciú, "Tom Cotton is Trying to Block F-35 Deployment to the UK (Due to Huawei Worries)," *Blog-The Buzz, The National Interest*, 2020. május 8., <https://nationalinterest.org/blog/buzz/tom-cotton-trying-block-f-35-deployment-uk-due-huawei-worries-152251>; Oriana Pawlyk and Richard Sisk, "Lawmakers Consider Blocking Some F-35 Deployments Over Huawei 5G Network: News," *Military.com*, 2020. május 13., <https://www.military.com/daily-news/2020/05/13/lawmakers-consider-blocking-some-f-35-deployments-over-huawei-5g-network-reports.html>.

²²⁸ Michael S. Goodman, "The Foundations of Anglo-American Intelligence Sharing", *Studies in Intelligence* 59, no.

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 51**

2 (Kivonat, 2015. június): 1-12, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-2/pdfs/Goodman-Evolution-UK-US-JIC-June-2015.pdf>.

²²⁹ David Bond és Jim Pickard, "US Intelligence Threats to Britain 'Not Realistic', Say Spies," Political Espionage, *Financial Times*, 2019. május, <https://www.ft.com/content/8cdc7aee-83aa-11e9-b592-5fe435b57a3b>.

²³⁰ Gould, "Key Republicans".

A Huawei kockázata azzal fenyeget, hogy tönkreteszi. A Huawei fenyegetettségének elismerésével a hírszerző ügynökségeket arra ösztönzik, hogy új módszereket mérlegeljenek e kockázatok elhárítására, azaz a külföldi szereplők által a kritikus hálózatokban jelentett fenyegetés korlátozására, aminek az Egyesült Királyságban most úgy tűnik, hogy ez folyamatban van²³¹. Egy összetett, globalizált világban többdimenziós értékeléseket kell készíteni a partnerségekről, azok kockázatairól, költségeiről, előnyeiről és a bizalomépítés lehetőségeiről. Ellenkező esetben mindenki veszít²³². Függetlenül az USA álláspontjától, a Huawei és a hasonló szervezetek brit felügyelete nagyban segíthet az ilyen fenyegetések enyhítésében, különösen, ha a felügyelet nemzetközi törekvéssé válik.

A Huawei kizárása a piacról nem oldja meg a Kínával szembeni bizalmatlanság eredendő problémáját. Valójában a Huawei kizárása további ellenségeskedésre ösztönzi a KNK-t egy olyan világban, ahol szinte lehetetlen nem együttműködni a KNK-val. A Huawei-ellenes politika nemzeti szinten és a többi nemzetközi partner hasonló intézkedések elfogadására való nyomásgyakorlás megzavarja a biztonságot, a piacot, és minden fél számára káros. Ez különösen igaznak tűnik, tekintve, hogy a Huawei technológiai szempontból a versenytársak előtt jár.

²³¹ Satariano, "Britain Defies"; "5G Round Up", NCSC.

²³² Richard Oliver, "Partnerség és biztonság: Wilson Center, 2005. július 12.,

<https://www.wilsoncenter.org/event/partnership-and-security-advancing-the-usuk-defense-technology-relationship-the-era>; Nietzsche and Rasser, "Washington's Reboot": "Advancing US/UK Defense Technology Relationship in the Era of Globalization", Event-Summary Transcript, Edited by Peter Bean, Wilson Center, 2005. július 12., <https://www.wilsoncenter.org/event/partnership-and-security-advancing-the-usuk-defense-technology-relationship-the->

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 53**

[era](#); Nietzsche and Rasser, "Washington's Reboot".

Harmadik rész - Lehetőségek, kihívások és megoldások

Lehetőségek

A HCSEC nemzetközivé tétele

Az előző és a következő problémákat az Egyesült Királyság számára lehetőségként lehet átfogalmazni. Úgy tűnik, hogy a Huawei ügyfélállamai közül az Egyesült Királyság vette a legkomolyabban a kiberbiztonságot a HCSEC létrehozásával és az arra szánt erőforrásokkal. Ha az Egyesült Királyság és a HCSEC vezető szerepet vállal, különösen a többoldalú megközelítés révén, akkor a világ számára a Huawei-nek a jobb kiberbiztonsági gyakorlatok többoldalú javítására irányuló számonkérése érdekében gyűjtőintézménnyé válhat. Továbbá az Egyesült Királyság egyedülálló helyzetben van ahhoz, hogy a Huawei felelősségre vonásával a Kínai Népköztársaság is felelősségre vonja.

A Kínai Népköztársaság jellemzően a Biztonsági Tanács vétójogának gyakorlásával és azzal, hogy a többoldalú tárgyalások helyett kétoldalú tárgyalásokat²³³ követelhet, elkerüli a nemzetközi elszámoltathatóságot. Ha az Egyesült Királyság nemzetközivé teszi a HCSEC-et, és agresszívebben kiterjeszti meglévő biztonsági megállapodásait, akkor ez a Huawei és a Kínai Népköztársaság elszámoltatásának lehetősége nagymértékben felerősödhet. Ha az EU követi az Egyesült Királyság közelmúltbeli példáját a kiberbiztonság és az együttműködés terén, amikor a Huawei-ről van szó, akkor az enyhítő koalíció valósággá²³⁴ válhat.

A Brexit kapcsán az Egyesült Királyságnak az EU-val fennálló kiberbiztonsági kapcsolata 2020 decemberéig fennmarad, mielőtt felülvizsgálják és esetleg meghosszabbítják. A meghosszabbítások vagy újratárgyalások szinte biztosan magukban foglalják majd az 5G és a 6G szakpolitikákról²³⁵, valamint az Egyesült Királyság következő nemzeti kiberbiztonsági stratégiájáról²³⁶ szóló megbeszéléseket is. Ha eljön az idő, az Egyesült Királyságnak hangsúlyoznia kell, sőt talán még ki is kell használnia a Huawei, az 5G és a 6G tekintetében meglévő egyedi eszközeit és képességeit, amelyeket a HCSEC testesít meg.

Ha az Egyesült Államokat meg lehet győzni arról, hogy a 2020. januári képviselőházi törvényjavaslat²³⁷ és a 2020²³⁸. március 11-én közzétett kongresszusi kibertér-szolárium bizottsági jelentés szerint diktálás helyett működjön együtt a szövetségesekkel és partnerekkel, annál jobb. Dr. Lewis azonban a jelentés áttekintésében úgy érvel, hogy míg a jelentés a kiberbiztonsági normák létrehozására és érvényesítésére vonatkozó felhívása egy vezetői csoport vezetésével

²³³ Sylvia Hui, "Egy feltörekvő szuperhatalom bevonása: Asia Programme Paper, Chatham House, 2011. július, https://www.chathamhouse.org/sites/default/files/0711pp_hui.pdf; China Team, "The Costs of International Advocacy: China's Interference in United Nations Human Rights Mechanisms," Report, Human Rights Watch, 2017. szeptember 5., <https://www.hrw.org/report/2017/09/05/costs-international-advocacy/chinas-interference-united-nations-human-rights>.

²³⁴ "EU-megállapodások", CNBC a Reutersen keresztül.

²³⁵ Doug Olenick, "Brexit Cybersecurity Implications Hold Steady During Transition Period", Security News, SC Magazine, 2020. január 31., <https://www.scmagazine.com/home/security-news/brexit-cybersecurity-implications->

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 55**

[hold-steady-during-transition-period/](#).

²³⁶ "National Cyber", HM kormány; "National Progress", HM kormány.

²³⁷ Emily Birnbaum, "House Passes Bills to Gain Upper Hand in Race to 5G," Policy, *The Hill*, január 08, 2020, <https://thehill.com/policy/technology/477429-house-passes-bills-to-gain-upper-hand-in-race-to-5g>.

²³⁸ U.S. Cyberspace Solarium Commission, elnöke Angus King és Mike Gallagher, "Report", US Congress, március 11, 2020, <https://www.solarium.gov/report>.

a demokráciák koalíciója erősség, több kérdés is jelentősen aláásta. Ezek voltak a jelentésben az elrettentés hangsúlyozása (amely passzív és megkerülhető), az amerikai politika jelenlegi pártoskodása, és különösen a jelenlegi vezetés a végrehajtó hatalomban és annak egészében²³⁹.

Dr. Lewis elemzése megerősíti azokat az érveket, amelyek az Egyesült Királyság vezető szerepe mellett szólnak.

A HCSEC nemzetközivé tétele jelentősen javíthatná mind a HCSEC, mind az Egyesült Királyság azon képességét, hogy azonosítsa és elhárítsa a jelenlegi, az 5G és a 6G infrastruktúrát fenyegető kiberbiztonsági veszélyeket. A HCSEC nemzetközivé tétele az Egyesült Királyságnak és partnereinek is nagyobb befolyást biztosíthatna, amikor a Huawei, a ZTE-t (egy másik kínai távközlési vállalat) és a KNK-t jobb kiberbiztonsági és kereskedelmi gyakorlatok követésére ösztönzik. Egy ilyen koalíció kölcsönösen előnyös lenne a kormányok, a magánszervezetek és a fogyasztók számára világszerte.

Továbbá egy ilyen koalíció jó helyzetben lehet ahhoz, hogy a 6G megjelenésekor proaktív legyen, talán vezető szerepet vállalva az éves 6G Wireless Summiton (alapítva 2019-ben)²⁴⁰, különösen mivel az USA küzd az 5G és a 6G vezető²⁴¹ szerepének megteremtéséért. A Huawei már 2019 elejére célul tűzte ki a 6G dominanciáját a kutatás-fejlesztés és a szellemi tulajdon²⁴² tekintetében. A Huawei nyugaton az 5G-vel kapcsolatos nehézségei és a 6G felsőbbrendűségére vonatkozó elképzelései között (ami még azt is eredményezte, hogy fontolóra vette az 5G feletti ellenőrzésről való lemondást nyugaton)²⁴³, egy olyan szervezet nemzetközivé válása, mint a HCSEC, felbecsülhetetlen értékű geopolitikai eszközzé válhat.

Az olyan szervezetek, mint a HCSEC azonban nem csak a Huawei-re kellene, hogy összpontosítsanak. Érdemes feltenni a kérdést, hogy miért tartják a Huawei-t ilyen egyedülálló mértékű ellenőrzésnek? Miért nincs kiberbiztonsági értékelő központ a ZTE számára? Persze, hogy kisebb, mint a Huawei, de állítólag kémkedési²⁴⁴ céllal hozták létre, korrupciós²⁴⁵ múltja van, és még ahhoz is elég fontos volt, hogy a KNK megkérje Trump elnököt, hogy különleges bánásmódot és mentességet²⁴⁶ adjon neki, amit ő a szélesebb körű következmények²⁴⁷ ellenére meg is adott. A ZTE-t félretéve, miért nincs kiberbiztonsági értékelő központ a

²³⁹ Lewis, "Cyber Solarium".

²⁴⁰ 6G Wireless Summit. <http://www.6gsummit.com/>

²⁴¹ Rasser, "A 6G beállítása"; Kania, "Miért nem".

²⁴² Iain Morris, "Huawei Sets Sights on 6G Stardom Amid 5G Strife," 5G, *Light Reading*, 2019. február 15., <https://www.lightreading.com/mobile/5g/huawei-sets-sights-on-6g-stardom-amid-5g-strife/d/d-id/749497>.

²⁴³ Morris, "6G fegyverkezési verseny".

²⁴⁴ Tara Francis Chan, "The Very Purpose of the Chinese Tech Company ZTE is to Spy on Other Countries, a Competitor Alleges in New Court Documents," *Business Insider*, 2018. június 1., <https://www.businessinsider.com/zte-created-to-spy-according-to-new-court-documents-2018-6>.

²⁴⁵ "ZTE," News-Topics, Anti-Corruption Digest, Hozzáférés: 2020. március 3., <https://anticorruptiondigest.com/news-topics/zte/#axzz6Hk3lZgYv>.

²⁴⁶ Henry Farrell, "Bolton azt állítja, hogy Trump kisegítette Kína vezetőjét a ZTE-vel kapcsolatban. Mi az a ZTE?," News- Monkey Cage-Analysis, *The Washington Post*, január28,2020., <https://www.washingtonpost.com/politics/2020/01/28/bolton-alleges-that-trump-helped-out-chinas-leader-zte-whats-zte/>.

²⁴⁷ Ewan Sutherland, "The Strange Case of US v. ZTE: A Prosecution, a Ban, a Fine and a Presidential

FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 57

Intervention", *Digital Policy, Regulation and Governance* no21., 6 (2019): 550-573, <https://doi.org/10.1108/DPRG-04-2019-0029>.

Nyugati kedvenc tech cégek Ericsson, Nokia, Samsung, vagy az Apple?

Legyen HCSEC ICSEC

Amint azt a tanulmány további részei bemutatják, a Huawei nem az egyetlen módja annak, hogy a Kínai Népköztársaság vagy más szereplők rosszindulatú cselekményeket hajtsanak végre. Egyértelműen szükség van egy nemzetközi testületre, amely az 5G, a 6G és tágabb értelemben véve a kiberbiztonság koordinálását végzi. Bár mások is szorgalmaztak egy ilyen szervezetet, eddig hiányzott a vezetés.

Továbbá, a Huawei-re²⁴⁸ összpontosítva sok ok, amiért *az összes* 5G és IoT vállalatot nagyobb vizsgálatnak kell alávetni, kimarad. Ezeket az okokat vizsgálva határozottan amellett szól, hogy az Egyesült Királyság létrehozhat és létre is kell hoznia egy Nemzetközi Kiberbiztonsági Értékelő Központot (ICSEC), amely nem csak a Huawei-re összpontosít. Ezáltal a már meglévő proaktív megközelítést továbbfejleszthetnék, és mások segítségével fejlesztenék azt.

Egyrészt a biztonsági aggályok nem egyenlőtlenek, mivel a nyugati technológiai vállalatoknak nagyobb kultúrája volt a biztonságnak az ipari tervezési folyamat részeként történő integrálására, ahelyett, hogy utólagosan, az alapvető folyamatok²⁴⁹ befejezése után építették volna be a biztonságot. Másrészt mind a nyugati, mind a nyugati preferált vállalatoknak és kormányoknak egyaránt megvannak a maguk biztonsági problémái és kockázatai.

Ezek elsősorban az ellátási láncuk, az infrastruktúrájuk és szolgáltatásaik (beleértve a rossz forráskódokat), az eszközeik, valamint a kevésbé tárgyalt korrupció és más belső emberi biztonsági kötelezettségek²⁵⁰ következményei. Az ellátási lánc problémáinak, a Nyugat és szövetségeseik által kedvelt 5G-s előfutároknak, valamint az 5G és a kiberbiztonság természetét is magában foglaló sarkalatos pontoknak a vizsgálata azt mutatja, hogy nem csak a Huawei-re összpontosító nemzetközi koalícióra van szükség, hanem az ICSEC-re is.

Kiberbiztonsági szakpolitikai központ

WEGNER, A KIBERSTATISZTIKÁK NEMZETKÖZI IRODÁJA (LÁSD A KOMPLEXITÁSRÓL SZÓLÓ RÉSZT), A KÖVETKEZŐ KORMÁNYZATI ÁTLÁTHATÓSÁGRÓL SZÓLÓ CIKK, STEIGER + VALERIANO A KIBERKONFLIKTUSOK MODELLJEINEK JAVÍTÁSÁRA IRÁNYULÓ LEHETŐSÉGEKRŐL.

KOLTON A KIBERDOKTRÍNÁK KIDOLGOZÁSÁNAK, KOMMUNIKÁCIÓJÁNAK ÉS MEGERŐSÍTÉSÉNEK JOBB KOORDINÁLÁSA ÉRDEKÉBEN

²⁴⁸ Wheeler és Simpson, "5G szükséges".

Elektronikusan elérhető a következő címen:

<https://ssrn.com/abstract=3646339>

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 59**

²⁴⁹ Rich Mogull, "Az Apple biztonsági stratégiája: Business-Security-Opinion, *MacWorld*, június 14.,
h2013, <https://www.macworld.com/article/2041724/apples-security-strategy-make-it-invisible.html>.

²⁵⁰ Medin et al., "5G Ecosystem"; Wheeler és Simpson, "5G Requires".

Kihívások

Ellátási láncok

Jon Boyens az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézetének számítógépes biztonsági részlegének helyettes vezetője és a kiberehívási láncok kockázatkezelésének programvezetője.

Annak ellenére, hogy az 5G RAN hardverellátási láncok viszonylag biztonságosak, többet kell tenni az 5G RAN ellátási láncok és az ellátási láncok szélesebb körű²⁵¹ biztonsága érdekében. Bár messze nem egy nagyszerű mérőszám, az Egyesült Királyság 2016-2021 közötti időszakra vonatkozó nemzeti kiberbiztonsági stratégiája csak háromszor említi az ellátási láncokat, és a 2019-es előrehaladási jelentés is csak kétszer²⁵² említi őket. Sőt, még 2020-ban is úgy tűnik, hogy az Egyesült Királyság és az Egyesült Államok állami és magánhatóságai húzták az időt, amikor az ellátási láncok fenyegetéseivel²⁵³ való agresszívebb foglalkozásról volt szó, bár a koronavírus miatt az ellátási láncok kockázatai²⁵⁴ kerültek a figyelem középpontjába. A rendelkezésre álló források és az Egyesült Államok magasabb színvonalra vonatkozó állításai miatt ez a szakasz az amerikai (védelmi) ellátási lánc problémáira összpontosít, amelyek vitathatatlanul hasonlóak az Egyesült Királyságéhoz.

Először is, az amerikai védelmi iparnak számos (kiber)biztonsággal kapcsolatos ellátási láncproblémája²⁵⁵ van. Ezek gyakran érintik a vállalkozókat és a KNK-t²⁵⁶, és súlyosbítja őket a korrupció²⁵⁷ szélesebb körű története. A káosz által motivált, szándékos csalás számos különböző

²⁵¹ "UK Telecoms Supply Chain Review Report," Notice, Department for Digital, Culture, Media & Sport, HM Government, July 22, 2019, <https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference>; Wheeler and Simpson, "5G Requires"; Sullivan and Lucas, "5G Cyber".

²⁵² "National Cyber", HM kormány; "National Progress", HM kormány.

²⁵³ Wheeler és Simpson, "5G Requires"; Trevor Taylor és Rebecca Lucas, "Management of Cyber Security in Defense Supply Chains", *RUSI News Brief*, 2020. április 24., <https://www.rusi.org/publication/rusi-newsbrief/management-cyber-security-defence-supply-chains>.

²⁵⁴ Conrad Prince, "The Coronavirus Pandemic and the Cyber Landscape," Commentary, RUSI, április 20, 2020, <https://rusi.org/commentary/coronavirus-pandemic-and-cyber-landscape>.

²⁵⁵ Medin et al., "5G Ecosystem"; Ariel (Eli) [sic] Levite, "ICT Supply Chain Integrity Principles for Governmental and Corporate Policies," Paper, The Carnegie Endowment for International Peace, 2019. október 4., <https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974>; "Supply Chain Risk Management," The National Counterintelligence and Security Center, Office of the Director of the National Intelligence, Accessed March 15, 2020, <https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats>.

²⁵⁶ Steven Aftergood, "Védelmi szerződéses csalás: Federation of American Scientists, 2019. május 10., <https://fas.org/blogs/secrecy/2019/05/defense-contracting-fraud/>; Darrel Williams, "US Logistics Boss Talks Risks to the Supply Chain and Protective Measures," By Jill Aitoro, Interviews, *DefenseNews*, 2019. október 28., <https://www.defensenews.com/interviews/2019/10/28/us-logistics-boss-talks-risks-to-the-supply-chain-and-protective-measures/>.

²⁵⁷ Philip M. Nichols, "To Whom Does a Defense Business Owe a Duty When There is an Opportunity to Pay a Bribe?," In *Ethical Dilemmas in the Global Defense Industry*, edited by Claire Finkelstein, Kevin Govern, and Daniel Schoeni, (pages tba), New York: Oxford University Press, 2020 (megjelenés előtt).

a kiberbiztonság²⁵⁸ és egyéb, a biztonságot, a műveleteket és a személyzetet veszélyeztető fenyegetések²⁵⁹. Úgy tűnik, az is probléma, hogy a védelmi ipar tagjai érzékeny eszközöket adnak el, vagy külföldi befektetések által kompromittálódnak, kevés felügyelet vagy következmény²⁶⁰ nélkül.

Mindezt bonyolítja, hogy a KNK az egyik legnagyobb megrendelője a kulcsfontosságú iparágakban tevékenykedő védelmi vállalkozóknak, amelyek közül néhányan segítenek a KNK tekintélyelvű modelljének²⁶¹ felépítésében és exportálásában. Ezek az iparágak viszont lobbierővel befolyásolhatják az amerikai kormányt. Különös aggodalomra és befolyásra ad okot a félvezetőipar, amely tekintetében a KNK jelenleg az USA-ra támaszkodik, és amely az 5G, az AI és a kvantumszámítástechnika²⁶² korában egyre fontosabbá válik.

2020 februárjában a Trump-kormányzat javasolta, hogy zárják be a tilalom azon kiskapuját, amely megakadályozza, hogy az amerikai vállalatok technológiai alkatrészeket adjanak el a Huawei-nek. A védelmi minisztérium beavatkozott azon iparágak nevében, amelyek aggódtak amiatt, hogy a korlátozások közvetlenül és közvetve hogyan befolyásolnák a Kínával folytatott kereskedelmüket, illetve azokat, akiket az befolyásolhat²⁶³. Mivel a félvezetőipar különösen aggódott amiatt, hogy a Huawei-nek történő csökkentett eladásai hogyan befolyásolhatják azt a képességüket, hogy az Egyesült Államok biztonsága érdekében termékeket állítsanak elő, a lobbizás átmenetileg leállította a terveket²⁶⁴. Heves vita után a Védelmi Minisztérium megfordította az irányt²⁶⁵. A cikk írásakor még nem jelentették be a végleges döntést.

Ahogy Dr. Lewis írja, komoly okok szólnak amellett, hogy továbbra is exportáljunk félvezetőket a következő országokba

²⁵⁸ Jonathan Dienst, Joe Valiquette, and Rich Schapiro, "New York Tech Firm Sold Chinese Equipment to U.S. Military, Feds Say," U.S. News, NBC News, November 7, 2019, <https://www.nbcnews.com/news/us-news/feds-raid-new-york-tech-firm-suspected-selling-chinese-equipment-n1078191>.

²⁵⁹ Kyle Rempfer, "DoD Bought Phony Military Gear Made in China, Including Counter-Night Vision Clothing that Didn't Actually Work," News-Your Military, *Military Times*, május 30, 2019, <https://www.militarytimes.com/news/your-air-force/2019/05/30/dod-bought-phony-military-gear-made-in-china-including-counter-night-vision-clothing-that-didnt-actually-work/>.

²⁶⁰ Sean Gallagher, "How US Software Ended Up Powering Chinese Assault Helicopters", Policy, *Ars Technica*, 2012. július 3., <https://arstechnica.com/tech-policy/2012/07/how-us-software-ended-up-in-chinese-assault-helikopterek/>; Cory Bennett és Bryan Bender, "How China Acquires 'the Crown Jewels' of U.S. Technology", Investigation, *Politico*, május 22, 2018, <https://www.politico.com/story/2018/05/22/china-us-tech-companies-cfius-572413>.

²⁶¹ Lindsay Gorman és Matt Schrader, "U.S. Firms Are Helping Build China's Orwellian State," Argument, *Foreign Policy*, 2019. március 19., <https://foreignpolicy.com/2019/03/19/962492-orwell-china-socialcredit-surveillance/>.

²⁶² Lewis, "Nyilatkozat igazságszolgáltatás".

²⁶³ Sanger és Perlroth, "Huawei Winning".

²⁶⁴ William Alan Reinsch, "Walk the Line", Commentary, CSIS, február h3, 2020, <https://www.csis.org/analysis/walk-line>.

²⁶⁵ Ellen Nakashima, Jeanne Whalen és David J. Lynch, "Pentagon Drops Opposition to New Rules that would Further Restrict Tech Sales to Huawei," Technology, *The Washington Post*, 2020. február 15.,

FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 62

<https://www.washingtonpost.com/technology/2020/02/14/pentagon-drops-opposition-new-rules-that-would-further-restrict-tech-sales-huawei/>.

a KNK²⁶⁶. Konkrétan, semmi sem akadályozza meg a KNK-t abban, hogy elérje saját, önálló félvezetőiparát, és bármilyen drasztikus korlátozás csak ártana az USA-nak, az amerikai félvezetőgyártó vállalatoknak, valamint az ezekre a vállalatokra támaszkodó amerikai vállalatoknak és szövetségeseknek (különösen Tajvannak²⁶⁷).

Hasonlóképpen, a globalizált világban a hagyományos exportellenőrzési politikák nem hatékonyak, és végrehajtásuk csak felgyorsítja a KNK fejlettebb félvezetőgyártóinak fejlődését.

Dr. Lewis szerint az USA-nak nem kell kizárnia a KNK-t vagy akár a Huawei a félvezetők exportjából. Inkább az USA érdekeit szolgálná jobban, ha az exportellenőrzést egy nagyobb stratégia részeként, körütekintően alkalmazná. Dr. Lewis azt javasolja, hogy az USA engedélyezze a félvezetőgyártó berendezések exportját a KNK-ba, de csak amerikai és megbízható, nem KNK-tulajdonban lévő cégeknek.

Az USA-nak a szövetségesekkel együtt kell dolgoznia a félvezető-kutatási és gyártási kapacitások fejlesztése érdekében, nyomást kell gyakorolnia a KNK piaci manipulációira és a szellemi tulajdon ellopására, és fokoznia kell a kémelhárítási erőfeszítéseket, nem a hallgatókra, hanem a kezelőkre összpontosítva. Ezt más, a Huawei és a KNK kockázatainak agresszívabb megfékezésével vagy elhárításával foglalkozó biztonsági szakértők is megerősítik, ugyanakkor el kell kerülni, hogy a csatát megnyerjük, csak azért, hogy a háborút elveszítsük a jelenlegi liberális rend, értékek és érdekek²⁶⁸ feláldozásával. Bár ezeket itt nem részletezzük, vannak konkrét lépések is, amelyeket a liberális kormányzati és nem kormányzati intézményeknek meg kellene tenniük a KNK-val²⁶⁹ fenntartott K+F-kapcsolataik biztonságának és jólétének javítása érdekében.

Ennek ellenére a Védelmi Minisztérium - részben a koronavírus miatt bekövetkezett - visszafordulása óta két másik ellátási láncra vonatkozó kockázat is a figyelem középpontjába került. Az első a ragadozó külföldi hitelezés, főként a KNK által, amely a védelmi iparon²⁷⁰ belüli és kívüli technológiai cégek széles körét célozza. A második az, hogy a kisebb védelmi vállalkozók a KNK-beli vállalatok technológiájára támaszkodnak. Ezek a vállalatok az amerikai védelmi ipar negyedét teszik ki, és jelenleg azért lobbiznak, hogy a 2020 augusztusi technológiai átállási határidőt februárra 2021²⁷¹ tegyék át.

Az ehhez hasonló példák egyértelműen bizonyítják, hogy átfogó kockázatcsökkentésre van szükség, amely képes

²⁶⁶ James Andrew Lewis, "Managing Semiconductor Exports to China", Commentary, CSIS, 2020. május 5., <https://www.csis.org/analysis/managing-semiconductor-exports-china>.

²⁶⁷ Cheng Ting-Fang és Lauly Li, "Chip Titan TSMC Caught in Crossfire between US and China," Business-Company in Focus, *Nikkei Asian Review*, május 15, 2020, <https://asia.nikkei.com/Business/Company-in-focus/Chip-titan-TSMC-caught-in-crossfire-between-US-and-China>.

²⁶⁸ Kania és Gorman, "United Talent"; Lairson, Skidmore és Xinbo, "US Backfired" (Az USA visszafelé sült el)

²⁶⁹ David Zweig és Siqin Kang, "America Challenges China's National Talent Programs," Report, CSIS, május 5, 2020, <https://www.csis.org/analysis/america-challenges-chinas-national-talent-programs>.

²⁷⁰ Valerie Insinna, "Pentagon Reports Boost in Predatory Foreign Investment to US Tech Firms Amid Pandemic Amid Pandemic," *C4ISRNET*, 2020. május 6., <https://www.c4isrnet.com/unmanned/2020/05/06/pentagon-reports-boost-in-predatory-foreign-investment-to-us-tech-firms-since-pandemic-start/>.

²⁷¹ Andrew Eversden, "Proposed Rule Banning Chinese Tech Needs to Consider Small Contractors, Senators

FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 64

Warn", Capital Hill, *Fifth Domain*, 2020. május 5., <https://www.fifthdomain.com/congress/capitol-hill/2020/05/05/proposed-rule-banning-chinese-tech-needs-to-consider-small-contractors-senators-warn/>.

a belső és külső tényezők kezelése. Az ellátási láncok biztonságának túl kell lépnie a partnereknek szóló kormányzati kérdőíveken és más jelenlegi szabványokon. Integrált kísérletet kell tenni arra, hogy adatokat gyűjtsünk mind a hagyományosabb internetalapú kiberfenyegetésekről, beleértve a rosszindulatú szoftvereket, mind pedig a rosszindulatú szereplők interakcióiról és beszélgetéseiről olyan helyeken, mint a sötét web, hogy "teljes képet" kapjunk²⁷².

Néhány nemzet lassan megpróbálja ezt megvalósítani, de a maximális hatékonysághoz nemzetközi erőfeszítésre és közös vezetésre lesz szükség. Ilyen vezetés valószínűleg nem fog egyhamar az USA részéről érkezni. Az USA belföldön és nemzetközileg is "a szakértők szerint az olyan alapvető kérdések széles skáláján, mint az 5G használatához szükséges spektrumgazdálkodás, a hálózati ellátási lánc biztonsága, az infrastruktúra fejlesztése és az adatmegosztás, a koherens politika hiánya miatt akadozik"²⁷³.

5G Előrelépők

A vállalati oldalon, a nyugati 5G-frontfutók közül csak az Apple-nek és a Samsungnak tűnik, hogy viszonylag minimális problémái vannak a korrupcióval és a biztonsággal. Az Apple nagymértékben támaszkodik a kínai telefongyártásra, és úgy tűnik, hogy minimális korrupciós problémái voltak, valószínűleg a felügyeletnek és a korrupcióval²⁷⁴ szembeni intoleranciának köszönhetően. A közelmúltban azonban legalább egy állítólagos korrupciós ügy történt, amely közvetlenül az Apple alkalmazottait érintette, és amely a Kínai Népköztársaságban történt. Úgy tűnik, hogy az Apple által lefolytatott vizsgálat tisztázta ezeket az állításokat²⁷⁵.

Ami még fontosabb, hogy az Apple már régóta állítja, hogy termékei és cége gyakorlatilag nem hackelhetőek. A közelmúlt eseményei ennek ellenkezőjét bizonyították. 2018-ban egy ausztrál tinédzser feltörte a biztonságos számítógépes rendszereiket²⁷⁶. A Google 2019-ben megállapította, hogy az Apple termékei évek óta feltörhetőek.

Elég volt meglátogatni a rossz weboldalt, vagy más feketepiaci (akár kormányok által vásárolt vagy készített)²⁷⁷ exploitokat. A Google is megállapította, és az Apple is elismerte, hogy a Kínai Népköztársaság feltörte a

²⁷² Brian Garmey, "How Federal Agencies Can Better Manage Supply-Chain Cyber Risks", Opinion, *Fifth Domain*, 2019. július 17., <https://www.fifthdomain.com/opinion/2019/07/17/how-federal-agencies-can-better-manage-supply-chain-cyber-risks/>.

²⁷³ Hitchens, "Amerikai kockázatok".

²⁷⁴ Christian Zibreg, "Corrupt Apple Manager Who Leaked Order Secrets to Asian Suppliers Brought to Justice," Apple, *Geek.com*, augusztus <https://www.geek.com/apple/corrupt-apple-manager-who-leaked-order-secrets-16-to-asian-suppliers-brought-to-justice-1277412/>2010.,

²⁷⁵ Yoko Kubota és Tripp Mickle, "Apple Investigated Possible Business Misconduct in its Supply Chain: Company Says it Found No Evidence of Bribery or Kickbacks," Tech, *The Wall Street Journal*, 2018. november 30., <https://www.wsj.com/articles/apple-investigated-possible-business-misconduct-in-its-supply-chain-1543620611>.

²⁷⁶ Erin Pearson, "Melbourne Teen Hacked into Apple's Secure Computer Network, Court Told," Crime, *The Age*, 2018. augusztus 16., <https://www.theage.com.au/national/victoria/melbourne-teen-hacked-into-apple-s-secure-computer-network-court-told-20180816-p4zxwu.html>.

²⁷⁷ John Naughton, "Gondolja, hogy az iPhone biztonságban van a hackerektől?: That's What They Want You to Think," Technology-Opinion, *The Guardian*, szeptember

FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 66

8,2019,<https://www.theguardian.com/technology/commentisfree>.

Apple-termékek az ujjur muszlimok megfigyelésére és bebörtönzésére, esetleg két évre. A megtorlástól való félelem miatt mindkét vállalat nem kívánta megemlíteni a KNK-t, mivel az ujjurokat rabszolgamunkára használják az Apple, a Google, a Dell, a Microsoft és más vállalatok, gyakran a Foxconn²⁷⁸ keresztül.

A tajvani gyártóóriás, a Foxconn az Apple legnagyobb gyártója, és a Kínában található gyáraiban az Apple termékeinek jelentős részét gyártja. A Foxconnnak is vannak saját korrupciós ügyei az Apple termékeivel²⁷⁹ kapcsolatban. Mind a korrupció, mind a Kínától való függés különböző ellátási lánc alapú kockázatokat jelent. A Foxconnt jelentős adatvédelmi incidensek is érték. Kettőt ugyanaz a hackercsoport követett el (2012-ben és 2019-ben)²⁸⁰, és legalább még egyet egymásik csoport 2015-ben²⁸¹. Úgy tűnik, hogy ezek a hackertámadások számos műszaki és személyzeti adathoz való hozzáférést eredményeztek, amelyeket sokféle módon lehetett és lehetett felhasználni.

2019 októberében a Samsung megszüntette mobiltelefon-gyártását a KNK-ban, és más délkelet-ázsiai országokba²⁸² helyezte át a termelést, bár ez nem teszi védetté a KNK-alapú kockázatokkal szemben. A dél-koreai korrupciós kultúra²⁸³, amely a Samsungot²⁸⁴ is érintette, kombinálva a

[/2019/sep/08/iphone-safe-from-hackers-think-again-ios-android-zero-day-exploit-zerodium-google-threat-analysis;](https://www.nbcnews.com/tech/security/iphone-spyware-lets-cops-log-suspects-passcodes-when-cracking-doesn-t-work-1209296) Olivia Solon, "iPhone Spyware Lets Police Log Suspects' Passcodes when Cracking Doesn't Work," Tech-Security, *NBC News*, May 18, 2020, <https://www.nbcnews.com/tech/security/iphone-spyware-lets-cops-log-suspects-passcodes-when-cracking-doesn-t-work-1209296>.

²⁷⁸ Patrick Howell O'Neill, "Apple Says China's Uighur Muslims were Targeted in the Recent iPhone Hacking Campaign," Computing, *MIT Technology Review*, szeptember 6, 2019, <https://www.technologyreview.com/2019/09/06/133138/apple-says-chinas-uighur-muslims-were-targeted-in-iphone-hacking-campaign/>; Jeremy Horwitz, "Apple, Foxconn, and 81 Others are Using Uighur Forced Labor", Mobile. *Venture Beat*, 2020. március 2., <https://venturebeat.com/2020/03/02/apple-foxconn-and-81-others-are-accused-of-using-uighur-forced-labor/>.

²⁷⁹ Aries Poon, "In Taiwan, Five Ex-Foxconn Employees are Indicted," Business, *The Wall Street Journal*, 2014. május 21., <https://www.wsj.com/articles/five-former-foxconn-employees-indicted-for-accepting-bribes-1400651370?tesla=y>; Malcom Owen, "Foxconn Investigating \$43M Fraud Ring Involving Faulty iPhone Parts," Articles, *Apple Insider*, 2019. december 18., <https://appleinsider.com/articles/19/12/18/foxconn-investigating-43m-fraud-ring-involving-faulty-iphone-parts>.

²⁸⁰ Juliette Garside, "Apple Supplier Foxconn Hacked in Factory Conditions Protest," Technology-Apple. 2012. február 9., <https://www.theguardian.com/technology/2012/feb/09/apple-foxconn-hackers-factory-conditions>; Duncan DeAeth, "Taiwan's Foxconn's Foxconn Victim of Webmail System Hack, Employee Data Compromised," Business, *Taiwan News*, 2019. április 15., <https://www.taiwannews.com.tw/en/news/3680809>.

²⁸¹ Kim Zetter, "Attackers Stole Certificate from Foxconn to Hack Kaspersky with Duqu 2.0," *WIRED*, június 15, 2015, <https://www.wired.com/2015/06/foxconn-hack-kaspersky-duqu-2/>.

²⁸² Ju-min Park, "Samsung Ends Mobile Phone Production in China," Technology News, *Reuters*, 2019. október 2., <https://www.reuters.com/article/us-samsung-elec-china/samsung-ends-mobile-phone-production-in-china-idUSKBNIWH0LR>.

²⁸³ Justin Fendos, "South Korea's Corruption Culture", The Korea's, *The Diplomat*, 2016. november 17., <https://thediplomat.com/2016/11/south-koreas-corruption-culture/>.

²⁸⁴ Heekyong Yang, "Samsung Sets Up Anti-Corruption Panel as Chief Faces Trials", Technology News, *Reuters*, 2020. január 8., <https://www.reuters.com/article/us-samsung-group-compliance/samsung-sets-up-anti-corruption-panel-as-chief-faces-trials-idUSKBN1Z80DR>.

FOLYTATANDÓ TERVEZET: 5G és a nemzetközi biztonság 68

Az, hogy Dél-Korea a Huawei-t használja az 5G-hálózatához,²⁸⁵ valamint a KNK-val²⁸⁶ fenntartott kapcsolatai minden bizonnyal vonzó célponttá teszik a KNK számára. Dél-Korea biztonsági és hírszerzési apparátusa nem kelt bizalmat a kémelhárításban²⁸⁷. Úgy tűnik azonban, hogy nincs közzétett angol nyelvű példa arra, hogy a Samsungnak bármilyen korrupciós ügye lenne a KNK-val kapcsolatban. Mindkét esetben úgy tűnik, hogy sem a Samsung, sem az Apple nem versenyez globálisan az 5G infrastruktúrában, és inkább a telefongyártásra összpontosítanak (bár a Samsung kezd a nyílt hálózati tervezésre összpontosítani²⁸⁸).

Nagyobb aggodalomra adnak okot a nyugat által favorizált 5G infrastruktúra élharcosai, a Nokia és az Ericsson. Mindkettő az amerikai ajánlatok és aggodalmak miatt a világ más részeire helyezi át a gyártás egy részét, ami enyhítheti a gyártáson alapuló biztonsági kérdéseket. A korrupció azonban valójában alattomosabb lehet a két vállalat és biztonságuk szempontjából.

Az Ericsson problémái közvetlenebbek és súlyosabbak. 2019-ben az Ericssonról és leányvállalatairól nemrégiben kiderült, hogy közel két évtizeden keresztül átható és nemzetközi korrupciós kultúrával rendelkeztek, többek között a Kínai²⁸⁹ Népköztársaságban. A korrupció magas rangú vezetőket érintett, és eddig több mint 1 milliárd USD bírságot és több mint 50 alkalmazott elbocsátását²⁹⁰ eredményezte.

A Nokia korrupcióval kapcsolatos biztonsági kockázatai ködösebbek, és kevésbé kapcsolódnak közvetlenül magához a Nokiához. A Nokia folyamatos jogi problémákkal²⁹¹ küzd, amelyek a francia Alcatel-Lucent vállalat 2016-os, 5G-orientált²⁹² felvásárlásából erednek. Alcatel (Franciaország) és Lucent (Egyesült Államok).

²⁸⁵ Richard L. Armitage és Victor Cha, "The 66-Year Alliance Between the U.S. and South Korea is in Deep Trouble," Newsletter, CSIS, 2019. november 25., <https://www.csis.org/analysis/66-year-alliance-between-us-and-south-korea-deep-trouble>; Clara Gillispie, "South Korea's 5G Ambitions," Academic Paper Series, Korea Economic Institute of America, 2020. március 23., http://keia.org/sites/default/files/publications/kei_aps_gillispie_200316.pdf.

²⁸⁶ Uri Friedman, "Hogyan válasszunk az USA és Kína között? It's Not That Easy," Politics, *The Atlantic*, július 26., 2019, <https://www.theatlantic.com/politics/archive/2019/07/south-korea-china-united-states-dilemma/594850/>.

²⁸⁷ "Risks of Intelligence Pathologies in South Korea", Asia, Report 259, International Crisis Group, augusztus 5., 2014, <https://www.crisisgroup.org/asia/north-east-asia/korean-peninsula/risks-intelligence-pathologies-south-korea>.

²⁸⁸ "5G Vision," Networks, Samsung, Hozzáférés 2020. április 21., <https://www.samsung.com/global/business/networks/insights/5g-vision/>.

²⁸⁹ "Ericsson 1 milliárd dollárra bírságotlák a széles körű korrupció miatt", News, *Deutsche Welle*, december 7, 2019, <https://p.dw.com/p/3UMt3>.

²⁹⁰ Helena Soderpalm és Olof Swahnberg, "Ericsson Has Dismissed 50 Employees Following U.S. Corruption Probe," Business News, *Reuters*, 2018. október 18., <https://www.reuters.com/article/us-ericsson-probe/ericsson-has-dismissed-50-employees-following-u-s-corruption-probe-idUSKCN1MS1R4>.

²⁹¹ Ray Le Maistre, "Nokia Unearths AlcaLu Compliance Timebomb", Business/Employment, *Light Reading*, 2019. március 22., <https://www.lightreading.com/business-employment/nokia-unearths-alcalu-compliance-timebomb/d/d/d-id/750356>.

²⁹² Morris, Iain. "A Nokia 5G chipválasztása kiteszi magát." 5G. *Light Reading*, 2019. október 28. <https://www.lightreading.com/5g/nokias-5g-chip-choice-leaves-it-exposed/d/d-id/755184>.

2006-ban egyesültek, és mindegyiküknek megvoltak a maga korrupciós²⁹³ problémái.

Az egyesüléskor az Alcatel több mint egy évtizedes globális korrupciós gyakorlattal²⁹⁴ rendelkezett, a Lucent pedig több évet töltött kínai tisztviselők megvesztegetésével. Mindkét vállalatnak az egyesülés előtt és után is voltak szerződésai a Kínai Népköztársaságban. Az Alcatel-Lucent a Nokia felvásárlása előtt és után is licenclte az Alcatel és a BlackBerry termékek gyártását a kínai TCL távközlési vállalatnak.

2018-ban világossá vált, hogy a TCL által készített különböző alkalmazások rosszindulatú szoftvereket tartalmaznak. Ezek közé tartoztak az előre feltöltött alkalmazások a TCL termékek széles skáláján, beleértve az Alcatel és BlackBerry készülékeket is. A rosszindulatú szoftverek más rosszindulatú és gyanús viselkedés²⁹⁵ mellett felhasználói adatokat gyűjtöttek és küldtek a KNK-nak.

Nem világos, hogy a Nokia milyen enyhítő lépéseket tett az Alcatel-Lucent vagy a TCL tekintetében. Tekintettel azonban arra, hogy az Alcatel-Lucent 5G chipjei központi szerepet játszanak a Nokia hálózati üzleti tervében (ami valójában visszavetette azt)²⁹⁶, indokoltnak tűnik a nagyobb kockázatértékelés. Aztán ott van a Nokia két másik kapcsolata.

2006-ban a Nokia és a Siemens közös vállalatot alapított távközlési hálózatok és szolgáltatások kiépítésére, amely felett a Nokia végül 2011-ben²⁹⁷ teljes irányítást szerzett. Mégis, 2006-ban a Siemens ellen is korrupcióval vádolták meg. A Siemens korrupciós botránya nem kis ügy volt. Azt mutatta, hogy az 1990-es évek elejére a korrupció globális rendszere a vállalaton és leányvállalatain²⁹⁸ belül normává vált. A korrupció egy része a KNK-t is érintette. Aggasztóan úgy tűnik, hogy ezek a korrupciós gyakorlatok 2006 után is folytatódtak, különösen a KNK-ban,

²⁹³ "Lucent elismeri a vesztegetést", News Wire Feed, *Light Reading*, december 21, 2007, <https://www.lightreading.com/lucent-admits-to-bribery/d/d-id/650564>;

"Former Alcatel Exec Sentenced," News Wire Feed, *Light Reading*, szeptember 24, 2008, <https://www.lightreading.com/former-alcatel-exec-sentenced/d/d-id/661544>.

²⁹⁴ Naim, Moises. "A korrupciós kitörés." *The Brown Journal of World Affairs* 2, no. 2 (Spring/Summer 1995): 245-261. <http://bjwa.brown.edu/2-2/the-currupction-eruption/>; Richard L. Cassin, "Alcatel-Lucent Settles Bribery Case," *The FCPA Blog*, December 28, 2010, <https://fcpublog.com/2010/12/28/alcatel-lucent-settles-bribery-case/>.

²⁹⁵ Catalin Cimpanu, "Malware Found Preinstalled on Some Alcatel Smartphones," *ZDNet*, 2019. január 10., <https://www.zdnet.com/article/malware-found-preinstalled-on-some-alcatel-smartphones/>; Octavio Mares, "The Most Dangerous & Spying Television Award Goes to TCL," *Information Security Newspaper*, 2020. február 4., <https://www.securitynewspaper.com/2020/02/04/the-most-dangerous-spying-television-award-goes-to-tcl/>.

²⁹⁶ Morris, "Nokia's 5G"; Iain Morris, "Nokia Hires 350 R&D Experts to Fix 5G Problems," *5G, Light Reading*, 2019. október 30., <https://www.lightreading.com/5g/nokia-hires-350-randd-experts-to-fix-5g-problems/d/d-id/755257>.

²⁹⁷ Stephen Lawson, "Nokia Closes Acquisition, Renames Nokia Siemens Networks," *News-IT Leadership, ComputerWorld*, 2013. augusztus 7., <https://www.computerworld.com/article/2484790/nokia-closes-acquisition--renames-nokia-siemens-networks.html>.

²⁹⁸ Bertrand Venard, "Lessons From the Massive Siemens Corruption Scandal One Decade Later", *Economy + Business, The Conversation*, 2018. december 13., <https://theconversation.com/lessons-from-the-massive-siemens-corruption-scandal-one-decade-later-108694>.

a legfrissebb jelentésekkel 2016²⁹⁹.

Érdemes megjegyezni, hogy a Siemens most a Qualcomm chipgyártóval dolgozik együtt az 5G hálózatok fejlesztésén. 2016-ban a Qualcomm egyezséget írt alá, hogy elkerülje az Egyesült Államok által a Kínában elkövetett korrupciós vádak, beleértve a "kínai tisztviselők rokonainak alkalmazását, akik befolyásolhatták mobiltechnológiai termékeinek kiválasztását a versenypiacon"³⁰⁰. 2018-ban az EU megbírságolta a Qualcommot, amiért jogellenesen fizetett az Apple-nek azért, hogy használja a termékeit³⁰¹. Ezután 2019-ben az USA és az EU egymástól függetlenül bűnösnek találta a Qualcommot a trösztellenes törvények megsértésében, így a szakértők kételkednek abban, hogy a büntetések elrettentik a Qualcommot a versenyellenes és korrumpáló gyakorlatok³⁰² folytatásától.

Végezetül a Nokia tekintetében még egy utolsó eseményt érdemes megemlíteni. Úgy tűnik, hogy egy szoftverhiba miatt egyes Nokia telefonok adatokat továbbítottak a China Telecommunications Corporation³⁰³ tulajdonában lévő szerverekre. A telefonok hardverét és adattároló proxyit a Nokia leányvállalata, a HMD Global Oy készítette, amely viszont a telefonjait a résztulajdonos Foxconn gyártja, és a Qualcommtól³⁰⁴ származó alkatrészeket tartalmaznak. A HMD és a Nokia azt állítja, hogy nem osztottak meg személyes adatokat, de ezt³⁰⁵ okkal lehet kétségbe vonni. Azóta, látszólag egymástól függetlenül, a Nokia bejelentette, hogy HMD termékei Szingapúr³⁰⁶ helyett Finnországban tárolják majd a felhasználói adatokat.

Annak ellenére, hogy a Huawei-hez képest a termékek minősége és biztonsága magasabb szintű, mind az Ericsson, mind a Nokia története riadalmat kell, hogy keltsen. Szinte nem lehet tudni, hogy a szereplők, köztük a Kínai Népköztársaság, a megvesztegetés, a zsarolás vagy a hardver és a szoftver közvetlen manipulálása révén veszélyeztették-e, vagy - ami még valószínűbb - milyen mértékben veszélyeztették-e a biztonságukat. A

²⁹⁹ Scilla Alecci, "German Media Reveals How Chinese Bribes for Siemens Products Flowed", Blog, International Consortium of Investigative Journalists, 2018. október 1., <https://www.icij.org/blog/2018/10/german-media-reveals-how-chinese-bribes-for-siemens-products-flowed/>.

³⁰⁰ John Ribeiro, "U.S. Slaps Qualcomm With Multi-Million Dollar Fine Over China Corruption Allegations," News-Legal, *PCWorld*, 2016. március 2., <https://www.pcworld.com/article/3040157/qualcomm-fined-in-the-us-over-china-corruption-allegations.html>.

³⁰¹ David Meyer, "Qualcomm Just Got Fined \$1.23 Billion for Illegal Payments to Apple," Tech-Antitrust, *Fortune*, január 24, 2018, <https://fortune.com/2018/01/24/qualcomm-apple-intel-antitrust-baseband-eu/>.

³⁰² Reed Albergotti, Hamza Shaban, and Taylor Telford, "Qualcomm Violated Antitrust Law, Judge Rules," Technology, *The Washington Post*, május 22, 2019, <https://www.washingtonpost.com/technology/2019/05/22/qualcomm-violated-antitrust-law-judge-rules/>; Associated Press, "EU Fines Chipmaker Qualcomm for 'Predatory Pricing'," Business News, *U.S. News & World Report*, 2019. július 18., <https://www.usnews.com/news/business/articles/2019-07-18/eu-fines-chipmaker-qualcomm-for-predatory-pricing>.

³⁰³ Wei Shi, "Nokia-Branded Phones Sent Personal Data from Norway to China," News, *Telecoms.com*, március 22., 2019, <https://telecoms.com/496471/nokia-branded-phones-sent-personal-data-from-norway-to-china/>.

³⁰⁴ Ralph Jennings, "Apple Contractor Foxconn Makes Gains With Its Own Brand of Phones in a Tough Market," Asia, *Forbes*, 2019. január 31., <https://www.forbes.com/sites/ralphjennings/2019/01/31/apple-contractor-foxconn-makes-gains-with-its-own-brand-of-phones-in-a-tough-market/#1ef048012c48>; Shi, "Nokia-Branded"; "Data Collection Technical Details FAQs," Phones, Nokia, https://www.nokia.com/phones/en_int/data-collection-tech-részletek.

³⁰⁵ Shi, "Nokia-Branded".

³⁰⁶ Wei Shi, "HMD Moves Nokia Phone User Data Storage to Finland," News, *Telecoms.com*, 2019. június

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 71**

19., <https://telecoms.com/498007/hmd-moves-nokia-phone-user-data-storage-to-finland/>.

az 5G szerződések és partnerségek bővülése a KNK-ban úgy tűnik, hogy növeli ezeket a kockázatokat³⁰⁷. A Nokia és az Ericsson elszármított³⁰⁸, látszólag nem vizsgált elfogadása vagy akár államosítása biztonsági szempontból kontraproduktív³⁰⁹nek tűnik, nem beszélve ideológiai vagy gazdasági szempontból.³¹⁰

Az ellátási lánc kockázatai mindig jelen lesznek, és a korrupció mindig problémát fog jelenteni, még a megbízható bennfentesek³¹¹ esetében is. A Huawei egyik vezető globális biztonsági és adatvédelmi tisztviselője kijelentette, hogy a megvesztegetés egyszerűbb és hatékonyabb lenne, mint egy hátsó³¹² ajtó kiépítése vagy használata. Bár a megvesztegetés és a zsarolás hosszú távon nem a leghatékonyabb eszközök egy bennfentes ellenőrzésére³¹³, a kibbiztonság veszélyeztetése csak egy pillanatnyi kihagyást igényel. Úgy tűnik, hogy e kérdések egyike sem kap megfelelő figyelmet, különösen akkor, ha feltételezhetően baráti vagy kompetens szereplőkről van szó.

Úgy tűnik azonban, hogy két másik, kapcsolódó, de sokkal átütőbb tényező kevesebb figyelmet kap, amikor az 5G és a hálózati biztonságról van szó. Az első az, hogy a szolgáltatótól függetlenül már most is szinte lehetetlen biztonságos 5G hálózatokat létrehozni. A második az úgynevezett társadalmi réteg. Egy nemzetközivé tett HCSEC, és különösen az ICSEC létrehozása erősebb, proaktívabb megközelítéseket hozhatna létre és koordinálhatna az ilyen kockázatokkal szemben.

Kormányok, vállalatok és jogok

Dr. Schneier kriptográfus és a Harvard Kennedy School munkatársa elismeri a Huawei és a KNK által jelentett kockázatokat és fenyegetéseket, de úgy véli, hogy "a nyugati világtól távol kell tartani őket".

³⁰⁷ Bevin Fletcher, "Ericsson, Nokia ink 5G Deals with Chinese Operators - Report," 5G, *Fierce Wireless*, november 8, 2019, <https://www.fiercewireless.com/5g/ericsson-nokia-ink-5g-deals-chinese-operators-report>.

³⁰⁸ Nick Statt, "US Pushing Tech and Telecom Industries to Build 5G Alternative to Huawei," Policy, *The Verge*, 2020. február 5., <https://www.theverge.com/2020/2/5/21124888/us-5g-huawei-white-house-trump-china-alternative-telecom-standard>.

³⁰⁹ William Barr, "William Barr igazságügyi miniszter főelőadása: China Initiative Conference," Transcript, CSIS, 2020. február 6., <https://www.csis.org/analysis/attorney-general-william-barrs-keynote-address-china-initiative-conference>.

³¹⁰ Josh Horwitz, "The Trump Team's Idea to Counter China with Nationalized 5G is Just What China Would Do", *Quartz*, 2018. január 29., <https://qz.com/1191154/the-trump-teams-idea-to-counter-china-with-nationalized-5g-is-just-what-china-would-do/>; Eric Boehm, "Corporate Socialism? Bill Barr javaslatára, hogy az USA-nak meg kellene vásárolnia a Nokiat vagy az Ericssont Kína ellenében, borzalmas ötlet", *Internet, Reason*, 2020. február, <https://reason.com/2020/02/12/corporate-socialism-bill-barr-suggests-the-u-s-should-counter-china-by-buying-nokia-or-ericsson/>.³¹¹

Mike Giglio, "China's Spies Are on the Offensive", *Politics, The Atlantic*, 2019. augusztus 26., <https://www.theatlantic.com/politics/archive/2019/08/inside-us-china-espionage-war/595747/>.

³¹² Eileen Yu, "Huawei: Könnyebb megvesztegetni a távközlési cégek munkatársait, mint hátsó ajtókat építeni", *Blog-By the Way, ZDNet*, október 23, 2019, <https://www.zdnet.com/article/huawei-easier-to-bribe-telco-staff-then-build-backdoors/>.

³¹³ Randy Burkett, "Az ügynöktoborzás alternatív kerete: From MICE to RASCALS," *Studies in Intelligence*

FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 73

57, no. 1 (Extracts, March 2013): 7-17, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-57-no.-1-a/vol.-57-no.-1-a-pdfs/Burkett-MICE%20to%20RASCALS.pdf>.

infrastruktúra nem elegendő az 5G biztosításához³¹⁴. Ennek oka, hogy "a bizonytalanságok a piaci erőknek köszönhetőek, amelyek a költségeket a biztonsággal szemben előnyben részesítik, valamint a kormányoknak, köztük az Egyesült Államoknak, amelyek meg akarják őrizni a felügyelet lehetőségét az 5G hálózatokban"³¹⁵. Az olyan kormányok, mint az Egyesült Királyság, az Egyesült Államok és mások által kért vagy akár kötelezővé³¹⁶ tett hátsó ajtók a kibertér és az 5G sokkal kevésbé biztonságos³¹⁷ (lásd még). Nem is beszélve az emberi jogi kérdésekről³¹⁸ és a "tekintélyelvű visszalépés" veszélyeiről, amelyeket az³¹⁹ ilyen döntések jelentenek, vagy arról, hogy hogyan néznek ki a Huawei és a KNK³²⁰ elleni érvek összefüggésében.

Dr. Schneier továbbá azt állítja, hogy az 5G biztonsági javulásai ellenére a 4G-hez képest három fő probléma van. Először is, a hardver és a szoftver tervezése és kölcsönhatása miatt a komplexitás miatt a biztonsági szabványok még nehezebben megvalósíthatók. Másodszor, a 4G-vel és más hálózatokkal való kiterjedt és elkerülhetetlen visszafelé kompatibilitás miatt "az 5G hálózatok számos meglévő problémát örökölnek"³²¹, amelyek leküzdése³²² több mint egy évtizedet vesz igénybe. Harmadszor, az 5G szabványügyi bizottságok számos biztonsági funkciót opcionálissá tettek, és a vállalatok "a fejlesztést, a teljesítményt, a költségeket és a piacra kerülési időt ... a biztonsággal szemben, amelyet utólagos szempontként kezeltek"³²³.

A kormányok már régóta képesek behatolni a hálózatokba, "anélkül, hogy bármilyen ellenőrzésük lenne a hardver, a szoftver vagy az eszközöket gyártó vállalatok felett", és,

³¹⁴ Bruce Schneier, "China isn't the Only Problem With 5G," Argument, *Foreign Policy*, 2020. január 10., <https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/>.

³¹⁵ Ibid.

³¹⁶ Jacob Kastrenakes, "US, UK, and Other Governments Asks Companies to Build Backdoors into Encrypted Devices," Cybersecurity, *The Verge*, 2018. szeptember 3., <https://www.theverge.com/2018/9/3/17815196/five-eyes-encryption-backdoors-us-uk-australia-nz-canada>.

³¹⁷ Harold Ableson, Ross Anderson, Steven M. Bellovin, Joshn Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter és Daniel J. Weitzner, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity* 1, no. 1 (September 2015): 69- 79. <https://doi.org/10.1093/cybsec/tyv009>; Riana Pfefferkorn, "Security Risks of Government Hacking," The Center for Internet and Society, Stanford Law School, September 2018, https://cyberlaw.stanford.edu/files/publication/files./2018.09.04_Security_Risks_of_Government_Hacking_Whitepaper.pdf; Schneier, "China Problem".

³¹⁸ Ryan Goodman, "International Proscriptions on Mass Surveillance (or What's Missing in the Greenwald vs. Wittes Debate)", *Just Security*, 2014. március 24., <https://www.justsecurity.org/8448/international-proscriptions-mass-surveillance-or-whats-missing-greenwald-vs-wittes-debate/>.

³¹⁹ Jessica Chen Weiss, "Understanding and Rolling Back Digital Authoritarianism", Commentary, *War on the Rocks*, 2020. február 17., <https://warontherocks.com/2020/02/understanding-and-rolling-back-digital-authoritarianism/>.

³²⁰ Jennifer Stisa Garnick, "Huawei Hacking is a Security Scandal," *Just Security*, 2014. március 24., <https://www.justsecurity.org/8488/huawei-hacking-security-scandal/>.

³²¹ Schneier, "Kína-probléma".

³²² Lily Hay Newman, "5G is More Secure than 4G and 3G-Except When it's Not," Security, *WIRED*, december 15, 2019, <https://www.wired.com/story/5g-more-secure-4g-except-when-not/>.

³²³ Schneier, "Kína-probléma".

"az 5G-ben semmi sem akadályozza meg, hogy ezek a tevékenységek a jövőben is folytatódjanak, sőt növekedjenek"³²⁴. Dr. Schneier szerint azon a korlátozott előnyökön kívül, amelyeket a meglévő és a készülő hálózatok biztonságos rétegekkel való kiegészítése jelent, nem sok mindent lehet tenni. Mint már említettük, a nyílt hálózatok egyike lehet a kevés ilyen megoldásnak³²⁵.

Ezek a hozzáadott biztonsági rétegek azonban csak annyira jók, amennyire a tervezésük, amelyeknek megvannak a maguk szabványokat és szabályozást³²⁶ igénylő problémái, amelyek közül sok a meglévő kormányzati és vállalati szabványok, szabályozási folyamatok és ösztönzők³²⁷ körül forog. Még a nyílt hálózatok szószólója, Dr. Wheeler is elismeri, hogy a Huawei-hardverek távol tartása nem fogja biztosítani az 5G-t, és a szűken erre való összpontosítás eltereli a figyelmet a valódi problémákról és megoldásokról³²⁸. Továbbá, mint túl gyakran, a tervezés csak akkor hatékony, ha megfelelően figyelembe veszi az emberi tényezőt.

A társadalmi réteg

Az emberi alapú hírszerzés továbbra is létfontosságú eleme a kémelhárításnak, és ezt a technológiai képességek³²⁹ csak fokozzák. Az emberi tényező, a kibertér³³⁰ úgynevezett "társadalmi rétegének" formájában a kiberbiztonság egyetlen olyan rétege, amelyet gyakorlatilag mindenki elhanyagol, pedig vitathatatlanul ez a legsebezhetőbb³³¹. A társadalmi réteg különösen akkor jelenthet problémát, ha az ellátási láncokról, a korrupcióról vagy a kiberbiztonság másik két, szélesebb körben összpontosított és támaszkodott rétegének, a "fizikai rétegnek" és a "logikai rétegnek" a megkerülésének számos módjáról van szó³³².

A társadalmi réteg az egyénekhez és szervezetekhez (legyen az személyes, tudományos, kereskedelmi vagy kormányzati) kapcsolódó valós és digitális információkat foglalja magában. Ez a

³²⁴ Ibid.

³²⁵ Wheeler, "Titkos szósz".

³²⁶ David Simpson, "FCC fehér könyv: Cybersecurity Risk Reduction," Report, Public Safety & Homeland Security Bureau-Federal Communications Commission, January 18, 2017, <https://www.fcc.gov/document/fcc-white-paper-cybersecurity-risk-reduction>; Vinod K. Aggarwal and Andrew W. Reddie, "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis," *Journal of Cyber Policy* 3, no. 3 (2018): 291-305, <https://doi.org/10.1080/23738871.2018.1553989>; Paul Maxwell és Robert Barnsby, "Insecure at any Bit Rate: Why Ralph Nader is the True OG of the Software Design Industry," *Journal of Cyber Security* 4, no. 3 (2019): 346-361, <https://doi.org/10.1080/23738871.2019.1671471>; Dunn-Cavelty és Wenger, "Cyber Security Politics".

³²⁷ "Special Issue", *Journal of Cyber Policy*; Wheeler és Simpson, "5G Requires".

³²⁸ Tom Wheeler és Robert D. Williams, "Keeping Huawei Hardware Out of the U.S. Is Not Enough to Secure 5G," *Lawfare*, 2019. február 20., <https://www.lawfareblog.com/keeping-huawei-hardware-out-us-not-enough-secure-5g>; Wheeler és Simpson, "5G Requires".

³²⁹ David V. Gioe, "Minél több dolog változik": *The Palgrave Handbook of Security, Risk and Intelligence*, szerkesztette Robert Dover, Huw Dylan és Michael Goodman, 213-227, London: Palgrave Macmillan, 2017.

³³⁰ "The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028," TRADOC Pamphlet 525-7-8, Department of the Army, február, 8-9. o.22,2010.,, <https://fas.org/irp/doddir/army/pam525-7-8.pdf>.

³³¹ David V. Gioe, Michael S. Goodman és Alicia Wanless, "Rebalancing Cybersecurity Imperatives: Patching the Social Layer," *Journal of Cyber Policy* 4, no. 1 (2019): 117-137, <https://doi.org/10.1080/23738871.2019.1604780>.

³³² "US Army's Cyberspace", Department of Army, 8-9. o.

a "személyiség" és a "kiber-személyiség" alkategóriákra bontva³³³. A személyiség az a személy, aki jogosult hozzáféréssel rendelkezik egy hálózaton. A kiber-személyiség "magában foglalja a személy azonosítását vagy személyiségét a hálózaton (e-mail cím, számítógép IP-címe, mobiltelefonszám és mások)"³³⁴. Továbbá "egy személynek több cyber-személyiséggel is rendelkezhet (például különböző számítógépeken különböző e-mailekkel), és egy cyber-személyiségnek több felhasználója is lehet (például több felhasználó férhet hozzá egyetlen eBay®-fiókhoz)"³³⁵.

A könnyű információmegosztás és -gyűjtés korában a társadalmi rétegből származó adatok széles skáláját könnyűvé vált összegyűjteni és hasznosítani. A társadalmi réteg felhasználható a jobban összpontosított és biztonságosabb fizikai és logikai rétegek kompromittálására, vagy a célzott egyének és csoportok manipulálására a (kiber)személyiségek manipulálásával vagy eltérítésével. Ez történhet széles körű vagy célzott propaganda- és adathalászkampanyok révén.

A társadalmi réteget sok szempontból nehezebb kezelni a számos, nehezebben ellenőrizhető, nagyon is emberi változó miatt. A társadalmi réteg elhanyagolása azonban nem lehetséges, és minden holisztikus kiberbiztonsági kezdeményezésnek kulcsfontosságú eleme kell, hogy legyen. Valójában "az emberi elme ténylegesen kritikus infrastruktúra", és "a kiberbiztonságban a szociális vagy kognitív réteg mennyire mélyen sebezhető", sokkal több figyelmet³³⁶ igényel.

ESETLEG BŐVÍTENI A GIOE ÉS A KÖVETKEZŐ KORMÁNYZATI CIKKET AZ ÁTLÁTHATÓSÁGRÓL + AZ ADATOK SZÜKSÉGESSÉGÉRŐL

³³³ Ibid.

³³⁴ Ibid.

³³⁵ Ibid.

³³⁶ Gioe et al., "Rebalancing", p. 122.

Innovatív megoldások

A nyílt hálózattervezés³³⁷ mellett számos innovatív kiberbiztonsági megoldás létezik vagy van fejlesztés alatt. Az alábbiakban hét olyan megközelítést mutatunk be, amelyekkel a politikai döntéshozók, a szervezeti vezetők, a műszaki szakemberek és a tudósok körében egyaránt érdemes lenne jobban megismertetni. A (kiber)biztonság fokozásának ezeket a proaktív, tematikusan összefüggő módszereit a kiberbiztonság és a fent említett kockázatok minden rétegére alkalmazni lehet és kell. A kiberbiztonsági politikának is részét képezhetik és kellene képezniük szélesebb értelemben.

Az első a "zéró bizalom" tervezése³³⁸, az "eredményalapú" kiberbiztonsági tervek³³⁹, a vörös sejtek³⁴⁰ (más néven vörös csapatok³⁴¹), a komplexitás/rendszeralapú megközelítések, mint például az anticipatív hírszerzés³⁴², a kiberbiztonsági szakpolitikai szakemberek sokszínűségének növelése és az akciókutatás³⁴³. E módszerek továbbfejlesztése, integrálása és alkalmazása a kiberbiztonságra és a biztonsági kockázatokra szélesebb körben is nagy szükség van. Ebben az Egyesült Királyság és egy esetleges ICSEC is segíthetne.

Egy konkrét példa jól érzékelteti az általunk vizsgált innovatív megoldások fontosságát. 2017-ben a Wikileaks megszerezte és nyilvánosságra hozta az amerikai hírszerző ügynökségek titkos hackereszközeinek és dokumentumainak 180 GB-os anyagát, amelyet Vault 7 kiszivárogtatásként³⁴⁴ ismerünk. A Vault 7 kiszivárogtatások a jelek szerint a CIA akkori rendszergazdájától, Joshua Schulte-tól származnak. A büntetőeljárás során kiderült, hogy "az összes eszközt tartalmazó virtuális gép jelszavaként nyilvánvalóan a "123ABCdef" jelszót használta"³⁴⁵. A helyzetet tovább súlyosbította, hogy "a közös admin jelszavaktól kezdve a cserélhető tárolókra vonatkozó korlátozások nélkülözése, az ügynökség gyakorlatilag minden létező szabályt megszegett, vagy megszegett"³⁴⁶. Úgy tűnik, hogy az ilyen problémák széles körben elterjedtek az amerikai hírszerzésben, és három évvel később úgy tűnik, hogy kevés dolog változott³⁴⁷.

³³⁷ Wheeler, "Titkos szósz".

³³⁸ Medin et al., "5G Ecosystem"; Stuart H., "Zero Trust Architecture Design Principles: Alpha Release for the ZTA Principles on GitHub," Blog Post, NCSC, november 20, 2019, <https://www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles>.

³³⁹ John Cosby, "The Most Resilient Organizations Follow Outcome Based Cybersecurity", Opinion, *Fifth Domain*, 2020. március 30., <https://www.fifthdomain.com/opinion/2020/03/31/the-most-resilient-organizations-follow-outcome-based-cybersecurity/>.

³⁴⁰ Eric C. Anderson, "Global Agenda 2012 - Red Cell," Global Agenda 2012 Speaker Series-Spies, Lies, & Sneaky Guys: Espionage & Intelligence in the Digital Age, University of Delaware, szeptember 11., videó2012., 1h:22m:36s, <https://www.youtube.com/watch?v=BAzBtVcNldY&t=1s>.

³⁴¹ Micah Zenko, *Vörös csapat: New York: How to Succeed by Thinking Like the Enemy: How to Succeed by Thinking Like the Enemy*: Basic Books, 2015.

³⁴² Josh Kerbel, "Coming to Terms With Anticipatory Intelligence," Commentary, *War on the Rocks*, augusztus 13, 2019, <https://warontherocks.com/2019/08/coming-to-terms-with-anticipatory-intelligence/>.

³⁴³ David Coghlan és Mary Brydon-Miller (szerkesztők), *The SAGE Encyclopedia of Action Research, Vol I & II*, London: SAGE Publications, Ltd., 2014.

³⁴⁴ Shaun Nichols, "Ha kétségbeesik a személyzet admin jelszavak megosztásán, nézze a jó oldalát. That's CIA-

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 78**

Grad Security," Security, *The Register*, 2020. június 16.,
https://www.theregister.com/2020/06/16/cia_report_vault_7_leak/.

³⁴⁵ Ibid.

³⁴⁶ Ibid.

³⁴⁷ Ibid.

Zéró bizalom

A DIB 2019. évi jelentése ³⁴⁸hivatkozik a "zéró bizalom" hálózatok tervezési elveire, és az Egyesült Királyság NCSC weboldalán található cikk is ezt ³⁴⁹vázolja. Figyelemre méltó, hogy az amerikai Cyber Solarium jelentésben³⁵⁰ a zéró bizalomról nem esik szó. Ez a hálózat-tervezés viszonylag új és fejlődő megközelítése, amely kulcsfontosságú az eddig tárgyalt kockázatok szinte mindegyikének kezelésében. A zéró bizalom megközelítése megszünteti a hálózatban rejlő bizalmat.

Ez azt jelenti, hogy a hálózathoz és annak összetevőihöz való hozzáférés erősen korlátozott és elkülönített, a tervezési elvek és a jól megtervezett és végrehajtott biztonsági politika alapján. Gyakran előfordul, hogy ha mégis betörés történik, a behatoló "oldalirányban mozoghat, mert a hálózaton minden megbízható", de "egy zéró bizalmi architektúrában a hálózatot ellenségesnek tekintik"³⁵¹.

A "bizalom eltávolítása a hálózatból" megköveteli, hogy "a felhasználók és a szolgáltatások hitelesítésébe, ellenőrzésébe és engedélyezésébe vetett bizalmat"³⁵². Ehhez a bizalmat "a felhasználó személyazonosságába (felhasználói hitelesítés), eszközeibe (eszköz-hitelesítés) és az általa igénybe vett szolgáltatásokba (szolgáltatásengedélyezés) kell beépíteni"³⁵³.

E modell hatékonysága megköveteli, hogy "minden egyes szolgáltatáshoz való kapcsolódást hitelesíteni kell, és az eszközt és a kapcsolatot egy házirend alapján engedélyezni kell, függetlenül attól, hogy a kapcsolódási kérelem honnan érkezik"³⁵⁴. Az engedélyezési döntések lehetővé tétele érdekében pedig "hozzáférési irányelveket kell meghatározni, amelyek alapján meg lehet határozni, hogy ki milyen szolgáltatáshoz vagy adathoz milyen körülmények között férhet hozzá"³⁵⁵. Konkrétan "az, hogy mennyire kell megbízni egy kapcsolatban, a hozzáférési adatok értékétől vagy az elvégzendő művelet hatásától függ"³⁵⁶.

Hasonlóképpen, "az eszközöket leltározni kell, és az eszközellenőrzésnek meghatározott irányelveken (például titkosítás, javítási szintek stb.) kell alapulnia"³⁵⁷. Ez csak egy rövid vázlata annak, hogy mit jelent a zéró bizalom. Az NCSC forrása jelentősen részletezi a zéró bizalom szükségességét és végrehajtását, a DIB-jelentés pedig hangsúlyozza a "kvantumrezisztens kulcs-csere-mechanismusok"³⁵⁸ szükségességét a KNK kvantumszámítógépes beruházásai miatt. Reméljük, hogy az együttműködés a közmondásos tó túloldalán már folyamatban van.

³⁴⁸ Medin et al, "5G Ecosystem", p. 29.

³⁴⁹ Stuart H., "Zéró bizalom".

³⁵⁰ U.S. Cyber Space Solarium Bizottság, "Jelentés".

³⁵¹ Ibid.

³⁵² Ibid.

³⁵³ Ibid.

³⁵⁴ Ibid.

³⁵⁵ Ibid.

³⁵⁶ Ibid.

³⁵⁷ Ibid.

³⁵⁸ Medin et al., "5G Ecosystem", p. 29.

Eredményalapú biztonság

Az eredményalapú kiberbiztonság "holisztikusabb"³⁵⁹ és proaktívabb filozófia, amely a kiberbiztonság meglévő megközelítéseire épül. Ez megköveteli "a szervezetek állapotának és kockázati környezetének folyamatos értékelését"³⁶⁰. Ezt úgy teszi, hogy "a szervezet kibervédelmének és vállalkozásának értékét és érvényességét aktív elemzés alapján a szervezet teljes kockázati profiljához viszonyítja"³⁶¹.

Mivel az egyes szervezetek állapota és környezete eltérő, az egyes szervezetek felelőssége, hogy megértsék, megtervezzék és folyamatosan újraértékeljék igényeiket. Mindezt az alapvető kiberbiztonsági követelményeken felül kell megtenni. A kiberbiztonság mind az alapvetőbb, mind pedig a kimeneti alapú módszereit tartalmazza a Védelmi Minisztérium 2020. március 18-i kiadványa, a Kiberbiztonsági Érettségi Modell tanúsítása, mint követelményeket azok számára, akik a Védelmi³⁶² Minisztériummal kívánnak üzletet kötni.

Van azonban egy kikötés. Bár az eredményalapú biztonság és a meglévő szabványok erős megközelítések, Frank Kendall volt amerikai védelmi miniszterhelyettes szerint az a tanúsítási rendszer, amelyben ezek a rendszerek működnek, több szinten is önpusztító, és inkább bonyolítja, mint kezeli a kiberbiztonsági ellátási lánc alapvető kérdéseit. Összefoglalva, igen hatásosan érvel amellett, hogy a tanúsítási rendszer nem ösztönzi az integritást, a hatékonyságot és ezáltal a hatékonyságot³⁶³. A politikai döntéshozóknak, akik az eredményalapú biztonság megvalósítására keresnek modellt, tanácsos figyelembe venniük a tanúsítási rendszer hibáit.

Vörösvértetek/csapatok

Minden biztonsági megközelítés kulcsa, és kifejezetten az eredményalapú kiberbiztonság kulcseleme a vörös sejtek³⁶⁴, vagy közismertebb nevükön a vörös csapatok³⁶⁵ alkalmazása. Ezek a kifejezések arra utalnak, hogy megbízható szakértőket alkalmaznak, akik potenciális fenyegetésekként gondolkodnak és cselekszenek, hogy azonosítsák és kezeljék a gyenge pontokat. Ezt a módszert az Egyesült Királyságban és az Egyesült Államokban már alkalmazzák különböző minőségben.

A használatuknál is fontosabb azonban, hogy az ilyen csoportok ajánlásait és más, a biztonság fokozására összpontosító csoportok megállapításait ténylegesen végrehajtsák,

³⁵⁹ Cosby, "Legkitartóbb".

³⁶⁰ Ibid.

³⁶¹ Ibid.

³⁶² "CMMC Model," Cybersecurity Maturity Model Certification, Office of the Undersecretary of Defense for Acquisition & Sustainment, Accessed March 30, 2020, <https://www.acq.osd.mil/cmmc/draft.html>; Cosby, "Most Resilient".

³⁶³ Frank Kendall, "Kiberbiztonsági érettségi modell tanúsítása: An Idea Whose Time Has Not Come and Never May," *Business, Forbes*, április 29, 2020, <https://www.forbes.com/sites/frankkendall/2020/04/29/cyber-security-maturity-model-certification-idea-whose-time-has-not-come-and-never-may/#35ea66773bf2>.

³⁶⁴ Anderson, "Vörös sejtek".

³⁶⁵ Zenko, *Vörös csapat*.

ami mind az Egyesült³⁶⁶ Királyságnak, mind az Egyesült³⁶⁷ Államoknak aggasztó eredményei vannak. Ez még inkább létfontosságú, ha nem alkalmaznak teljes tilalmat, mint az Egyesült Királyságban. Ideális esetben bármely szervezet, amely az 5G vagy általában a kibertér biztonságának fokozásával van megbízva, teljes mértékben kihasználja ezt a módszert.

Előre látó intelligencia

Végezetül, a 2019-es amerikai nemzeti hírszerzési stratégiában³⁶⁸ felvázolt komplexitási és rendszerszintű paradigmák, mint például az anticipatív hírszerzés, felhasználása és alkalmazása a kiberbiztonságra döntő fontosságú. Az anticipatív hírszerzés célja, hogy "elképzelje vagy elképzelhetővé tegye a lehetőségeket, mielőtt azok felmerülnének"³⁶⁹. Dr. Kerbel, a Nemzeti Hírszerző Egyetem oktatója tisztázza a fogalmat. A következőképpen határozza meg: "az a hírszerzési folyamat vagy gyakorlat, amelynek során az egyre összetettebb biztonsági környezetből eredő, potenciálisan felmerülő fejleményeket holisztikus perspektívák kialakításával előre látjuk"³⁷⁰.

A hidegháború volt a jelenlegi biztonsági és hírszerzési paradigmák meghatározó tapasztalata. A hidegháború kétpólusú jellege lehetővé tette a szereplők számára, hogy figyelmen kívül hagyják a valóság és a nemzetközi környezet összetett jellegét, és viszonylag stabil, vagy legalábbis látszólagos fenyegetésekre összpontosítsanak. Ugyanakkor "a hidegháború utáni biztonsági környezetet jellemző, kiugró globális komplexitás (összekapcsolhatóság és kölcsönös függőség, mind virtuális, mind fizikai), amely hajlamos a kialakuló (nem additív vagy nem lineáris) jelenségek létrehozására, alapvetően új"³⁷¹.

A kiberbiztonság és tágabb értelemben a biztonsági kihívások összefüggésében ez azt jelenti, hogy a rendszer- és komplexitástudományokat teljes mértékben alkalmazni kell. Az amerikai kibertér-szoláriumbizottság vezető kutatási igazgatójaként és vezető szerzőjeként Dr. Jensen a bizottság jelentésének közzététele után kijelentette, hogy nem elég csupán a komplex rendszerek kockázatait és hibáit kutatni, mivel azok a kibertérre vonatkoznak. Az összetett kockázatokra kell összpontosítani.

³⁶⁶ Lewis, "Egyesült Királyság".

³⁶⁷ Mark Pomerleau, "The Pentagon is Handling Cyber Vulnerabilities Inconsistently," DoD, *Fifth Domain*, 2020. március 17., <https://www.fifthdomain.com/dod/2020/03/17/the-pentagon-is-handling-cyber-vulnerabilities-inconsistently/>; Mariam Baksh, "Stop Hiding Vulnerabilities Found by Red Teams, Joint Staff to Tell Military," Tech, *Defense One*, 2020. március 18., <https://www.defenseone.com/threats/2020/03/stop-hiding-vulnerabilities-found-red-teams-joint-staff-tells-military/163868/?oref=d1-related-article>; Mariam Baksh, "Pentagon Isn't Following the Cyber Steps it Asks from Suppliers, GAO Says," Tech, *Defense One*, április 15, 2020, <https://www.defenseone.com/technology/2020/04/pentagon-lacks-cyber-hygiene-it-will-demand-suppliers-gao-says/164638/?oref=d-nextpost>.

³⁶⁸ "Az Amerikai Egyesült Államok nemzeti hírszerzési stratégiája 2019". A Nemzeti Hírszerzés Igazgatójának Hivatala. 2019, 7., 9., 32. o.

https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf?utm_source=Press%20Release&utm_medium=Email&utm_campaign=NIS_2019.

³⁶⁹ Kerbel, "Előrelátó intelligencia".

³⁷⁰ Ibid.

³⁷¹ Ibid.

rendszer szintű kockázatok³⁷². Ahogy Dr. Wheeler és a társszerző, Simpson nyugalmazott ellentengernagy állítja, az 5G-n belül ez azt jelenti, hogy meg kell érteni, hogy a köz- és magánszféra ökoszisztémájának leggyengébb kiberbiztonsági láncszemei hogyan veszélyeztetik³⁷³ a többi.

Dr. Jensen számára ez azt jelenti, hogy megvizsgálja, hogy az olyan emberi biztonsági kihívások, mint a világjárványok, a gazdaság, a politikai instabilitás, az éghajlatváltozás, a migráció, a kibertér, és így tovább, hogyan hatnak egymásra, és hogyan hoznak létre új jelenségeket³⁷⁴. Megjegyzi, hogy bár a jelentés kitér a komplex rendszerek vizsgálatának szükségességére, a jelentésből hiányoznak a kritikus ajánlások.

Konkrétan, a világnak szüksége van "új kutatási kezdeményezésekre, amelyek a rendszerkockázatot értékelik", beleértve valami olyasmit, mint "egy Kiberstatisztikai Hivatal"³⁷⁵. Példaként³⁷⁷ említi a Center for Systemic Peace³⁷⁶ politikai instabilitással foglalkozó munkacsoportját.

Összefoglalva, a transzdiszciplináris munka nagyobb mértékű adaptációja a rendszer- és komplexitási paradigmákkal felbecsülhetetlen értékű lenne a kimenetel-alapú kiberbiztonság, a vörös csapatok és az előretételező hírszerzés, és ezen keresztül a béke és a jólét szempontjából. Összességében az Egyesült Királyságnak - talán a HCSEC/ICSEC révén - bőséges lehetősége van arra, hogy stratégiai partnerei és a világ élére álljon az 5G és a kiberbiztonság területén. A kiberbiztonsággal kapcsolatos eddigi proaktív megközelítése, a kialakulóban lévő kiberbiztonsági erőfeszítések integrálására és koordinálására vonatkozó lehetőségei, valamint nemzetközi tekintélye alapján alkalmasnak tűnik arra, hogy felvegye a kesztyűt az évszázad 21st komplexitásával szemben.

Komplex rendszerek paradigmái

Mint a legtöbb tudományos kifejezés és téma esetében, a komplexitás és a rendszertudomány definíciói és kapcsolatai is jelentősen eltérhetnek attól függően, hogy melyik tudományág, terület vagy szerző írja le őket. Egyesek szerint a komplexitás átfogja és meghaladja a rendszereket, mások szerint fordítva, és vannak, akik úgy vélik, hogy a kettő egyenrangú. Egyesek még csak a komplex rendszertudományra hivatkoznak. E nézőpontok egyike sem helyes vagy helytelen.

Inkább a paraméterek és következményeik változatossága az erősség, amely hozzájárul a személyre szabott eszközökhöz és célokhoz, valamint a tágabb értelemben vett diskurzushoz és gyakorlathoz. Azok számára, akik kevésbé ismerik a komplexitást és a rendszertudományokat, illetve ezek (gyakran elmosódó) megkülönböztetését és felhasználását, ez a függelék áttekint néhány komplex rendszerforrást. Az általános forrásokkal kezdjük, majd

³⁷² Benjamin Jensen, "Amikor a rendszerek meghibásodnak: Commentary, *War on the Rocks*, 2020. április 9., <https://warontherocks.com/2020/04/when-systems-fail-what-pandemics-and-cyberspace-tell-us-about-the-future-of-national-security/>.

³⁷³ Wheeler és Simpson, "5G igényli".

³⁷⁴ Jensen, "When Systems".

³⁷⁵ Ibid.

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 83**

³⁷⁶ "INSCR Data Page," Center for Systemic Peace, Hozzáférés április
h9,2020,<http://www.systemicpeace.org/inscrdata.html>.

³⁷⁷ Jack A. Goldstone, Robert H. Bates, David L. Epstein, Ted Robert Gurr, Michael B. Lustik, Monty G. Marshall,
Jay Ulfelder és Mark Woodward, "A Global Model for Forecasting Political Instability," *American Journal of
Political Science* 54, no. 1 (2010): 190-208, www.jstor.org/stable/20647979.

a komplex rendszerek irodalmának a nemzetközi kapcsolatokkal és biztonsággal, a KNK-val és a kiberbiztonsággal való kapcsolódási pontjai felé mozdul el. Végül az akciókutatás érdemeire bólintunk.

Általános erőforrások

Castellini létrehozott egy interaktív térképet a komplexitás (és a rendszerek) tudományáról az idők³⁷⁸ folyamán. Ez egy nagyon könnyen hozzáférhető metaperspektívát tesz lehetővé, és az alján egy útmutató segít az értelmezésben és a használatban. Míg Castellini a komplexitást ernyőfogalomként használja, Hieronymi cikke hasonló kísérletet tesz a különböző komplex rendszerparadigmák vizualizálására, miközben a rendszereket ernyő- és egyenrangú fogalomként használja, részletezve néhány vitát³⁷⁹.

A Santa Fe Institute Complexity Explorer honlapja rendszeresen frissül, és sokféle forrást kínál, többek között kurzusokat, tudományos szövegeket, virtuális laboratóriumot, szójegyzéket, a komplexitással és a rendszertudományokkal foglalkozó szervezeteket és még sok más. A mondat végén található lábjegyzet a komplexitásba való ingyenes bevezető tanfolyamukhoz vezet, és használható a következőkhöz

navigáljon máshová³⁸⁰. Hasonlóképpen, a Complexity Explained weboldal is kiváló oktatási eszközöket és hivatkozásokat³⁸¹ kínál. Az oldal és a hozzá tartozó ingyenes húszoldalas füzet³⁸² a komplex rendszerekkel foglalkozó szakértők, gyakorlati szakemberek és diákok világméretű együttműködésének és felmérésének eredménye.

Nemzetközi kapcsolatok és biztonság

A komplex rendszerek, a nemzetközi kapcsolatok és a biztonság elméleti és gyakorlati metszéspontján több forrás is említésre méltó. Janzwood és Piereder az Oxford Bibliographies nemzetközi kapcsolatok alszekciójának, a "Complex Systems Approaches to Global Politics" (Komplex rendszerek megközelítései a globális politikában) műveit gondozzák³⁸³. Lewis, Mackin és Darken keretrendszere kiemelkedik a kritikus infrastruktúrák és a kapcsolódó kockázatmegelőzési és -reagálási intézkedések elemzésével, mint komplex kialakulóban lévő

³⁷⁸ Brian Castellani, "Map of the Complexity Sciences", Art & Science Factory, 2018, https://www.art-sciencefactory.com/complexity-map_feb09.html.

³⁷⁹ Andreas Hieronymi, "A rendszertudomány megértése: *Systems Research and Behavioral Science* 30, no. 5 (2013): 580-595, <https://doi.org/10.1002/sres.2215>.

³⁸⁰ Melanie Mitchell és Santiago Guisasola. "Introduction to Complexity," Courses, Complexity Explorer, Santa Fe Institute, Hozzáférés: 2020. február 23., <https://www.complexityexplorer.org/courses/104-introduction-to-complexity>. ³⁸¹ Manlio De Domenico és Hiroki Sayama, (koordinátorok), Complexity Explained, Hozzáférés: 2020. május 1., <https://complexityexplained.github.io/>.

³⁸² Manlio De Domenico, Dirk Brockmann, Chico Camargo, Carlos Gershenson, Daniel Goldsmith, Sabine Jeschonnek, Lorren Kay, Stefano Nichele, Jose R. Nicolas, Thomas Schmickl, Massimo Stella, Josh Brandoff, Angel Jose Martinez Salinas és Hiroki Sayama. *A komplexitás magyarázata*. Creative Commons, DOI2019. 10.17605/OSF.IO/TQGNW.

³⁸³ Scott Janzwood és Jinelle Piereder, "Complex Systems Approaches to Global Politics", International Relations. Oxford Bibliographies, Oxford University Press, 2020. február 26., Hozzáférés 2020. április 28., <https://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292->

FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 85

[0278.xml?q=cyber#firstMatch.](#)

rendszer³⁸⁴. Az eredmény egy árnyaltabb, holisztikusabb és koherensebb megközelítés a váratlan események előrejelzésére, az azokra való felkészülésre és az azokra való reagálásra. Choucri és Clark könyve tűnik az egyetlen olyan műnek, amely integrálja a komplex rendszereket, a nemzetközi kapcsolatok elméletét és a kibertérrel³⁸⁵ kapcsolatos kérdéseket.

A komplexitás, a biztonság és a nemzetközi kapcsolatok metszéspontján számos további ingyenes kiadványról van tudomásunk. A Védelmi Minisztériummal kapcsolatban Alberts és Czerwinski 1997-es könyve tűnik a legkorábbi összeállításnak, amely a témák³⁸⁶ metszéspontjával kapcsolatos szakmai és tudományos szempontokat foglalja össze. Szintén a Védelmi Minisztériumhoz kapcsolódik Moffat technikai és katonai jellegű³⁸⁷ könyve. A béke- és konfliktustanulmányokkal összefüggésben Hendrick 2009-es munkadokumentuma³⁸⁸, valamint Leoroux-Martin és O'Connor 2017-es jelentése interdiszciplináris áttekintést³⁸⁹ nyújt a komplex rendszerek jelentéséről és alkalmazásairól.

A KNK

A KNK és a komplexitás tekintetében két figyelemre méltó munka van. Dr. Kerbel 2004-es cikke hasznos, mert leírja az amerikai-KNK kognitív előítéleteit, amelyek az emberi és hidegháborús egyszerűség iránti vágyon alapulnak, és azt, hogy a komplexitástudomány hogyan segíthet az elemzés és a cselekvés javításában ezen a területen³⁹⁰. Garlick elemzése a Kínai Népköztársaság felemelkedéséről a komplexitás, a neorealizmus, az offenzív realizmus és a konstruktivizmus nemzetközi kapcsolatokra vonatkozó elméletein keresztül szépen³⁹¹ kiegészíti Kerbel munkáját.

Kiberbiztonság

A szakirodalmi áttekintésünk során több figyelemre méltó, komplex rendszerekkel és kiberbiztonsággal foglalkozó művet találtunk. A legkorábbi általunk azonosított publikáció Armstrong, Mayo és Siebenlist "Complexity Science Challenges in Cybersecurity" 2009-című jelentése az USA számára.

³⁸⁴ Ted G. Lewis, Thomas J. Mackin és Rudy Darken. "A kritikus infrastruktúra mint komplexen kialakuló rendszer". *International Journal of Cyber Warfare and Terrorism* 1, no. 1 (2011): 1-12. DOI: 10.4018/ijcwt.20110101010101.

³⁸⁵ Nazli Choucri és David D. Clark, *International Relations in the Cyber Age: The Co-Evolution Dilemma*, Cambridge, MA, US: MIT Press, 2019.

³⁸⁶ David S. Alberts és Thomas J. Czerwinski, *Complexity, Global Politics, and National Security*, Washington D.C.: National Defense University Press, 1997, http://www.dodccrp.org/files/Alberts_Complexity_Global.pdf.

³⁸⁷ James Moffat, *Complexity Theory and Network Centric Warfare*, Information Age Transformation Series, Washington, D.C.: CCRP Publication Series, h2003, http://www.dodccrp.org/files/Moffat_Complexity.pdf.

³⁸⁸ Diana Hendrick, "Komplexitáselmélet és konfliktusátalakítás: An Exploration of Potential and Implications," Working Paper 17, Centre for Conflict Resolution-Department of Peace Studies, University of Bradford, 2009. június,

https://www.beyondintractability.org/bi_affiliated_projects/dsap/publications/complexity-theory-transformation-hendrick.pdf.

³⁸⁹ Philippe Leroux-Martin és Vivienne O'Connor, "Systems Thinking for Peacebuilding and Rule of Law: Jelentés, Peaceworks, United States Institute of Peace, október

h23,2017, <https://www.usip.org/publications/2017/10/systems-thinking-peacebuilding-and-rule-law>. ³⁹⁰ Kerbel, "Egyenes gondolkodás".

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 87**

³⁹¹ Jeremy Garlick, "Nem olyan egyszerű: *China Report* 52, no. 4 (2016): 284-305,
<https://doi.org/10.1177/0009445516661884>.

kormány³⁹². Rámutat a komplexitástudomány kiberbiztonságra való alkalmazásának szükségességére, különösen a kritikus kiberinfrastruktúrák esetében, jelezve, hogy akkoriban ez egy viszonylag új és nem alkalmazott megközelítés volt a kiberbiztonságban. Ezzel összefüggésben megállapítják, hogy a komplexitástudomány kulcsfontosságú a reaktív és proaktív védelmi formák javításához, és kutatási irányokat tárnak fel.

Dr. Tisdale kiberbiztonsági 2015 irányítási keretrendszerét³⁹³ és az arról³⁹⁴ szóló későbbi tanulmányt is érdemes megfontolni. A keretrendszer a tudásmenedzsment, a komplexitás, a rendszerek és az üzleti intelligencia integrálásával és alkalmazásával a szervezetek kiberbiztonsági igényeire figyelemre méltó. Mint ilyen, a keretrendszer az eredményalapú biztonságra és a megelőző intelligenciára szabottak tűnik.

Brantly 2019-es, a kiberpolitikára és a komplexitáselméletre vonatkozó cikke meglehetősen egyedinek³⁹⁵ tűnik. Azt állítja, hogy a kibertérre vonatkozó törvények és politikák károsan leegyszerűsítőek, két kriptográfiai esetpélda segítségével demonstrálja ezt. Ezeket az eseteket arra is használják, hogy amellet érveljenek, hogy a hatékony kiberpolitika kialakítása a komplexitáselmélet szélesebb körű felkarolását igényli.

Sokszínűség

Az 5G-vitában és tágabb értelemben a kiberbiztonsági diskurzusokban a többszereplősséget hangsúlyozták, miközben szó szerint a sokféleség hiányától is szenvedtek. Dr. Dunn-Cavelty és Dr. Wegner megfogalmazása és elemzése a kiberbiztonsági politikáról leírja a szakmai sokszínűség és koordináció szükségességét az azt alkotó technológiai, politikai és tudományos szférák szereplői és érdekeltjei között³⁹⁶. Bizonyos mértékig foglalkoznak a szervezeti és nemzeti kultúrákkal, de más szempontból nem tárgyalják a sokféleséget. S

Ahhoz, hogy a kiberbiztonság hatékony legyen, és ezáltal a vállalatok, a nemzetek és az 5G gazdasági és biztonsági érdekei is optimálisak legyenek, a kiberbiztonsági politikan belül és a kiberbiztonsági politika szféráiban minden szinten elő kell mozdítani a sokszínűséget. A sokszínűségre való törekvést folyamatos kritikának és javításnak³⁹⁷ kell alávetni. A kutatásban és a gyakorlatban a magán- és közintézményeken belül figyelmet kell fordítani a nemre, a fajra, a kultúrára, a nemzetiségre, a szexualitásra, a társadalmi-gazdasági

³⁹² Robert C. Armstrong, Jackson R. Mayo és Frank Siebenlist, "Complexity Science Challenges in Cybersecurity", Sandia Report-SAND2009-2007, Sandia National Laboratories, 2009. március, <https://wiki.cac.washington.edu/download/attachments/7478403/Complexity+Science+Challenges+in+Cybersecurity.pdf>.

³⁹³ Susan M. Tisdale, "Kiberbiztonság: *Issues in Information Systems* 16, no. 3 (2015): 191-198, https://iacis.org/iis/2015/3_iis_2015_191-198.pdf.

³⁹⁴ Susan M. Tisdale, "Architecting a Cybersecurity Management Framework", *Issues in Information Systems* no17, 4 (2016): 227-236, https://iacis.org/iis/2016/4_iis_2016_227-236.pdf.

³⁹⁵ Aaron F. Brantly, "Conceptualizing Cyber Policy Through Complexity Theory," *Journal of Cyber Policy* 4, no. 2 (2019): 275-289, <https://doi.org/10.1080/23738871.2019.1583763>.

³⁹⁶ Dunn-Cavelty és Wenger, "Kiberbiztonsági politika".

³⁹⁷ Dunn-Cavelty és Wenger, "Kiberbiztonsági politika".

osztály, oktatás, szakma, életkor, fogyatékoság és egyéb változók. E szakasz alkalmazásában a sokféleséget a következőképpen lehet elképzelni:

- Az egyéneket alkotó vagy az egyéneknek tulajdonítható tényezők.
- Magán- és közsférában tevékenykedő személyek.
- A klasszikus értelemben vett érdekelt feleknek tekintett magán- és közintézmények típusai és jellege.

A különböző közösségek nézőpontjainak, igényeinek és szükségleteinek megértése és képviselése óriási hatással van az oktatás, a kutatás, a fejlesztés, a műveletek, a biztonság és a fogyasztói tapasztalatok hatókörére és hatékonyságára. A sokféleség figyelembevétele nélkül a kiberbiztonságot fenyegető veszélyek fokozódnak, és az enyhítő megközelítések súlyosan aláássák. A nők és a mesterséges intelligencia által a kiberbiztonságra és tágabb értelemben véve a biztonsági kérdésekre gyakorolt hatások vizsgálata ezt jól érzékelteti.

A sokszínűség a kiberbiztonsági politika mindhárom területén hatással van a kutatás és a gyakorlat minőségére. Ez hatással van a kiberbiztonsági politikában érintett valamennyi szereplő felfogására és viselkedésére, akár ember, akár nem. Különösen aggasztó, hogy a biztonság, a kiberbiztonság és a kapcsolódó politikák alakítása és irányítása egyre inkább a mesterséges intelligenciára támaszkodik, tekintettel azokra az előítéletekre, amelyeket a mesterséges intelligencia átvesz az emberektől, és azokra, amelyeket az emberek viszont átvesznek tőle.

Az adatminőség, mint a tervező és az adatok torzításainak függvénye, amely hatással van a megbízhatóságra, pontosságra, etikára, és így a fenyegetés előrejelzésének, felderítésének, elemzésének és enyhítésének tervezésének és funkcionalitásának érvényességére, akár egyénekről, akár szervezetekről van szó, nem is beszélve az általános etikáról....

A sokféleség egyéni és összesített skálája egyaránt fontos. Azonban, ahogyan a többszereplőség története megmutatta, meglehetősen nehéz lehet elérni, hogy könnyebben és gyorsabban előnyös lehet a szervezeteken és érdekcsoportokon belül az egyének, különösen a kiberbiztonsági szakértők diverzifikációjára összpontosítani, szemben a kollektív egységek szükséges, de nehezebb koordinációjával³⁹⁸.

Mégis, az olyan dokumentumokban, mint az amerikai Cyber Solarium Report, a több érdekelt fél kifejezés kizárólag magán- és állami szervezetekre utal, nemzeteken³⁹⁹ belül és nemzetek között.

Egyéni statisztikák a nőkre és más forrásokra (Microsoft stb.).

A nők jelentős előnyöket kínálnak a kiberbiztonsági szakma számára, de nem csak alulreprezentáltak, de jelenlétüket és részvételüket az előítéletek rétegei akadályozzák. Dr. Kshetri menedzsmentprofesszor, aki az "online bűnözéssel és a fogyasztókkal szembenező biztonsági kérdésekkel" foglalkozik,

³⁹⁸ Jeanette Hofmann, "Multi-Stakeholderism in Internet Governance: A fikciót a fikcióba helyezve Gyakorlat", *Journal of Cyber Policy* no1., 1 (2016): 29-49, <https://doi.org/10.1080/23738871.2016.1158303>.

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 90**

³⁹⁹ U.S. Cyber Space Solarium Bizottság, "Jelentés".

szervezetek és nemzetek". Dr. Kshetri "megállapította, hogy az internet biztonságához a technikai megoldásokon túlmenően stratégiákra is szükség van".

Ebben az összefüggésben "a nők képviselete azért fontos, mert a nők általában a férfiakétól eltérő nézőpontokat és nézőpontokat képviselnek, és ezek az alulreprezentált nézőpontok kritikusak a kiberkockázatok kezelésében". A kiberbiztonsági vezetői pozíciókat betöltő nők "hajlamosak olyan fontos területeket előtérbe helyezni, amelyeket a férfiak gyakran figyelmen kívül hagynak". Ez részben az iskolai végzettségüknek tudható be: "az információbiztonsági területeken dolgozó nők negyvennégy százaléka üzleti és társadalomtudományi diplomával rendelkezik, míg a férfiak 30 százaléka".

Ez kihatással van a vállalkozások biztonságára, működésére és eredményességére. A kiberbiztonságban dolgozó nők "nagyobb hangsúlyt fektetnek a belső képzésre és oktatásra a biztonság és a kockázatkezelés terén". Ők "erősebben támogatják az online képzést is, amely rugalmas és alacsony költségű módja annak, hogy az alkalmazottak tudatosságát növeljék a biztonsági kérdésekben".

Talán még ennél is fontosabb, hogy a női kiberbiztonsági szakemberek kívánatos tendenciákat mutatnak "a biztonságos szoftverek fejlesztéséhez partner szervezetek kiválasztásában". Konkrétan, "a nők hajlamosak nagyobb figyelmet fordítani a partnerszervezetek képzettségére és személyzetére, és értékelik a partnerek képességét [sic] a szerződéses kötelezettségek teljesítésére". A nők "olyan partnereket is előnyben részesítenek, amelyek hajlandóak független biztonsági tesztet végezni".

Annak ellenére, hogy a nők a kiberbiztonságban milyen előnyökkel jár, továbbra is alulreprezentáltak, és számos akadállyal kell szembenézniük, amelyek közül néhányat könnyebb gyorsan orvosolni, mint másokat. 2013-ban a nők a globális kiberbiztonsági munkaerő 11 százalékát tették ki, és ez a szám 2019-re 20 százalékra emelkedik. 2017-ben megállapították, hogy globálisan a nők a felsővezetői és vezetői kiberbiztonsági pozícióknak mindössze 1 százalékát teszik ki, a színesbőrű nők pedig még jelentősebb akadályokkal szembesülnek.

A Fortune 500-as vállalatok csak egy kicsivel járnak jobban. A globális vezető informatikusok mindössze 2017, százaléka 13 volt nő. 2019-ben körülbelül "a Fortune 500 globális vezető informatikusainak (CIO-k) 20 százaléka" volt nő.

Ezekben az összefüggésekben az Egyesült Királyságnak szembe kellett néznie bizonyos kihívásokkal, de ígéretesnek is bizonyult. A 2004 és 2017 közötti tanulmányok látszólag következetesen azt találták, hogy a nők az Egyesült Királyságban a kiberbiztonsági munkaerőnek csak mintegy 8 százalékát tették ki. Úgy tűnik, hogy az Egyesült Királyság újabb erőfeszítései meghozták gyümölcsüket, és a kiberbiztonsági ágazat 18 százalékát teszik ki a nők.

Más országok és régiók is kontrasztot adnak. Az Egyesült Államokban 2017-ben a kiberbiztonságban dolgozók mindössze 14 százaléka volt nő, míg az amerikai munkaerő 48 százaléka volt nő.

Az Egyesült Államokon kívül rosszabb a képviselet. A nők 2018, "a kiberbiztonsági

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 92**

**munkaerő százalékát 10-tettki az ázsiai és csendes-óceáni térségben, 9 százalékát
Afrikában, 8 százalékát Latin-Amerikában, 7 százalékát Európában és 5 százalékát a Közel-
Keleten".**

Az Egyesült Királyság egyértelműen jelentős erőfeszítéseket tett a nők számának növelése érdekében a kiberbiztonság területén, de még többet kell tenni.

Az amerikai kiberszolárium-jelentés rávilágít arra, hogy a köz- és a magánszféra számos érdekeltje között együttműködésre van szükség, belföldön és nemzetközi szinten egyaránt. Ez egy lépés a helyes irányba, de van néhány dolog, amit érdemes megjegyezni, különösen mivel a jelentés csupán ajánlásokat tartalmaz. Először is, dicséretes, hogy a jelentés az egyéni sokszínűségre is kitér a legfontosabb ajánlás részeként, amely szerint "jobban kell toborozni, fejleszteni és megtartani a kibertehetségeket... a szövetségi kormányzat kibermunkája számára"⁴⁰⁰.

Külön megemlíti, hogy "meg kell határozni a lehetőségeket és a felvételi lehetőségeket az alulreprezentált közösségek tagjai számára, beleértve a neurodiverzeket, a nőket és a színesbőrűeket"⁴⁰¹. Megjegyzi továbbá, hogy "a mai kiberbiztonsági készségek és tapasztalatok szokatlanul könnyen megszerezhetők a szokásos oktatási és képzési csatornákon kívül", és "a kormánynak hatékonyabban kell kihasználnia ezeket a nem hagyományos utakat"⁴⁰². A fenti idézetek azonban - bár nem elhanyagolhatóak - lényegében az egyedek sokszínűségére vonatkozó egyetlen utalás.

A jelentés továbbá a sokszínűséget pusztán a munkaerő számának növelésére és megtartására irányuló törekvésként fogalmazza meg. Nem említi a sokszínűséget, mint olyasvalamit, amelynek megvannak a maga egyedi érdemei és hatásai a kiberbiztonság minőségére. Továbbá az egyének sokszínűségére vonatkozó felhívás a szövetségi foglalkoztatottakra vonatkozik, nem pedig az állami vagy nemzetközi partnerekre (bár az USA minden állampolgárának nyújtott, a k-karrierre vonatkozó oktatási lehetőségek növelésére vonatkozó felhívás hosszú távon segíthet a belföldieknek).

A legfontosabb, hogy a jelenlegi amerikai politika aláássa ezeket a nemzeti, szervezeti és egyéni célokat, és az Egyesült Királyságnak ezt tudomásul kell vennie. **Nemzeti és szervezeti szinten az USA zéróösszegű megközelítése aláássa kiber-, 5G- és nagyhatalmi stratégiáit, elüldözve a szövetségeseket és potenciális partnereket.** Egyéni szinten, legalábbis kulturális és tudományos szinten, megfosztja magát a nagyon szükséges emberi tőkétől, és figyelmen kívül hagyja vagy aláássa a helyi közönséget és a külföldi érdekeket. A KNK által exportálni kívánt tekintélyelvű modell és az illiberális nemzetek koalíciójának létrehozására irányuló törekvése ellen nem lehet a KNK és az általa udvaroltak⁴⁰³ bírálataival és megbüntetésével fellépni.

A Kínai Népköztársasággal szembeni fellépéshez a liberális értékek és az általuk kínált komparatív előnyök megduplázása szükséges. Ennél is fontosabb, hogy "nagyobb figyelmet kell fordítani a helyi közönség megértésére és a számukra fontos kérdések megvitatására a saját feltételeik szerint... reális és vonzó megoldásokat kell kínálni a más nemzetek előtt álló gyakorlati problémákra"⁴⁰⁴. A gyakorlatban ez a következőket jelenti

⁴⁰⁰ U.S. Cyber Space Solarium Commission, "Report", p. 43.

⁴⁰¹ Ibid.

⁴⁰² Ibid.

⁴⁰³ Daniel Markey, "Responding to China's New Tools of Global Influence", Commentary, *War on the Rocks*, április 1, 2020, <https://warontherocks.com/2020/04/responding-to-chinas-new-tools-of-global-influence/>.

⁴⁰⁴ Ibid.

a humán tőkébe való befektetés itthon és külföldön az oktatás, az egészségügyi ellátás, az utazás, a munkahelyek, a szabad sajtó, a létfontosságú infrastruktúra, az emberi jogok és az igazságszolgáltatás minőségének és hozzáférhetőségének javítása révén. Ez akár azt is jelentheti, hogy "a kínai projektekre építve olyan módon szolgálják a helyi igényeket, miközben demonstrálják... a jó szándékot és a technikai kapacitást"⁴⁰⁵.

Az Egyesült Királyság elkerülheti és el kell kerülnie, hogy szabotálja saját erőforrásait otthon és külföldön, és hogy elvakítsa magát a lehetőségektől, valamint hogy az Egyesült Államok aláássa a több érdekelt fél részvételével zajló partnerségeket... Az Egyesült Királyságnak közös vagyona van + EU + 5 szem, amivel együtt dolgozhat.

Akciókutatás

Az akciókutatás felbecsülhetetlen értékű és rugalmas kutatási és gyakorlati paradigma gyakorlatilag bármilyen kontextusban. Az akciókutatás egy olyan ernyőparadigma, amely bármely tudományág vagy szakma által, és bármely más kutatási paradigmával, módszertannal vagy módszerrel együtt használható. Kiválóan alkalmas arra, hogy a kutatás, a politika és a technológia minden szintjén lehetővé tegye a hatékony és fenntartható innovációt az érdekelt felek integrációjának és a kialakuló, iteratív, több módszert alkalmazó kutatási ciklusoknak⁴⁰⁶ a hangsúlyozása révén.

Az akciókutatási megközelítések alapvetően...ciklus...értékek....other...?

Az akciókutatási megközelítéseket alkalmazni lehet és kell a kiberbiztonságra, az előrettekintő hírszerzésre és tágabb értelemben vett biztonsági kérdésekre. A rendszerszintű akciókutatás különösen hasznos lehet ezekben az összefüggésekben⁴⁰⁷. Történelmileg az akciókutatási paradigmákat leginkább a szervezeti, egészségügyi, fejlesztési, béke/konfliktus, szociális, politikai és oktatási kutatás és gyakorlat összefüggésében használták. Úgy tűnik, hogy a kiberbiztonság és a tágabb értelemben vett biztonság területén kevés munkát végeztek kifejezetten ezzel a módszerrel, így a kutatás és az alkalmazás új irányai számára rengeteg teret hagy. Röviden, az akciókutatás természetéből adódóan egyedülállóan alkalmas arra, hogy integrálja és javítsa az ebben a tanulmányban vagy más módon tárgyalt lehetőségeket, kihívásokat és megoldásokat.

⁴⁰⁵ Ibid.

⁴⁰⁶ Coghlan és Brydon-Miller, *SAGE Action Research*.

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 96**

⁴⁰⁷ Danny Burns, *Rendszeres akciókutatás*: Bristol, Egyesült Királyság: Policy Press, 2007.

Következtetés

Ahogy Dr. Wheeler és Dr. Williams állítja, az a tény, hogy a Huawei és a kínai hardverek távol tartása "nem egyenlő a külföldi kémkedés vagy a hálózatok elleni szabotázs sikeres megakadályozásával"⁴⁰⁸. Inkább a biztonság hamis érzetét kelti. Sőt, ami még rosszabb, "a minimálisan kielégítő 5G kiberkockázati eredmények elérése felé tett hatékony előrelépést veszélyezteti a Huawei-jel kapcsolatos jogos aggodalmakra való túlzott összpontosítás"⁴⁰⁹.

A Nyugatnak és a világnak "kiegyensúlyozottabb kockázatértékelést kellene végeznie, szélesebb körben összpontosítva a sebezhetőségekre, a fenyegetések valószínűségére és a kiberkockázati egyenlet hatásmechanizmusaira"⁴¹⁰. Ezek a lépések felügyeletet igényelnek annak biztosítása érdekében, hogy "az 5G ígéretét ne döntsék meg a kibersebezhetőségek, amelyek az elhamarkodott telepítésekből fakadnak, amelyek nem fektetnek be kellőképpen a kiberkockázatok csökkentésébe"⁴¹¹. Ellenkező esetben "a proaktív kiberbiztonsági lehetőségek elmulasztásának utólagos költségei sokkal nagyobbak lesznek, mint az előzetes kibergondosság költségei"⁴¹².

Aztán ott vannak a tágabb stratégiai, különösen a gazdasági és ideológiai dimenziók, amelyeket figyelembe kell venni. Miután majdnem minden írásunk elkészült, a *BBC News* interjút készített Eric Schmidttel, aki a Google és anyavállalata, az Alphabet korábbi vezérigazgatója és ügyvezető elnöke volt, jelenleg pedig az amerikai védelmi minisztérium védelmi innovációs tanácsának⁴¹³ elnöke. Schmidt elismeri a Huawei és a KNK által jelentett veszélyeket, kijelentve, hogy így vagy úgy, de a Huawei-en keresztül adatok kerültek a KNK kezébe.

Schmidt szerint azonban "a Nyugatnak inkább Kínával és annak technológiáival kellene versenyeznie, mintsem elzárkózni"⁴¹⁴. Véleménye szerint "az igazi probléma a Huawei-jel kapcsolatban az, hogy kihívást jelent az Egyesült Államok vezető szerepére nézve: egy olyan kínai vállalat, amely globális szinten tevékenykedik, és jobb terméket készít, mint a versenytársai"⁴¹⁵. Rendkívül fontos, "hogyan van választási lehetőségünk... a Huawei-re adott válasz... az, hogy egy ugyanolyan jó termékkel és termékcsaláddal versenyezzünk"⁴¹⁶.

Továbbá a KNK gyorsan felzárkózik a nyugati országokhoz, sőt felülmúlja őket innovációs képességeik és technológiai kapacitásuk tekintetében. Ez nagyrészt a célzott állami beruházásoknak köszönhető. Schmidt, "tagadja, hogy az állam által irányított technológiai beruházások kínai modellje önmagában véve sikeresebb lenne, mint a szabadpiaci modell"⁴¹⁷. A Nyugatnak azonban nem szabad figyelmen kívül hagynia vagy aláásnia a kulcsfontosságú stratégiákat és eszközöket.

⁴⁰⁸ Wheeler és Williams, "Keeping Huawei".

⁴⁰⁹ Ibid.

⁴¹⁰ Ibid.

⁴¹¹ Ibid.

⁴¹² Ibid.

⁴¹³ Corera, "Eric Schmidt".

⁴¹⁴ Ibid.

⁴¹⁵ Ibid.

⁴¹⁶ Ibid.

⁴¹⁷ Ibid.

Különösen az Egyesült Államok egyre inkább árt magának a kutatás és az oktatás finanszírozásának csökkentésével, a bevándorlás megakadályozásával, valamint a különböző káros propagandával, amely démonizálja és eltemeti az amerikai kormányzatnak a kutatás és az innováció támogatásában játszott létfontosságú szerepét. Schmidt úr szerint "az Egyesült Államokban és különösen a Szilícium-völgyben az egyik probléma az, hogy a kormányzatnak a kutatás támogatásában betöltött szerepe iránt történelmi vakság uralkodik"; "minden, amit a Szilícium-völgyben látunk, első sorban a kezdeti szövetségi tudományos támogatásokból származik"⁴¹⁸ Schmidt szerint "a Nyugatnak a lehető legtöbbet kell kihoznia erősségeiből: többet kell befektetnie a kutatásfinanszírozásba, nagyobb együttműködést kell biztosítania a magánszektor, az állam és a tudományos élet között, [és] nyitottnak kell maradnia a világ legjobb tehetségei iránt"⁴¹⁹.

Ami ennél is fontosabb, "Schmidt úgy véli, hogy a kínai és az amerikai technológiai szektorok szétválasztása "nem kívánatos", mert úgy véli, hogy ez két különböző rendszerhez vezetne"⁴²⁰. A problémát az jelenti, hogy "ha egyszer szétválasztjuk ezeket a globális platformokat, nem kapjuk vissza őket... előnyünkre válik, ha közös platformunk van a cserére... és aggódom, hogy ha ezeket a platformokat külön építjük, az országok kevésbé fogják megérteni egymást"⁴²¹. Schmidt véleménye szerint "Kína fog dominálni, akár összekapcsolódunk, akár szétválunk"⁴²².

Schmidt számára a kérdés az, hogy "globális platformokon vagy a saját platformjaikon működnek-e"⁴²³. Mivel "a Nyugat érdeke, hogy minden technológiai platformban nyugati értékek legyenek... minél inkább szegregáltak a platformok, annál veszélyesebb"⁴²⁴. Ebben az értelemben "a nacionalizmus és a protekcionizmus erősödése világszerte "nagy aggodalomra ad okot"⁴²⁵.

Schmidt szerint "a legjobb stratégia, ha úgy gondolunk erre, mint egy versenyre, amely nem különbözik a technológiai vállalatoktól, ahol brutális verseny van... [sic] olyan durva lesz, amilyen csak lehet - nagyrészt szabályozatlan a különböző szereplők között -, ahol arra törekszünk, hogy nyerjünk"⁴²⁶. Így "Schmidt óvatos a nemzeti bajnokok kiválasztásával és támogatásával kapcsolatban"⁴²⁷. Hasonlóképpen, bár elismeri, hogy "vannak gyengeségek a Nyugat saját kapacitásában, különösen azáltal, hogy nincsenek félvezető chipeket gyártó öntödék"⁴²⁸, nem hiszi, hogy a közelmúltbeli amerikai lépések, amelyek a Kínába és környékén történő félvezető-értékesítés és -gyártás sávositására irányulnak, előnyösek. **A tilalom valójában csak ártott az USA-nak, miközben felgyorsította a KNK félvezető-függetlenségét.**

Végső soron, akár az 5G-ről, akár a kiberbiztonságról általában, akár arról, hogy hogyan kezeljük a KNK-t,

⁴¹⁸ Carera, "Eric Schmidt".

⁴¹⁹ Ibid.

⁴²⁰ Ibid.

⁴²¹ Ibid.

⁴²² Ibid.

⁴²³ Ibid.

⁴²⁴ Ibid.

⁴²⁵ Ibid.

⁴²⁶ Ibid.

⁴²⁷ Ibid.

⁴²⁸ Ibid.

gyakorlatilag valamennyi nyugati ország és szövetséges egyetért abban, hogy nemzetközi együttműködésre van szükség. Úgy tűnik, hogy a koronavírus világjárvány lecsengése⁴²⁹ után egyre inkább egy nemzetközi technológiai szövetségre van szükség. De hogy ez az együttműködés hogyan néz ki, kiket és hogyan vonnak be, és ki fogja átvenni a vezetést, az jelenleg még a levegőben lóg. Úgy tűnik, hogy az USA és a Kín nem áll készen a vezetésre⁴³⁰. Ebben az összefüggésben a Huawei fenyegetései lehetőségként is átfogalmazhatók, különösen az Egyesült Királyság számára.

Szükséges a HCSEC nemzetközivé tétele vagy egy ezzel egyenértékű szerv létrehozása, amely a proaktív és innovatív megközelítések kialakítására és végrehajtására összpontosít. A reaktív és passzív kiberbiztonsági intézkedésekre, például az elrettentésre való támaszkodás nem hatékony⁴³¹. Még Észak-Koreát sem látszik rettenetesen aggasztani⁴³².

Ami ezt illeti, az amerikai kiberdoktrínák jelenlegi koncepciója szerint az elrettentés vitathatóan kontraproduktív a Kín-val⁴³³ szemben. Hasonlóképpen, a biztonsági intézkedések utólagos telepítése természetesen korlátozza a rendszerarchitektúrában lehetséges biztonság mértékét, mivel az alaprendszerek módosítására vonatkozó, a funkcionalitást⁴³⁴ érintő korlátozások miatt. Röviden, a konfliktusok és különösen a nagyhatalmi verseny összefüggésében az ilyen passzív és reaktív megközelítések "tarthatatlanok - lehetővé teszik az ellenfél számára, hogy alakítsa a verseny szabályait"⁴³⁵. A proaktivitás a saját és a versenytársak⁴³⁶ céljainak és eszközeinek világos és összehangolt megértését igényli.

A HCSEC nemzetközi erőfeszítése és/vagy a kiberbiztonsági szakértelem nagyobb mértékű megosztása jelentősen javítani fogja a hálózatbiztonságot világszerte. A Huawei és más gyártók által jelentett kockázatok azonosítására irányuló erőfeszítések összehangolása lehetővé teszi a jobb biztonsági, enyhítési és vészhelyzeti tervek kidolgozását. Ez természetesen a tipikusabb megközelítéseken felül történne, mint például a szoftverfrissítések azonnali felülvizsgálata a forráskódban, a kárelhárítás és a hálózat korlátozása.

⁴²⁹ Martijn Rasser, "Technology Alliances Will Help Shape Our Post-Pandemic Future", Opinion, *CSISRNET*, 2020. április 14., <https://www.c4isrnet.com/opinion/2020/04/14/technology-alliances-will-help-shape-our-post-pandemic-future/>.

⁴³⁰ Elizabeth C. Economy, "A hidra a fej nélküli lovas ellen: Kína és az Egyesült Államok", Blog-Asia Unbound, Council on Foreign Relations, 2020. április 15., <https://www.cfr.org/blog/hydra-vs-headless-horseman-china-and-united-states>.

⁴³¹ James Andrew Lewis, "Strategy After Deterrence", Commentary, CSIS, március 11, 2020, <https://www.csis.org/analysis/strategy-after-deterrence>; Lewis, "Cyber Solarium".

⁴³² David E. Sanger és Nicole Perlroth, "U.S. Accuses North Korea of Cyberattacks, a Sign that Deterrence is Failing", Asia Pacific, *The New York Times*, 2020. április 15., <https://www.nytimes.com/2020/04/15/world/asia/north-korea-cyber.html>.

⁴³³ Kolton, "China's Cyber Sovereignty", p. 143.

⁴³⁴ "Security-by-Design Framework Version: 1.0," Cyber Security Agency of Singapore, Hozzáférés: 2019. július 20., https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/security_by_design_framework.pdf.

⁴³⁵ Peter Roberts és Sidharth Kaushal, "Competitive Advantage and Rules in Persistent Competitions," Occasional Papers, RUSI, April 29, 2020, <https://www.rusi.org/publication/occasional-papers/competitive-advantage-and-rules-persistent-competitions>.

⁴³⁶ Kolton, "China's Cyber Sovereignty"; Roberts és Kaushal, "Competitive Advantage".

behatolás.

A HCSEC nemzetközivé válása lehetőséget kínál az Egyesült Királyság számára is, hogy a Huawei a biztonsági integráció, a világszintűen a politikai tőke növekedése, a technológiai innováció és a gazdasági fejlődés szempontjából is hasznot húzzon belőle. A Huawei gazdasági integrációja az Egyesült Királyságba és a világ gazdaságba viszont visszatartja a rosszindulatú magatartást. Azzal, hogy beengedjük őket az Egyesült Királyság piacára, a Huawei-nek van vesztenivalója.

A Huawei piaci szerepének a biztonságra és a fenyegetettségre hivatkozva történő elutasítása, legalábbis az eddigi állítások szerint, nem elegendő indok a teljes betiltásról szóló döntés meghozatalához.

A világ legnagyobb 5G-szállítójának elutasítása nem szül sem baráti versenyt, sem jólétet és békét⁴³⁷. Továbbá a Huawei mindent átható globális jelenléte lehetetlenné teszi a kockázatainak kiküszöbölését, ahogyan "az MI5, az Egyesült Királyság belföldi hírszerző szolgálatának főigazgatója" érvelt, miközben "ragaszkodott ahhoz, hogy a Huawei szerepe és az általa okozott kockázatok kezelhetők"⁴³⁸. Az ellenségeskedés és az elutasítás tehát kontraproduktívnak tűnik az Egyesült Királyság és a liberális demokráciák⁴³⁹ globális biztonsági és gazdasági érdekei szempontjából.

A Huawei piacra lépése által kínált lehetőségek közé tartozik a hálózatbiztonság globális javítására irányuló együttműködés, a gazdasági előnyök, és főként a liberális demokráciák közötti és a Kínával való kapcsolatok javításának lehetősége. Azáltal, hogy a piacvezetők, mint a Huawei, az Ericsson és a Nokia magasabb szintű normákhoz kötődnek, a kiberbiztonság javulása az egész 5G iparágban és az 5G-re épülő összes jövőbeli iparágban is éreztetheti hatását. A piacvezetők kiberbiztonság terén történő felelősségre vonása gazdasági és biztonsági szempontból egyaránt pozitívan hat a jövőbeli technológiák és rendszerek számára. Ezért előnyösebb az együttműködésre és a pozitív versenyre való törekvés, mint egyáltalán nem próbálkozni.

Bár általánosságban feltételezhető, hogy a Kínai Népköztársaság globális gazdaságba való integrálódásának kilátása miatt nem kockáztatnák meg, hogy a Huawei politikai célok követésére és rosszindulatú magatartásra használják, továbbra is fennáll annak a lehetősége, hogy a Huawei utasítják a hátsó ajtók telepítésére, ha eddig nem tették volna. Az USA és a Kínai Népköztársaság szétválasztásának kérdéseivel, amelyeket ⁴⁴⁰Trump 2020 májusában azzal fenyegetett, hogy "megszakítja az egész kapcsolatot"⁴⁴¹ a Kínai Népköztársasággal, a gazdasági integráció biztosítóka egyre inkább veszélybe kerül, és a rosszindulatú viselkedés kockázata is felmerül. Ez két kérdést vet fel. Nevezetesen, hogy mit kell tenni, és ki vezessen?

⁴³⁷ Muhammad Faizal Bin Abdul Rahman és Russell Huang, "The Asia-Pacific's Huawei Conundrum," Flashpoints-Security, *The Diplomat*, 2020. március 12., <https://thediplomat.com/2020/03/the-asia-pacifics-huawei-conundrum/>.

⁴³⁸ Glosserman, "Huawei realitások".

⁴³⁹ Kania és Gorman, "United Talent"; Lairson, Skidmore és Xinbo, "US Backfired".

⁴⁴⁰ Ibid.

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 103**

⁴⁴¹ Laura Widener, "Trump Says 'We Could Cut Off Whole Relationship' with China; Among Options," *American Military News*, 2020. május 14., <https://americanmilitarynews.com/2020/05/trump-says-we-could-cut-off-whole-relationship-with-china-among-opciók/>.

Ahogy azt már említettük, Dr. Lewis szerint a legbiztonságosabb megoldás az amerikai megközelítés, amely a Huawei teljes betiltását jelenti, szemben azzal, hogy csak távol tartja őket a kritikus hálózatoktól. Azonban még ő is elismerte, hogy egyes országok különböző okokból nem hisznek abban, hogy a teljes tilalom szükséges vagy az általános érdekükben áll. Ismétlem, a probléma egy része - legalábbis az Egyesült Királyság és feltehetően mások számára - az, hogy a Kínai Népköztársaság már számos eszközt alkalmazott a különböző hálózatokba való sikeres behatoláshoz. Ennél is fontosabb, hogy sokan, köztük az Egyesült Királyság is, arra a következtetésre jutottak, hogy gazdasági és biztonsági érdekeiket egyaránt maximalizálhatják egy jól végrehajtott, a kritikus infrastruktúrák védelmére összpontosító részleges tilalom révén.

Nyilvánvalóan megoszlanak a vélemények, amikor arról van szó, hogy mit kell tenni. Ami még rosszabb, hogy ez a megosztottság a szövetségesek és stratégiai partnerek között ellenségessé vált, és elvonja a figyelmet a konstruktív kompromisszum számos lehetőségétől, amelyekkel mindenki érdekeit maximalizálni lehetne. Ez a szövetségesek közötti szakadás hasonló ahhoz a kettősséghez, amelyet az USA és a Kínai Népköztársaság a világrendre kényszerít. Ezek a szakadások sok tekintetben a vezetés függvényei.

Trump elnök hivatalba lépése előtt az Egyesült Államok részt vett a 3rd Generation Partnership Project (3GPP) keretében a globális 5G szabványok, felügyelet és biztonság kialakítására irányuló nemzetközi köz- és magánszféra közötti erőfeszítésekben. Az Obama-kormányzat az Egyesült Államokon belül és a 3GPP-vel együtt arra összpontosított, hogy összehozza a szakértőket, hogy "azonosítsák a közbiztonsági és kiberbiztonsági kockázati megfontolásokat", és "a fejlesztési és telepítési ciklus részeként megvalósítsák a kiberbiztonsági kockázatok csökkentését."⁴⁴² Azonban, ahogy Dr. Schneier is utal rá, a profit, a politika és a könnyebbség elsőbbséget élveztek a biztonsággal⁴⁴³ szemben.

A lobbisták és a republikánus szövetségi kommunikációs bizottsági tagok megakadályozták ezeket az erőfeszítéseket. 2016-ban a kiberbiztonsági kezdeményezéseket a Trump-kormányzat elvetette, majd kilépett a 3GPP-ből⁴⁴⁴. Az ezt követő években az USA kiberbiztonsági és 5G-politikája belföldön és nemzetközi szinten egyaránt nélkülözötte a koherens stratégiát, a Trump-kormányzat pedig ingadozott a kiberbiztonsági erőfeszítések figyelmen kívül hagyása, megzavarása és felszámolása között. A "felelősség" a Kongresszusra maradt, amely hagyományosan lemondott erről a szerepéről a lobbistáknak⁴⁴⁵.

A Cyberspace Solarium Bizottság⁴⁴⁶ vitathatatlanul az első erőteljes kongresszusi erőfeszítés⁴⁴⁷. A tárgyalatok szerint azonban vannak gyenge⁴⁴⁸ pontjai is. Ezen túlmenően, az ajánlásai

⁴⁴² Wheeler és Simpson, "5G igényli".

⁴⁴³ Wheeler és Simpson, "5G Requires"; Schneier, "China Problem".

⁴⁴⁴ Wheeler és Simpson, "5G igényli".

⁴⁴⁵ Ishan Mehta, "Under Trump, the Fight Against Cybercrime has Waned," Security-Opinion, *WIRED*, 2019.

június 20., <https://www.wired.com/story/under-trump-the-fight-against-cybercrime-has-waned/>; Susan Landau,

"A Security Failure in the White House," *Cyber & Technology, Lawfare*, 2019. november 1.,

<https://www.lawfareblog.com/security-failure-white-house>; Breanne Deppisch, "DHS was Finally Getting Serious

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 105**

About Cybersecurity. Then Came Trump," Magazine Feature, *Politico*, december 18.,
2019, <https://www.politico.com/news/magazine/2019/12/18/america-cybersecurity-homeland-security-trump-nielsen-070149>

⁴⁴⁶ U.S. Cyber Space Solarium Bizottság, "Jelentés".

⁴⁴⁷ Mehta, "Trump alatt".

szinte biztosan lassan és szelektíven fogják törvénybe iktatni és végrehajtani⁴⁴⁹.

Riasztó, hogy a kongresszusnak kényszerítene kellett a Trump-kormányzatot, hogy cselekedjen az 5G biztonságával⁴⁵⁰ kapcsolatban.

Az Egyesült Államok 2020⁴⁵¹. március 23-án törvénybe iktatott Secure 5G and Beyond Act című törvénye arra kötelezi a végrehajtó hatalmat, hogy 180 napon⁴⁵² belül dolgozzon ki nemzeti és nemzetközi stratégiát "az 5G és a vezeték nélküli hálózatok jövőbeli generációi által támasztott problémákra". Az ágazati partnerségek⁴⁵³ megerősítése mellett azt is előírja, hogy a végrehajtó hatalom "segítse a kölcsönös védelmi szerződéses szövetségeket, stratégiai partnereket és más országokat az 5G rendszerek és infrastruktúra biztonságának maximalizálásában"⁴⁵⁴.

Nem sokkal később, március végén a Fehér Ház nyilvánosságra hozott egy nagy vonalakban felvázolt stratégiát⁴⁵⁵. Ez elsősorban a 2019. májusi prágai 5G biztonsági konferencián született "Prágai javaslatokra" hivatkozik⁴⁵⁶, különösen a nemzetközi szabványok és partnerségek tekintetében. A konferencián részt vett az összes ötoldalú partner, az EU-tagok, Japán, Dél-Korea, Izrael és néhány más, elsősorban NATO-tag. A Kínai Népköztársaság nem szerepelt, és bár sem ő, sem a Huawei nem került említésre, a dokumentum céljai részben az ő kockázataik⁴⁵⁷ mérséklésére irányulnak.

A prágai javaslatok a résztvevő nemzetek közötti minden fronton történő együttműködést hangsúlyozzák. Az Egyesült Államok és a Fehér Ház stratégiája is felvázolja az ilyen együttműködés szükségességét, ugyanakkor az USA vezető szerepét hangsúlyozza. A prágai javaslatok közzététele és a Fehér Ház stratégiájának közzététele között történt események fényében érdemes megkérdőjelezni, hogy

⁴⁴⁸ Lewis, "Cyber Solarium".

⁴⁴⁹ Andrew Eversden, "Cyber Policy Suggestions for Pentagon Could be Implemented This Year", Capital Hill, *Fifth Domain*, 2020. április 22., <https://www.fifthdomain.com/congress/capitol-hill/2020/04/22/cyber-policy-suggestions-for-pentagon-could-be-implemented-this-year/>.

⁴⁵⁰ Wheeler és Simpson, "5G igényli".

⁴⁵¹ John Cornyn, "S.893 - Secure 5G and Beyond Act of 2020," 116thCongress Public Law U129., S. Government Publishing Office, 2020. március 23., <https://www.congress.gov/bill/116th-congress/senate-bill/893/text?overview=closed>.

⁴⁵² Andrew Eversden, "Trump Administration Must Produce 5G Security Strategy Under New Law," Critical Infrastructure, *Fifth Domain*, 2020. március 24., <https://www.fifthdomain.com/civilian/2020/03/24/trump-administration-must-produce-5g-security-strategy-under-new-law/>.

⁴⁵³ Andrew Eversden, "Ways Government, Industry Can Overcome a Perpetual Challenge", Industry, *Fifth Domain*, 2020. március 16., <https://www.fifthdomain.com/home/2020/03/16/ways-government-industry-can-overcome-a-perpetual-challenge/>.

⁴⁵⁴ Cornyn, "S.893".

⁴⁵⁵ Donald J. Trump, "Nemzeti stratégia az Amerikai Egyesült Államok 5G biztonságának biztosítására", Fehér Ház. Március 2020, <https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf>.

⁴⁵⁶ "The Prague Proposals," Government of the Czech Republic, 2019. március 5., <https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/>.

⁴⁵⁷ Michael Kahn és Jan Lopatka, "Western Allies Agree 5G Security Guidelines, Warn of Outside Influence," Technology News, *Reuters*, May 3, 2019, <https://www.reuters.com/article/us-telecoms-5g-security/western-allies-agree-5g-security-guidelines-warn-of-outside-influence-idUSKCN1S91D2>.

az USA együttműködésre törekszik, vagy csak kényszerítő, kontraproduktív módszereket alkalmaz.

Az 5G-ért folytatott harc sok szempontból azon múlik, hogy ki befolyásolja a technológiai és jogi normákat⁴⁵⁸. A 3GPP-ből való kilépésével és a Huawei-t célzó, 2019 májusában kezdődő politikájával az USA gyakorlatilag kivonta magát a szabványok meghatározásából és a csatából, amelyet vezetni és megnyerni⁴⁵⁹ szeretne. 2020. május 11-től kezdve hiányzik⁴⁶⁰ a részvétel és az egységes stratégia.

A koronavírus⁴⁶¹, a jelenlegi vezetés és a nemzetközi kapcsolatok helyzete között Európa és mások számára kockázatosnak tűnik, hogy az USA-tól függjön egy ilyen nemzetközi stratégia⁴⁶² kidolgozása és végrehajtása. Továbbá, az eddig tárgyalaton túlmenően, az USA kiberstratégiai megközelítésének néhány dimenziója nem tetszik a szövetségeseknek, és valójában számos lehetőséget kínálhat az ellenfelek számára, amelyeket kihasználhatnak⁴⁶³. Hasonló dinamika játszódik le a nem szövetséges országok között is, amelyek az USA és a KNK érdekeinek egyensúlyáért küzdenek (pl. a Délkelet-ázsiai Nemzetek Szövetségének tagjai)⁴⁶⁴. Valójában, bár Dr. Lewis bizonyos mértékig nem ért egyet, dr. Schneier úgy tűnik, hogy az USA általában elszalasztotta a proaktív globális vezető szerep lehetőségeit az 5G és a kiberbiztonság terén rövid és hosszú távon.

Legalábbis egyelőre a liberális demokráciák gazdasági és biztonsági érdekeinek eszközei és céljai, nem is beszélve más nemzetek érdekeiről, nyilvánvalóan nem teljesen azonosak. A hatékony

⁴⁵⁸ Nicol Turner Lee, "Navigating the U.S.-China 5G Competition," Report, Global China, The Brookings Institution, 2020. április, <https://www.brookings.edu/research/navigating-the-us-china-5g-competition/>; Aaron Klein, Nicol Turner Lee, Carrick Flynn, Frank A. Rose és Sheena Chestnut Greitens, "Panel Conversation: Globális technológiai infrastruktúra", moderátor: Chris Meserole, webinárium: Global China-Assessing China's Technological Reach in the World, The Brookings Institution, 2020. május 8., Transcript and Video, <https://www.brookings.edu/events/webinar-global-china-assessing-chinas-technological-reach-in-the-world/>.

⁴⁵⁹ Lindsay Gorman, "The U.S. Needs to Get in the Standards Game-With Like-Minded Democracies", Cybersecurity and Deterrence, *Lawfare*, 2020. április 2., <https://www.lawfareblog.com/us-needs-get-standards-game-minded-democracies>.

⁴⁶⁰ Hitchens, "Amerikai kockázatok".

⁴⁶¹ Campbell és Doshi, "Coronavirus Order"; George N. Tzogopoulos, "Coronavirus, Security, and the Cyber-Order", Perspectives Papers, Begin-Sadat Center for Strategic Studies, április 21, 2020, <https://besacenter.org/perspectives-papers/coronavirus-security-and-the-cyber-order/>; John Seaman, (szerkesztő), "Covid-19 and Europe China Relations: A Country-Level Analysis," Special Report, European Think-Tank Network on China, French Institute of International Relations, 2020. április 29., <https://merics.org/en/report/covid-19-and-europe-china-relations>. ⁴⁶² Julianne Smith és Garima Mohan, "In a Crisis, a Fumbling America Confirms Europe's Worst Fears", Commentary, *War on the Rocks*, 2020. április 23., <https://warontherocks.com/2020/04/in-a-crisis-a-fumbling-america-confirms-europes-worst-fears/>.

⁴⁶³ Max Smeets, "Cyber Command's Strategy Risks Friction With Allies," Cybersecurity and Deterrence, *Lawfare*, május 28, 2019, <https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies>; Mark Pomerleau, "Two Years in, How Has a New Strategy Changed Cyber Operations?", CyberCon, *Fifth Domain*, november 11, 2019, <https://www.fifthdomain.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations/>.

⁴⁶⁴ Seungha Lee, "Délkelet-ázsiai harc: *The SAIS China Studies Review*, május

**FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 108**

h1,2020,https://saicsr.org/2020/05/01/southeast-asian-struggle-caught-up-in-the-u-s-china-5g-rivalry/.

Mivel az USA vezető szerepe az 5G⁴⁶⁵ és a 6G⁴⁶⁶ terén valószínűtlennek tűnik, Európa pedig egyedülálló helyzetben van a Kínai Népköztársaság és az Egyesült⁴⁶⁷ Államok között, úgy tűnik, hogy az Egyesült Királyságnak lehetősége van a vezetésre. Ha az Egyesült Királyság folytatja az 5G-vel kapcsolatos proaktív munkáját, akkor a Huawei és a KNK jelenlegi fenyegetései enyhíthetők, sőt, akár lehetőségekké is alakíthatók.

A HCSEC és más brit erőfeszítések modellként szolgálhatnak, amelyet tovább lehet bővíteni, és talán egy ICSEC létrehozásához vezethetnek. Az Egyesült Királyságnak megvannak az eszközei és lehetőségei arra, hogy innovatív nemzetközi (kiber)biztonsági erőfeszítések élére álljon. Valójában az Egyesült Államoknál jobb helyzetben lehet ahhoz, hogy a "szövetségi innovációs bázison"⁴⁶⁹ és a "nemzetközi kiberbiztonsági kapacitásépítő közösségen", a "kibertudás közvetítőin" keresztül létrehozza és vezesse a kiberbiztonsági politikát^{468,470}, elkerülve ugyanakkor az ezzel⁴⁷¹ járó lehetséges buktatókat. Az Egyesült Királyság az élen járva maximalizálhatja a saját és partnerei biztonságát és gazdasági eredményeit, miközben sokkal erősebb mechanizmust hozhat létre a Huawei és a Kínai Népköztársaság konstruktív kezelésére⁴⁷².

⁴⁶⁵ Kania, "Miért nem".

⁴⁶⁶ Rasser, "6G beállítás".

⁴⁶⁷ Amy Zhou, "Huawei or the Highway", World, *Harvard Political Review*, 2020. március 5., <https://harvardpolitics.com/world/huawei-or-the-highway/>.

⁴⁶⁸ Dunn-Cavelty és Wenger, "Kiberbiztonsági politika".

⁴⁶⁹ Kliman et al., "Forging Alliance".

⁴⁷⁰ Patryk Pawlak és Panagiota-Nayia Barmaliou, "Politics of Cybersecurity Capacity Building : Conundrum and Opportunity," *Journal of Cyber Policy* no2., 1 (2017): 123, <https://doi.org/10.1080/23738871.2017.1294610>.

⁴⁷¹ Zine Homburger, "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace," *Global Society*, no33., 2 (2019): 224-242, <https://doi.org/10.1080/13600826.2019.1569502>.

⁴⁷² Thomas Renard, "Az EU kiberpartnerségei: A harmadik országokkal a kibertérben folytatott uniós stratégiai partnerségek értékelése". *European Politics and Society* 19, no. 3 (2018).

<https://doi.org/10.1080/23745118.2018.1430720>; "Special Issue", *Journal of Cyber Policy*; Fabrice Pothier és David Fernandez, "China-EU: Living Up to the Ten Actions?", *Rasmussen Global*, május 2020, <https://rasmussenglobal.com/wp-content/uploads/2020/05/EU-China->

FOLYTATANDÓ TERVEZET: 5G és a nemzetközi
biztonság 110

[audit_Rasmussen_Global.pdf](#); Seaman, (szerkesztő), "Covid Europe-China".

Bibliográfia

- "5G Innovációs Központ (5GIC) - Surrey Egyetem." UK Research Partnership Initiative Fund (brit kutatási partnerségi kezdeményezési alap). Hozzáférés: 2020. március 10.
<https://re.ukri.org/funding/our-funds-overview/uk-research-partnership-initiative-fund/case-studies/5g-innovation-centre-5gic-university-of-surrey/>.
- "5G biztonság: ". Politika. Amerikai Külügyminisztérium. November 2019.
<https://policystatic.state.gov/uploads/2019/11/5G-What-is-Trust.pdf>.
- "5G Round-Up: Az Egyesült Királyság kormányának 5G bejelentését követően közzétett NCSC-tartalmak összefoglalása." NCSC. Január 31, 2020.
<https://www.ncsc.gov.uk/information/5g-round-up>.
- "5G Vision." Hálózatok. Samsung. Hozzáférés 2020. április 21.
<https://www.samsung.com/global/business/networks/insights/5g-vision/>.
- 6G Wireless Summit. <http://www.6gsummit.com/>
- "A Huawei tranzakciós kockázati profilja". RWR tanácsadó csoport. 2018. február 13.
<https://www.rwradvisory.com/wp-content/uploads/2019/03/RWR-Huawei-Risk-Report-2-13-18.pdf>.
- Ableson, Harold, Ross Anderson, Steven M. Bellovin, Joshn Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter és Daniel J. Weitzner. "Kulcsok a lábtörő alatt: Mandating Insecurity by Requiring Government Access to All Data and Communications." (Bizonytalanság előírása az összes adathoz és kommunikációhoz való kormányzati hozzáférés megkövetelésével). *Journal of Cybersecurity* 1, no. 1 (September 2015): 69- 79. <https://doi.org/10.1093/cybsec/tyv009>.
<https://doi.org/10.1093/cybsec/tyv009>.
- Abrami, Regina M., William C. Kirby és F. Warren McFarlan. "Miért nem tud Kína innoválni?". Innováció. *Harvard Business Review*, 2014. március.
<https://hbr.org/2014/03/why-china-cant-innovate>.
- Aftergood, Steven. "Védelmi szerződéses csalás: A Persistent Problem." Blogok-Secret News-Dept of Defense. Amerikai Tudósok Szövetsége. May 10, 2019.
<https://fas.org/blogs/secretcy/2019/05/defense-contracting-fraud/>.

Aggarwal, Vinod K. és Andrew W. Reddie. "Összehasonlító iparpolitika és kiberbiztonság: A Framework for Analysis." *Journal of Cyber Policy* 3, no. 3 (2018): 291-305.
<https://doi.org/10.1080/23738871.2018.1553989>.

Albergotti, Reed, Hamza Shaban és Taylor Telford. "A Qualcomm megsértette a trösztellenes törvényt, a bíró szerint". Technológia. *The Washington Post*, 2019. május 22.
<https://www.washingtonpost.com/technology/2019/05/22/qualcomm-violated-antitrust-law-judge-rules/>

Alberts, David S. és Thomas J. Czerwinski. *Komplexitás, globális politika és nemzetbiztonság*. Washington D.C.: National Defense University Press, 1997.
http://www.dodccrp.org/files/Alberts_Complexity_Global.pdf.

Alecci, Scilla. "A német média feltárja, hogyan folytak a kínai kenőpénzek a Siemens-termékekért". Blog. Oknyomozó Újságírók Nemzetközi Konzorciuma. 2018. október 1. <https://www.icij.org/blog/2018/10/german-media-reveals-how-chinese-bribes-for-siemens-products-flowed/>.

Al-Heeti, Abrar. "Elemző szerint a Huawei a világ legjobb 5G telefongyártója". *CNET*, 2020. január 28. <https://www.cnet.com/news/huawei-is-the-worlds-top-5g-phone-vendor-analyst-says/>.

Al-Heeti, Abrar. "Az USA 23 vádiratot nyújtott be a Huawei ellen állítólagos üzleti titoklopás és csalás miatt." *CNET*, 2019. január 29. <https://www.cnet.com/news/us-hammers-huawei-with-23-indictments-for-alleged-trade-secret-theft-fraud/>.

Allison, Graham. "Kína megelőzi Amerikát az AI szupremáciában?". *The National Interest*, 2019. december 22. <https://nationalinterest.org/feature/china-beating-america-ai-supremacy-106861>.

"Amerika nem akarja, hogy Kína uralja az 5G mobilhálózatokat.: Rossz úton jár." Üzleti-5Geopolitika. *The Economist*, 2020. április 8.
<https://www.economist.com/business/2020/04/08/america-does-not-want-china-to-dominate-5g-mobile-networks>.

Anderson, Eric C. *China Restored: A Középső Királyság 2020-ig és azon túl*. Santa Barbara, Kalifornia: Praeger, 2010.

- Anderson, Eric C. "Globális menetrend 2012 - Vörös sejt". Global Agenda 2012 Speaker Series- Spies, Lies, & Sneaky Guys: Espionage & Intelligence in the Digital Age. University of Delaware. 2012. szeptember 11. Videó, 1h:22m:36s.
<https://www.youtube.com/watch?v=BAzBtVcNldY&t=1s>.
- Anderson, Eric C. *Sinophobia: A Huawei története*. CreateSpace Independent Publishing Platform, 2013.
- Araya, Daniel. "A Huawei 5G dominanciája a posztamerikai világban". *Forbes*, 2019. április 5. <https://www.forbes.com/sites/danielaraya/2019/04/05/huaweis-5g-dominance-in-the-post-american-world/#47d130c748f7>.
- Armitage, Richard L. és Victor Cha. "Az Egyesült Államok és Dél-Korea 66 éves szövetsége mély bajban van." Newsletter. CSIS. November 25, 2019.
<https://www.csis.org/analysis/66-year-alliance-between-us-and-south-korea-deep-trouble>.
- Armstrong, Robert C., Jackson R. Mayo és Frank Siebenlist. "Komplexitás-tudományi kihívások a kiberbiztonságban". Sandia Report-SAND2009-2007. Sandia National Laboratories. Március 2009.
<https://wiki.cac.washington.edu/download/attachments/7478403/Complexity+Science+C+challenges+in+Cybersecurity.pdf>.
- Associated Press. "Az EU bírságot szabott ki a Qualcomm chipgyártóra 'ragadozó árképzés' miatt." Business News.
U.S. News & World Report, 2019. július 18.
<https://www.usnews.com/news/business/articles/2019-07-18/eu-fines-chipmaker-qualcomm-for-predatory-pricing>.
- Baksh, Mariam. "Ne rejtegetsek tovább a vörös csapatok által talált sebezhetőségeket, a vezérkar a hadseregnek üzeni." Tech. *Defense One*, 2020. március 18.
<https://www.defenseone.com/threats/2020/03/stop-hiding-vulnerabilities-found-red-teams-joint-staff-tells-military/163868/?oref=d1-related-article>.
- Baksh, Mariam. "A Pentagon nem követi a beszállítóktól kért kiberlépéseket, állítja a GAO." Tech. *Defense One*, 2020. április 15.
<https://www.defenseone.com/technology/2020/04/pentagon-lacks-cyber-hygiene-it-will-demand-suppliers-gao-says/164638/?oref=d-nextpost>.
- Barr, William. "William Barr igazságügyi miniszter főelőadása: China Initiative Conference." Átirat. CSIS. Február <https://www.csis.org/analysis/attorney-6-general-william-barrs-keynote-address-china-initiative-conference2020>..

- Bedford, Tom és Basil Kronfli. "Harmony OS: Amit a Huawei új operációs rendszeréről tudni kell." Hírek. *TechRadar*, 2020. január 17. <https://www.techradar.com/news/harmonyos>.
- Bennett, Cory és Bryan Bender. "Hogyan szerzi meg Kína az amerikai technológia 'koronaékszereit'". Investigation. *Politico*, 2018. május 22. <https://www.politico.com/story/2018/05/22/china-us-tech-companies-cfius-572413>.
- Bery, Akhil és Clarise Brown. "India és Kína digitális válása". Eurasia Live. Eurasia Group. 2020. július 1. Videó. 11m:35s. <https://www.eurasiagroup.net/live-post/india-china-digital-digital-divorce>.
- Bienkov, Adam. "Az Egyesült Királyság feladja szövetségét Trumppal, ahogy az Egyesült Államok 'kivonul a világ vezető szerepéből'". Elemzés. *Business Insider*, 2020. január 12. <https://www.businessinsider.com/uk-abandoning-trump-iran-us-withdraw-leadership-world-qassem-soleiman2020-1>.
- Bin Abdul Rahman, Muhammad Faizal és Russell Huang. "Az ázsiai-csendes-óceáni térség Huawei-kérdése". Flashpoints-Security. *The Diplomat*, 2020. március 12. <https://thediplomat.com/2020/03/the-asia-pacifics-huawei-conundrum/>.
- Birnbaum, Emily. "A képviselőház elfogadta a törvényjavaslatokat, hogy az 5G-ért folytatott versenyben feljebb kerüljön." Policy. *The Hill*, 2020. január 08. <https://thehill.com/policy/technology/477429-house-passes-bills-to-gain-upper-hand-in-race-to-5g>.
- Blackstone, Erwin A., Larry F. Darby és Joseph P. Fuhr Jr. "A duopólium esete: az iparági szerkezet nem elegendő alap a szabályozás bevezetéséhez". *Regulation* (Winter 2011-2012): 12-17. <https://www.cato.org/sites/cato.org/files/serials/files/regulation/2012/6/v34n4-3.pdf>.
- Blanchard, Ben és Perry Michael. "Az innováció hiánya a kínai gazdaság 'Achilles-sarka', Xi szerint." World News. *Reuters*, 2019. május 15. <https://www.reuters.com/article/us-china-politics-xi/lack-of-innovation-is-achilles-heel-for-chinas-economy-xi-says-idUSKCN1SM08G>.
- Boehm, Eric. "Vállalati szocializmus? Bill Barr javaslata, miszerint az USA-nak meg kellene vásárolnia a Nokiát vagy az Ericssont Kína ellenében, borzalmas ötlet." Internet. *Reason*, 2020. február 12. <https://reason.com/2020/02/12/corporate-socialism-bill-barr-suggests-the-u-s-should-counter-china-by-buying-nokia-or-ericsson/>.

- Bohn, Dieter. "A Google állítólag azzal érvel, hogy a Huawei Androidról való leválasztása veszélyezteti az USA biztonságát." *The Verge*, 2019. június 7.
<https://www.theverge.com/2019/6/7/18656163/google-huawei-android-security-ban-allitasok>.
- Bond, David és Jim Pickard. "Az amerikai hírszerzés fenyegetései Nagy-Britanniára 'nem reálisak', mondják a kémek." *Political Espionage. Financial Times*, 2019. május 31.
<https://www.ft.com/content/8cdc7aee-83aa-11e9-b592-5fe435b57a3b>.
- Borghard, Erica D. és Shawn W. Lonergan. "Az 5G-viták figyelmen kívül hagyott katonai vonatkozásai". *Blog-Net Politics. Council on Foreign Relations*. 2019. április 25.
<https://www.cfr.org/blog/overlooked-military-implications-5g-debate>.
- Boulding, William és Markus Christen. "Az első piaci szereplő hátránya." *Financial Management. Harvard Business Review*, 2001. október. <https://hbr.org/2001/10/first-mover-hatranly>.
- Boxall, Andy. "Mi a 6G? Az 5G-t a 2G-hez hasonlíthatja, de még csak a közelében sincs a valóságnak". *Mobile. Digital Trends*, 2020. február 3.
<https://www.digitaltrends.com/mobile/what-is-6g/>.
- Brantly, Aaron F. "A kiberpolitika konceptualizálása a komplexitáselmélet segítségével". *Journal of Cyber Policy* no4., 2 (2019): 275-289.
<https://doi.org/10.1080/23738871.2019.1583763>.
- Brattberg, Erik és Philipple Le Corre. "A Huawei és Európa 5G-konfliktusa". *The National Interest*, 2018. december 27. <https://nationalinterest.org/feature/huawei-and-europe%E2%80%99s-5g-conundrum-39972>.
- Brinza, Andreea. "Hogyan segített Oroszország az Egyesült Államoknak harcolni a Huawei ellen Közép- és Kelet-Európában". *War on the Rocks*, 2020. március 12.
<https://warontherocks.com/2020/03/how-russia-helped-the-united-states-fight-huawei-in-central-and-eastern-europe/>.
- Budden, Phil és Fiona Murray. "Védelmi innovációs jelentés: A MIT innovációs ökoszisztéma és az érdekelt felek megközelítése a védelmi innovációra országonkénti bontásban". *Working Paper. MIT LAB for Innovation Science and Policy*. May 2019.
<https://innovation.mit.edu/assets/Defense-Innovation-Report.pdf>.

- Burkett, Randy. "Az ügynöktoborzás alternatív kerete: A MICE-től a RASCALS-ig." *Studies in Intelligence* 57, no. 1 (Kivonat, 2013. március): 7-17.
<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-57-no.-1-a/vol.-57-no.-1-a-pdfs/Burkett-MICE%20to%20RASCALS.pdf>.
- Burns, Danny. *Rendszeres akciókutatás: A Strategy for Whole System Change*. Bristol, UK: Policy Press, 2007.
- Campbell, Kurt M. és Rush Doshi. "A koronavírus átformálhatja a globális rendet". *Foreign Affairs*, 2020. március 18. <https://www.foreignaffairs.com/articles/china/2020-03-18/coronavirus-could-reshape-global-order>.
- Campbell, Sheila és Chad Shirley. "A szövetségi K+F-kiadások hosszú távú hatásainak becslése: CBO jelenlegi megközelítése és kutatási szükségletei." Blog. Kongresszusi Költségvetési Hivatal. 2018. június 21. <https://www.cbo.gov/publication/54089>.
- Carmichael, Kevin. "Kanada tétovázása az 5G-vel kapcsolatban csak egy a bizonytalanságok közül, amelyek megfojtják a gazdaság életét." Business. *Financial Post*, 2020. február 7. <https://business.financialpost.com/news/economy/canadas-waffling-on-5g-is-just-one-of-the-uncertainties-choking-the-life-out-of-the-economy>.
- Carr, Madeline és Leonie Maria Tanczer. "Az Egyesült Királyság kiberbiztonsági iparpolitikája: An Analysis of Drivers, Market Failures and Interventions (A mozgatórugók, a piac kudarcai és a beavatkozások elemzése)." *Journal of Cyber Policy* 3, no. 3 (2018): 430-444. <https://doi.org/10.1080/23738871.2018.1550523>.
- Cassin, Richard L. "Az Alcatel-Lucent megállapodott a vesztegetési ügyben." *The FCPA Blog*, 2010. december 28. <https://fcpublog.com/2010/12/28/alcatel-lucent-settles-bribery-case/>.
- Castellani, Brian. "A komplexitástudományok térképe." Art & Science Factory. h2018. https://www.art-sciencefactory.com/complexity-map_feb09.html.
- Chaffin, Larry. "A 60 Minutes 15 perc alatt megtorpedózza a Huawei-t: A kiberkémkedés, a Huawei és a kínai [sic] kormány". Putting Realism into Your Network. *Network World*, 2012. október 7. <https://www.networkworld.com/article/2223272/60-minutes-torpedoes-huawei-in-less-than-15-minutes.html>.

- Chan, Tara Francis. "A ZTE kínai technológiai vállalat célja, hogy más országok után kémkedjen, állítja egy versenytársuk új bírósági dokumentumokban". *Business Insider*, 2018. június 1. <https://www.businessinsider.com/zte-created-to-spy-according-to-new-court-documents-2018-6>.
- Chandler, Mark. "A Huawei és a Cisco forráskódja: Correcting the Record." Executive Platform. *Cisco Blogs*, 2012. október 11. <https://blogs.cisco.com/news/huawei-and-ciscos-source-code-correcting-the-record>.
- Chatzky, Andrew és James McBride. "Kína hatalmas öv- és útkezdeményezése". Backgrounder. Council on Foreign Relations. Hozzáférés 2020. március 24. <https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative>.
- Cheney, Clayton. "Kína digitális selyemútja: Stratégiai technológiai verseny és a politikai illiberalizmus exportálása." Blog-Net Politics. Council on Foreign Relations. September 26, 2019. <https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political>.
- Chhabra, Tarun, Rush Doshi, Ryan Hass és Mira Rapp-Hooper. "Az amerikai-kínai verseny újragondolása: Következő generációs perspektívák - Brookings-interjú." Bruce Jones. Szerkesztette Bruce Jones és Will Moreland. Foreign Policy at Brookings. The Brookings Institution, 2019. június. https://www.brookings.edu/wp-content/uploads/2019/06/FP_20190625_global_china.pdf.
- Kínai csapat. "A nemzetközi érdekérvényesítés költségei: Kína beavatkozása az ENSZ emberi jogi mechanizmusába." Jelentés. Human Rights Watch. 2017. szeptember 5. <https://www.hrw.org/report/2017/09/05/costs-international-advocacy/chinas-interference-united-nations-human-rights>.
- "A Huawei kínai távközlési konglomerátum és leányvállalatai vádat emelnek a zsarolással és az üzleti titkok ellopására irányuló összeesküvéssel kapcsolatban." Justice News. Az Egyesült Államok Igazságügyi Minisztériuma - Közkapcsolati Hivatal. February 13, 2020. <https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering>.
- Choucri, Nazli és David D. Clark. *Nemzetközi kapcsolatok a kiberkorszakban: a társfejlődés dilemmája*. Cambridge, MA, USA: MIT Press, 2019.

- Cimpanu, Catalin. "Malware Found Preinstalled on Some Alcatel Smartphones." *ZDNet*, 2019. január 10. <https://www.zdnet.com/article/malware-found-preinstalled-on-some-alcatel-smartphones/>.
- Clark, Robert. "Senki sem akar beszélni a Huawei állami támogatásairól". Hírelemzés. *Light Reading*, 2020. január 9. <https://www.lightreading.com/asia-pacific/no-one-wants-to-talk-about-huaweis-state-subsidies/d/d-id/756697>.
- "CMMC modell." Kiberbiztonsági érettségi modell tanúsítás. A Védelmi Minisztérium beszerzési és fenntartási miniszterhelyettesének hivatala. Hozzáférés 2020. március 30. <https://www.acq.osd.mil/cmmc/draft.html>
- Coghlan, David és Mary Brydon-Miller. (Szerkesztők). *The SAGE Encyclopedia of Action Research, I. és II. kötet*. London: SAGE Publications, Ltd, 2014.
- Corera, Gordan. "Eric Schmidt: a Huawei elfogadhatatlan gyakorlatot folytat." Technológia. *BBC News*, június 18, 2020. <https://www.bbc.com/news/technology-53080113>.
- Cornyn, John. "S.893 - Biztonságos 5G és azon túl 2020. évi törvény". 116th Kongresszusi közjogi 129.
U.S. Government Publishing Office. March 23, 2020.
<https://www.congress.gov/bill/116th-congress/senate-bill/893/text?overview=closed>.
- Cosby, John. "A legellenállóbb szervezetek az eredményalapú kiberbiztonságot követik." Vélemény. *Fifth Domain*, 2020. március 30.
<https://www.fifthdomain.com/opinion/2020/03/31/the-most-resilient-organizations-follow-outcome-based-cybersecurity/>.
- Crawford, Susan P. *Foglyul ejtett közönség: A távközlési ipar és a monopolhatalom az új aranykorban*. New Haven, Connecticut, USA: Yale University Press, 2013.
- "Cumulative Index for *International Security*, 44. kötet, 4. szám (2020 tavasz). Negyedéves folyóirat - Nemzetközi biztonság. Harvard Egyetem Belfer Center for Science and International Affairs. The MIT Press. Hozzáférés 2020. április 25.
<https://www.belfercenter.org/journal-international-security/overview#!cumulative-index>.
- "Kiberbűnözés." Egyesült Nemzetek Szervezete - Kábítószer- és Bűnügyi Hivatal. Hozzáférés március 25, 2020. <https://www.unodc.org/unodc/en/cybercrime/index.html>.

- Danov, Mihail. "Globális versenyjogi keretrendszer: Nemzetközi magánjogi megoldás szükséges." *Journal of Private International Law* 12, no. 1 (2016): 77-105.
<https://doi.org/10.1080/17441048.2016.1150103>.
- "Adatgyűjtés technikai részletei GYIK." Telefonok. Nokia.
https://www.nokia.com/phones/en_int/data-collection-tech-details.
- Davidson, Helen és Ben Doherty. "Explainer: India-Kína határvita: Miről szól a halálos indiai-kínai határvita?". World-India. *The Guardian*, 2020. június 16.
<https://www.theguardian.com/world/2020/jun/17/explainer-what-is-the-deadly-india-china-border-dispute-about>.
- Davies, Jamie. "Az Egyesült Királyság kormánya 6,8 milliárd fontot különít el az 5G álm megvalósítására 2027-ig". Hírek. *Telecoms*, 2018. november 27.
<https://telecoms.com/493818/uk-gov-reserves-6-8bn-to-realise-5g-dream-by-2027/>.
- De Domenico, M., Dirk Brockmann, Chico Camargo, Carlos Gershenson, Daniel Goldsmith, Sabine Jeschonnek, Lorren Kay, Stefano Nichele, Jose R. Nicolas, Thomas Schmickl, Massimo Stella, Josh Brandoff, Angel Jose Martinez Salinas és Hiroki Sayama.
A komplexitás magyarázata. Creative Commons, DOI2019. 10.17605/OSF.IO/TQGNW.
- De Domenico, Manlio és Hiroki Sayama. (Koordinátorok). *A komplexitás magyarázata*. Hozzáférés: 2020. május 1. <https://complexityexplained.github.io/>.
- DeAeth, Duncan. "A tajvani Foxconn a webmail rendszer feltörésének áldozata, az alkalmazottak adatai veszélybe kerültek". Business. *Taiwan News*, 2019. április 15. <https://www.taiwannews.com.tw/en/news/3680809>.
- "A Kereskedelmi Minisztérium 45 napra megújítja az ideiglenes általános engedélyt." Sajtóközlemények - Kereskedelmi végrehajtás. *Amerikai Kereskedelmi Minisztérium - Közkapcsolati Hivatal*. February 13, 2020. <https://www.commerce.gov/news/press-releases/2020/02/department-commerce-renews-temporary-general-license-45-days>.
- "A Kereskedelmi Minisztérium meghosszabbítja a nyilvános véleményezési időszakot a Huawei ideiglenes általános engedélyek meghosszabbítására vonatkozóan." Sajtóközlemények - Kereskedelmi végrehajtás. *Amerikai Kereskedelmi Minisztérium - Közkapcsolati Hivatal*. March 25, 2020. <https://www.commerce.gov/news/press-releases/2020/03/department-commerce-extends-public-comment-period-input-huawei>.

Deppisch, Breanne. "A DHS végre komolyan vette a kiberbiztonságot. Aztán jött Trump."
Magazine Feature. *Politico*, 2019. december 18.

<https://www.politico.com/news/magazine/2019/12/18/america-cybersecurity-homeland-security-trump-nielsen-070149>.

DeVine, Michael E. "Az Egyesült Államok külföldi hírszerzési kapcsolatai: Háttér, politikai és jogi felhatalmazások, kockázatok, előnyök". Jelentés. Congressional Research Service. Május 15. 2019. <https://fas.org/sgp/crs/intel/R45720.pdf>.

Dienst, Jonathan, Joe Valiquette és Rich Schapiro. "New York-i technológiai cég kínai berendezéseket adott el az amerikai hadseregnek, állítják a szövetségi". U.S. News. NBC News. November <https://www.nbcnews.com/news/us-news/feds-raid-new-york-tech-firm-suspected-7-selling-chinese-equipment-n1078191> 2019..

Doffman, Zak. "A Huawei-t 'lopással és kétes etikával' vádolják - - De nem ez a legrosszabb." Innováció. *Forbes*, 2019. május 25.

<https://www.forbes.com/sites/zakdoffman/2019/05/25/huawei-accused-of-theft-and-dubious-ethics-why-it-should-come-as-no-surprise/#296527373f59>.

Doffman, Zak. "Kína most lépett át egy veszélyes új vonalat a Huawei számára: "Lesznek következmények"." Innováció. *Forbes*, 2019. december 16.

<https://www.forbes.com/sites/zakdoffman/2019/12/16/china-just-crossed-a-dangerous-new-line-for-huawei-there-will-be-consequences/#1d3effb575a3>.

Doffman, Zak. "Kína épp most bocsátott ki új fenyegetéseket a Huawei miatt: ezúttal a Nokia és az Ericsson van a célkeresztjében." Innováció. *Forbes*, 2020. február 9.

<https://www.forbes.com/sites/zakdoffman/2020/02/09/china-just-issued-stark-new-threats-over-huawei-this-time-nokia-and-ericsson-are-in-its-sights/#57f21d2119d7>.

Dunn-Cavelty, Myriam és Andreas Wenger. "A kiberbiztonság találkozik a biztonságpolitikával: Complex Technology, Fragmented Politics, and Networked Science" (Komplex technológia, töredezett politika és hálózatos tudomány). *Contemporary Security Policy* 41, no. 1 (2020): 5-32. <https://doi.org/10.1080/13523260.2019.1678855>.

Dwyer, Morgan. "A Védelmi Minisztérium új, technológia-központú szervezeteinek alternatívája". Kommentár. CSIS. January 22, 2020.

<https://www.csis.org/analysis/alternative-defense-departments-new-technology-focused-szervezetek>.

- Economy, Elizabeth C. "A hidra a fejetlen lovas ellen: Kína és az Egyesült Államok." Blog-Asia Unbound. Council on Foreign Relations. 2020. április 15.
<https://www.cfr.org/blog/hydra-vs-headless-horseman-china-and-united-states>.
- Eaglen, Mackenzie. "Mi lenne, ha a Pentagon kihagyná az 5G-t?". Ötletek. *Defense One*, május 11, 2020. <https://www.defenseone.com/ideas/2020/05/what-if-pentagon-skipped-5g/165277/>.
- "Az Ericsson 1 milliárd dollárra bírságolták a széleskörű korrupció miatt." Hírek. *Deutsche Welle*, december 7, 2019. <https://p.dw.com/p/3UMt3>.
- Esper, Mark. "Globális Biztonsági Fórum: Emerging Technologies Governance." Kathleen H. Hicks. Átirat. CSIS. January 24, 2020. <https://www.csis.org/analysis/global-security-forum-emerging-technologies-governance>.
- "Az EU újabb csapást mér az Egyesült Államokra, lehetővé téve a tagok számára, hogy döntsenek a Huawei 5G szerepéről." Europe News. CNBC via Reuters. January 29, 2020. <https://www.cbc.com/2020/01/29/eu-deals-blow-to-us-allowing-members-to-decide-on-huaweis-5g-role.html>.
- Eversden, Andrew. "Kína 5G technológiája nemzetbiztonsági kérdés... vagy kereskedelmi kérdés?". *C4ISRNET*, 2020. február 28. <https://www.c4isrnet.com/show-reporters/rsa/2020/02/28/huaweis-a-national-security-issue-or-is-it-a-trade-issue/>.
- Eversden, Andrew. "A kormányzat és az ipar hogyan küzdheti le az örökös kihívást". Ipar. *Fifth Domain*, 2020. március 16. <https://www.fifthdomain.com/home/2020/03/16/ways-government-industry-can-overcome-a-perpetual-challenge/>.
- Eversden, Andrew. "A Trump-kormányzatnak az új törvény értelmében 5G biztonsági stratégiát kell kidolgoznia". Kritikus infrastruktúra. *Fifth Domain*, 2020. március 24. <https://www.fifthdomain.com/civilian/2020/03/24/trump-administration-must-produce-5g-security-strategy-under-new-law/>.
- Eversden, Andrew. "A Pentagon kiberpolitikai javaslati idén megvalósulhatnak". Capital Hill. *Fifth Domain*, 2020. április 22. <https://www.fifthdomain.com/congress/capitol-hill/2020/04/22/cyber-policy-suggestions-for-pentagon-could-be-implemented-this-year/>.

- Eversden, Andrew. "A kínai technológiát tiltó szabályjavaslatnak figyelembe kell vennie a kisvállalkozókat, figyelmeztetnek a szenátorok". Capital Hill. *Fifth Domain*, 2020. május 5. <https://www.fifthdomain.com/congress/capitol-hill/2020/05/05/proposed-rule-banning-chinese-tech-needs-to-consider-small-contractors-senators-warn/>.
- Falk, Rachael. "Tényleg szétválasztható-e az 5G hálózat "magja" és "széle"?". Strategist Special Report. *The Strategist*, 2020. január 17. <https://www.aspistrategist.org.au/can-the-core-and-edge-of-a-5g-network-really-be-separated/>.
- Farivar, Masood. "Vesztegetési és korrupciós vádak követik a Huawei-t a világ minden táján". Kelet-Ázsia és a csendes-óceáni térség. *VOA News*, 2019. február 11. <https://www.voanews.com/east-asia-pacific/bribery-corruption-charges-follow-huawei-around-world>.
- Farrell, Henry. "Bolton azt állítja, hogy Trump kisegítette Kína vezetőjét a ZTE-vel kapcsolatban. Mi az a ZTE?". Hírek- Majomketrec-elemzés. *The Washington Post*, 2020. január 28. <https://www.washingtonpost.com/politics/2020/01/28/bolton-alleges-that-trump-helped-out-chinas-leader-zte-whats-zte/>.
- Feldstein, Steven. "A digitális tekintélyelvűség terén Kína kihívást jelent - de nem az egyetlen kihívás". *War on the Rocks*, 2020. február 12. <https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/>.
- Fendos, Justin. "Dél-Korea korrupciós kultúrája". The Koreas. *The Diplomat*, november 17, 2016. <https://thediplomat.com/2016/11/south-koreas-corruption-culture/>.
- Field, Matthew. "Miért gondolják a brit kémek, hogy jobban tudják a Huawei-t, mint az USA." Technology Intelligence. *The Telegraph*, 2020. január 29. <https://www.telegraph.co.uk/technology/2020/01/29/britains-spooks-think-know-better-us-huawei/>.
- Finley, Clint. "A WIRED útmutatója az 5G-hez". WIRED. December 18, 2019. <https://www.wired.com/story/wired-guide-5g/>.
- Finley, Clint. "A szenátorok 1 milliárd dollárt javasolnak, hogy megelőzzék a Huawei-t az 5G-ben. Ez aprópénz." Business. *WIRED*, 2020. január 14. <https://www.wired.com/story/billion-outpace-huawei-5g-small-change/>.

- Fletcher, Bevin. "Az Ericsson, a Nokia 5G-szerződéseket köt a kínai szolgáltatókkal - jelentés." 5G. *Fierce Wireless*, 2019. november 8. <https://www.fiercewireless.com/5g/ericsson-nokia-ink-5g-deals-chinese-operators-report>.
- Ford, Lindsey. "A Kína-vita újrafókuszálása: Az amerikai szövetségesek és az amerikai-kínai "szétválasztás" kérdése. Blog-Order from Chaos. The Brookings Institution. February 7, 2020. <https://www.brookings.edu/blog/order-from-chaos/2020/02/07/refocusing-the-china-debate-american-allies-and-the-question-of-us-china-decoupling/>.
- "Elítélték az Alcatel korábbi vezetőjét." News Wire Feed. *Light Reading*, szeptember 24, 2008. <https://www.lightreading.com/former-alcatel-exec-sentenced/d/d-id/661544>.
- Fravel, M. Taylor, J. Stapleton Roy, Michael D. Swaine, Susan A. Thornton és Ezra Vogel. "Kína nem ellenség." Vélemények. *The Washington Post*, 2019. július 3. https://www.washingtonpost.com/opinions/making-china-a-us-enemy-is-counterproductive/2019/07/02/647d49d0-9bfa-11e9-b27f-ed2942f73d70_story.html.
- Friedman, Uri. "Hogyan válasszunk az USA és Kína között? It's Not That Easy." Politics. *The Atlantic*, 2019. július 26. <https://www.theatlantic.com/politics/archive/2019/07/south-korea-china-united-states-dilemma/594850/>.
- Fulton III, Scott. "Mi az 5G? Üzleti útmutató a következő generációs vezeték nélküli technológiához." Hogyan fogja az 5G átalakítani az üzleti életet. *ZDNet*, 2019. szeptember 19. <https://www.zdnet.com/article/what-is-5g-the-business-guide-to-next-generation-wireless-technology/>.
- Gallagher, Sean. "How US Software Ended Up Powering Chinese Assault Helicopters". Policy. *Ars Technica*, 2012. július 3. <https://arstechnica.com/tech-policy/2012/07/how-us-software-ended-up-in-chinese-assault-helicopters/>.
- Garfinkle, Adam. "Hatalomkoncentrációk: A nettó hatás." *The American Interest*, április 7., 2020. <https://www.the-american-interest.com/2020/04/07/the-net-effect/>.
- Garlick, Jeremy. "Nem olyan egyszerű: A komplexitás elmélete és Kína felemelkedése." *China Report* no52., 4 (2016): 284-305. <https://doi.org/10.1177/0009445516661884>.
- Garmey, Brian. "Hogyan tudják a szövetségi ügynökségek jobban kezelni az ellátási lánc kiberkockázatait?". Vélemény. *Fifth Domain*, 2019. július 17. <https://www.fifthdomain.com/opinion/2019/07/17/how-federal-agencies-can-better-manage-supply-chain-cyber-risks/>.

- Garnick, Jennifer Stisa. "A Huawei Hacking egy biztonsági botrány." *Just Security*, március 24., h2014.ttps://www.justsecurity.org/8488/huawei-hacking-security-scandal/.
- Garside, Juliette. "Az Apple beszállítója, a Foxconn meghekkelte a gyári körülmények elleni tiltakozás során." *Technology-Apple*. 2012. február 9.
<https://www.theguardian.com/technology/2012/feb/09/apple-foxconn-hackers-factory-feltételek>.
- Geer, Dan, Eric Jardine és Eireann Leverett. "A piaci koncentrációról és a kiberbiztonsági kockázatról". *Journal of Cyber Policy* (online megjelent 2020. február 24.).
<https://doi.org/10.1080/23738871.2020.1728355>.
- Ghoshal, Anirban. "A Nokia és az Ericsson hamarosan exportálja az Indiában gyártott 5G berendezéseket." *Technológia. TechCircle*, 2018. október 26.
<https://www.techcircle.in/2018/10/26/nokia-ericsson-to-soon-export-5g-equipment-made-in-india>.
- Giglio, Mike. "A kínai kémek támadásban vannak." *Politika. The Atlantic*, augusztus
<https://www.theatlantic.com/politics/archive/2019/08/inside-us-china-espionage-26,war/595747/2019..>
- Gilding, Simeon. "5G választások: A világügyek sorsdöntő pillanata." *The Strategist*, január 29., h2020.ttps://www.aspistrategist.org.au/5g-choices-a-pivotal-moment-in-world-affairs/.
- Gill, Indermit. "Aki a mesterséges intelligencia terén élen jár, az fogja 2030-uralni a világot 2100-ig". *Blog-Future Development. The Brookings Institution*. January 17, 2020.
<https://www.brookings.edu/blog/future-development/2020/01/17/whoever-leads-in-artificial-intelligence-in-2030-will-rule-the-world-until-2100/>.
- Gillispie, Clara. "Dél-Korea 5G ambíciói". *Academic Paper Series. Korea Economic Institute of America*. 2020. március 23.
http://keia.org/sites/default/files/publications/kei_aps_gillispie_200316.pdf.
- Gioe, David V. "'Minél több dolog változik': HUMINT in the Cyber Age." In *The Palgrave Handbook of Security, Risk and Intelligence*, szerkesztette: Robert Dover, Huw Dylan és Michael Goodman, 213-227. London: Palgrave Macmillan, 2017.
- Gioe, David V., Michael S. Goodman és Alicia Wanless. "A kiberbiztonsági imperatívuszok újbóli kiegyensúlyozása: A társadalmi réteg foltozása." *Journal of Cyber Policy* 4, no. 1 (2019): 117- h137.ttps://doi.org/10.1080/23738871.2019.1604780.

- Glosserman, Brad. "A Huawei és az 5G világ realitásai". Kommentár/Világ. *The Japan Times*, 2020. február 3. <https://www.japantimes.co.jp/opinion/2020/02/03/commentary/world-commentary/huawei-realities-5g-world/#.Xptzo-pKjIV>.
<https://www.japantimes.co.jp/opinion/2020/02/03/commentary/world->
- Goldstone, Jack A., Robert H. Bates, David L. Epstein, Ted Robert Gurr, Michael B. Lustik, Monty G. Marshall, Jay Ulfelder és Mark Woodward. "Egy globális modell a politikai instabilitás előrejelzésére". *American Journal of Political Science* 54, no. 1 (2010): 190-208. www.jstor.org/stable/20647979.
- Gong, Yeming. *Globális működési stratégia: Alapelvek és gyakorlat*. Berlin: Berlin: Springer- Verlag, 2013.
- Goodman, Matthew P. "Predatory Economics and the China Challenge". *Global Economics Monthly* 6, no. 11 (November 2017): 1-2. <https://www.csis.org/analysis/predatory-economics-and-china-challenge>.
- Goodman, Michael S. "Az angol-amerikai hírszerzés megosztásának alapjai". *Studies in Intelligence* 59, no. 2 (Kivonat, 2015. június): 1-12. <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-2/pdfs/Goodman-Evolution-UK-US-JIC-June-2015.pdf>.
- Goodman, Ryan. "A tömeges megfigyelés nemzetközi előírásai (avagy mi hiányzik a Greenwald vs. Wittes vitából)". *Just Security*, 2014. március 24. <https://www.justsecurity.org/8448/international-proscriptions-mass-surveillance-or-whats-missing-greenwald-vs-wittes-debate/>.
- Gorman, Lindsay és Matt Schrader. "Az amerikai cégek segítik Kína orwelli államának felépítését." *Érv. Foreign Policy*, 2019. március 19. <https://foreignpolicy.com/2019/03/19/962492-orwell-china-socialcredit-surveillance/>.
- Gorman, Lindsay. "Az USA-nak be kell szállnia a szabványok játékába - a hasonlóan gondolkodó demokráciákkal". Kiberbiztonság és elrettentés. *Lawfare*, 2020. április 2. <https://www.lawfareblog.com/us-needs-get-standards-game-minded-democracies>.
- Gould, Joe. "Key Republicans Seek Ban on Intel Sharing with Countries that Use Huawei." *5G. C4ISRNET*, 2020. január 27. <https://www.c4isrnet.com/congress/2020/01/27/key-republicans-seek-ban-on-intel-sharing-with-countries-that-use-huawei/>.

- Graff, Garrett M. "Az USA elveszíti a Huawei elleni harcot". Business. *WIRED*, január 29., h2020.<https://www.wired.com/story/uk-huawei-5g-networks-us/>.
- Greene, Jay és Shara Tibken. "Törvényhozók az amerikai vállalatoknak: Huawei, ZTE." *CNET*, október 8, 2012.
- Haass, Richard N. "A nem-polaritás kora: Mi fogja követni az amerikai dominanciát?" *Foreign Affairs*, 2008. május-június. <https://www.foreignaffairs.com/articles/united-states/2008-05-03/age-nonpolarity>.
- Hamilton, Isobel Asher. "A Trump-adminisztrációnak nem sikerült meggyőznie az Egyesült Királyságot, hogy dobja ki a Huawei-t, és más szövetségesei sem hallgatnak rá." *Business Insider*, 2020. március 11. <https://www.businessinsider.com/huawei-how-allies-are-reacting-to-us-calls-to-avoid-the-tech-firm-2019-2>.
- Harrington Jr., Joseph E. *Az összjátékos elmélete és versenypolitika*. Cambridge, Massachusetts: Massachusetts Institute of Technology, 2017.
- Harris, Peter. "Mikor ér véget az egypólusú világ?: A hegemonia az ázsiai és európai dominanciára épül". *The National Interest*, 2019. május 27. <https://nationalinterest.org/feature/when-will-unipolar-world-end-59202>.
- H., Stuart. "Zéró bizalom architektúra tervezési elvei: Alpha Release for the ZTA Principles on GitHub." Blogbejegyzés. NCSC. November 20, 2019. <https://www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles>.
- Hemphill, Thomas A. és George O. White III. "Kína nemzeti bajnokai: A nemzeti iparpolitika fejlődése - vagy a gazdasági protekcionizmus új korszaka?". *Thunderbird International Business Review* 255., szám (2013. március/április). DOI: 10.1002/tie.21535.
- Hendrick, Diane. "Komplexitáselmélet és konfliktusátalakítás: A lehetőségek és következmények feltárása". Working Paper 17. Centre for Conflict Resolution-Department of Peace Studies. University of Bradford. June 2009. https://www.beyondintractability.org/bi_affiliated_projects/dsap/publications/complexity-theory-transformation-hendrick.pdf.
- Hicks, Kathleen H., Joseph Federici, Seamus P. Daniels, Rhys McCormick és Lindsey R. Sheppard. "Kevesebbre jutni? Az innovációs felsőbbrendűségi stratégia." Jelentés. CSIS. Január h23, 2020. <https://www.csis.org/analysis/getting-less-innovation-superiority-strategy>.

- Hieronymi, Andreas. "A rendszertudomány megértése: A Visual and Integrative Approach." *Systems Research and Behavioral Science* 30, no. 5 (2013): 580-595.
<https://doi.org/10.1002/sres.2215>.
- Hitchens, Theresa. "Szakértők szerint az USA elveszítheti az 5G szabványosítási csatát Kínával szemben". *Networks/Cyber. Breaking Defense*, 2020. május 11.
<https://breakingdefense.com/2020/05/us-risks-losing-5g-standard-setting-battle-to-china-experts-say/>.
- Hoffman, Samantha és Elsa Kania. "A Huawei és a kínai hírszerzési és kémelhárítási törvények kétértelműsége". *The Strategist*, 2018. szeptember 13.
<https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/>.
- Hofmann, Jeanette. "Több érdekelt fél részvételével működő internetirányítás: A fikció gyakorlatba ültetése." *Journal of Cyber Policy* 1, no. 1 (2016): 29-49.
<https://doi.org/10.1080/23738871.2016.1158303>.
- Homburger, Zine. "A kiberbiztonsági kapacitásépítés szükségessége és buktatói a normafejlesztés érdekében a kibertérben". *Global Society*, 33, no. 2 (2019): 224-242.
<https://doi.org/10.1080/13600826.2019.1569502>.
- Horwitz, Jeremy. "Az USA 5G biztonságát veszélyezteti a Trump-adminisztráció harcossága és fantáziálása". *Biztonság - Vélemény. Venture Beat*, 2020. február 6.
<https://venturebeat.com/2020/02/06/u-s-5g-security-is-imperiled-by-trump-administration-infighting-and-fantasies/>.
- Horwitz, Jeremy. "Az Apple, a Foxconn és mások 81 ujjur kényszermunkát alkalmaznak". *Mobile. Venture Beat*, 2020. március 2. <https://venturebeat.com/2020/03/02/apple-foxconn-and-81-others-are-accused-of-using-ughur-forced-labor/>.
- Horwitz, Josh. "A Trump-csapat ötlete, hogy államosított 5G-vel szálljanak szembe Kínával, pont az, amit Kína is tenne". *Quartz*, január 29, 2018. <https://qz.com/1191154/the-trump-teams-idea-to-counter-china-with-nationalized-5g-is-just-what-china-would-do/>.
- Huawei Kiberbiztonsági Értékelő Központ (HCSEC) Felügyeleti Testület. "Éves jelentés: 2019." HCSEC. 2019. március.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

- Hui, Sylvia. "Egy feltörekvő szuperhatalom bevonása: Kína mint külpolitikai szereplő megértése." Asia Programme Paper. Chatham House. 2011. július.
https://www.chathamhouse.org/sites/default/files/0711pp_hui.pdf.
- "INSCR adatlap." Center for Systemic Peace. Hozzáférés április 19,2020.
<http://www.systemicpeace.org/inscrdata.html>.
- Insinna, Valerie. "A Pentagon jelentése szerint az amerikai technológiai cégekbe irányuló ragadozó külföldi befektetések növekedtek a járvány közepette." *C4ISRNET*, 2020. május 6. <https://www.c4isrnet.com/unmanned/2020/05/06/pentagon-reports-boost-in-predatory-foreign-investment-to-us-tech-firms-since-pandemic-start/>.
- "Nemzetközi szervezet." Folyóiratok. Cambridge University Press. Hozzáférés április 19,2020.
<https://www.cambridge.org/core/journals/international-organization>.
- Ivaldi, Marc, Bruno Jullien, Patrick Rey, Paul Seabright és Jean Tirole. "A hallgatólagos összejátszás közgazdaságtana". Zárójelentés a Versenypolitikai Főigazgatóság számára. Európai Bizottság, március
https://ec.europa.eu/competition/mergers/studies_reports/the_economics_of_tacit_collusion_2013_en.pdf.
- Janzwood, Scott és Jinelle Piereder. "A globális politika komplex rendszerszemlélete". International Relations. Oxford Bibliographies. Oxford University Press. Február
Hozzáférés 26,2020. április 28.
<https://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-2020.9780199743292-0278.xml?q=cyber#firstMatch>.
- Jennings, Ralph. "Az Apple vállalkozója, a Foxconn saját márkás telefonjaival nyereszkesedik a nehéz piacon". Ázsia. *Forbes*, 2019. január 31.
<https://www.forbes.com/sites/ralphjennings/2019/01/31/apple-contractor-foxconn-makes-gains-with-its-own-brand-of-phones-in-a-tough-market/#1ef048012c48>.
- Jensen, Benjamin. "Amikor a rendszerek meghibásodnak: Mit mondanak a járványok és a kibertér a nemzetbiztonság jövőjéről. Kommentár. *War on the Rocks*, 2020. április 9.
<https://warontherocks.com/2020/04/when-systems-fail-what-pandemics-and-cyberspace-tell-us-about-the-future-of-national-security/>.
- Jiang, Sijia. "A kínai Huawei legalább 15 milliárd dollárra emeli éves K+F költségvetését." Technology News. *Reuters*, július 26,2018. <https://www.reuters.com/article/us-huawei-r-d/chinas-huawei-to-raise-annual-rd-budget-to-at-least-15-billion-idUSKBN1KG169>.

- Jie, Yu és Joseph Barnsley. "Dengtől Xiig: A gazdasági reform, a Selyemút és a Középbirodalom visszatérése." Különjelentés (023). LSE IDEAS. May, 2017. <http://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-From-Deng-to-Xi.pdf>.
- "Johnson: A Huawei 5G döntése egyensúlyt teremt az innováció és a biztonság között." AJ Impact / Kína. *Al Jazeera*, 2020. január 27. <https://www.aljazeera.com/ajimpact/johnson-huawei-5g-decision-balance-innovation-security-200127181107270.html>.
- Johnson, Keith és Elias Groll. "A Huawei valószínűtlen felemelkedése: Hogyan jutott el egy kínai magánvállalat a világ legfontosabb feltörekvő technológiájának uralmához?". *Foreign Policy*, 2019. április 3. <https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/>.
- Kahn, Michael és Jan Lopatka. "A nyugati szövetségesek megállapodtak az 5G biztonsági irányelveiben, de figyelmeztetnek a külső befolyásra." Technológiai hírek. *Reuters*, 2019. május 3. <https://www.reuters.com/article/us-telecoms-5g-security/western-allies-agree-5g-security-guidelines-warn-of-outside-influence-idUSKCN1S91D2>.
- Kania, Elsa B. "Az 5G jövőnk biztosítása: A verseny kihívása és megfontolások a U.S. Policy." Jelentések. Center for a New American Security. November 07, 2019. <https://www.cnas.org/publications/reports/securing-our-5g-future>.
- Kania, Elsa B. "Miért nincs az USA-nak saját Huawei-je?". The 5G Future-Opinion. *Politico*, 2020. február 25. <https://www.politico.com/news/agenda/2020/02/25/five-g-failures-future-american-innovation-strategy-106378>.
- Kania, Elsa B. és Lindsay Gorman. "Az Egyesült Államok nem engedheti meg magának, hogy elutasítsa a kínai tehetségeket". Argument. *Foreign Policy*, 2020. május 13. <https://foreignpolicy.com/2020/05/13/united-states-cant-afford-turn-away-chinese-talent/>.
- Kaplan, Robert D. "Amerikának fel kell készülnie az eljövendő kínai birodalomra". *The National Interest*, 2019. június 17. <https://nationalinterest.org/print/feature/america-must-prepare-coming-chinese-empire-63102>.
- Kaplan, Robert D. "Miért lesz más az amerikai-kínai hidegháború". *The National Interest*, 2020. január 19. <https://nationalinterest.org/blog/buzz/why-us-china-cold-war-will-be-different-114986>.

Kastrenakes, Jacob. "Az Egyesült Államok, az Egyesült Királyság és más kormányok arra kéri a vállalatokat, hogy építsenek hátsó ajtókat a titkosított eszközökbe". *Cybersecurity. The Verge*, 2018. szeptember 3. <https://www.theverge.com/2018/9/3/17815196/five-eyes-encryption-backdoors-us-uk-australia-nz-canada>.

Katwala, Amit. "Így kutatja át a GCHQ a Huawei hardverét rosszindulatú kódok után." *WIRED UK*, 2019. február 22. <https://www.wired.co.uk/article/huawei-gchq-security-evaluation-uk>.

Keane, Sean. "Huawei-tilalom: Huawei Huawei: Teljes időrend, mivel figyelmeztet a brit 5G bevezetésében játszott szerepének megzavarására." *CNET*, 2020. április 17. Hozzáférés: 2020. április 17. (rendszeresen frissítve). <https://www.cnet.com/news/huawei-ban-full-timeline-us-government-china-trump-security-threat-5g-p40/>.

Kendall, Frank. "Kiberbiztonsági érettségi modell tanúsítása: Egy ötlet, amelynek még nem jött el az ideje, és soha nem is jöhet el". *Business. Forbes*, 2020. április 29. <https://www.forbes.com/sites/frankkendall/2020/04/29/cyber-security-maturity-model-certification-idea-whose-time-has-not-come-and-never-may/#35ea66773bf2>.

Kennedy, Scott. "Kína egyenlőtlen csúcstechnológiai lendülete: Implications for the United States." Jelentés. CSIS. February 27, 2020. <https://www.csis.org/analysis/chinas-uneven-high-tech-drive-implications-united-states>.

Kerbel, Josh. "Thinking Straight: Kognitív torzítás a Kínáról szóló amerikai vitában." *Studies in Intelligence* 48, no. 3 (2004): 27-35. <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol48no3/pdf/v48i3a03p.pdf>.

Kerbel, Josh. "Coming to Terms With Anticipatory Intelligence". Commentary. *War on the Rocks*, 2019. augusztus 13. <https://warontherocks.com/2019/08/coming-to-terms-with-anticipatory-intelligence/>.

Kerber, Wolfgang és Heike Schweitzer. "Interoperabilitás a digitális gazdaságban". *Journal of Intellectual Property, Information Technology and E-Commerce Law* 8, no. 1 (2017): 39-58.

Kim, Joseph. "A Huawei rejtélyes vezeték nélküli projektje Észak-Koreában". George W. Bush Presidential Center, 2019. szeptember 3. <https://www.bushcenter.org/publications/articles/2019/09/huawei-wireless-north-korea.html>.

- Kissinger, Henry A. "Az amerikai-kínai kapcsolatok jövője: A konfliktus választás, nem szükségszerűség." *Foreign Affairs*, 91, no. 2 (2012): 44-55.
<https://www.jstor.org/stable/23217220>.
- Klein, Aaron, Nicol Turner Lee, Carrick Flynn, Frank A. Rose és Sheena Chestnut Greitens. "Panelbeszélgetés: Globális technológiai infrastruktúra." Moderátor: Chris Meserole. Webinárium: Global China-Assessing China's Technological Reach in the World. The Brookings Institution. 2020. május 8. Transcript and Video.
<https://www.brookings.edu/events/webinar-global-china-assessing-chinas-technological-reach-in-the-world/>.
- Kliman, Daniel, Ben FitzGerald, Kristine Lee és Joshua Fitt. "A szövetség innovációs bázisának kialakítása." Jelentés - Amerika versenyez 2020. CNAS. March 29, 2020.
<https://www.cnas.org/publications/reports/forging-an-alliance-innovation-base>.
- Klingebiel, Ronald és John Joseph. "Amikor az elsőként mozdulókat jutalmazzák, és amikor nem". Innováció. *Harvard Business Review*, 2015. augusztus 11.
https://hbr.org/2015/08/when-first-movers-are-rewarded-and-when-theyre-not?referral=03759&cm_vc=rr_item_page.bottom.
- Knight, Will. "A kínai Huawei-t érintő legújabb amerikai szankciók visszafelé süllhetnek el." Business.
WIRED, 2020. március. <https://www.wired.com/story/newest-us-sanctions-chinas-huawei-backfire/>.
- Kolton, Michael. "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence." (Kína kiber-szuverenitásra való törekvésének és a kiber-elrettetéssel kapcsolatos nézeteinek értelmezése). *The Cyber Defense Review* 2, no. 1 (2017): 119-54. www.jstor.org/stable/26267405. www.jstor.org/stable/26267405.
- Kubota, Yoko és Tripp Mickle. "Az Apple vizsgálta az ellátási láncában elkövetett lehetséges üzleti visszaéléseket: Company Says it Found No Evidence of Bribery or Kickbacks." Tech. *The Wall Street Journal*, 2018. november 30. <https://www.wsj.com/articles/apple-investigated-possible-business-misconduct-in-its-supply-chain-1543620611>.
- Kupchan, Cliff és Paul Triolo. "Bizalmatlanság, de ellenőrizze: Hogyan működhet együtt az USA és Kína a fejlett technológia területén?". Business and Tech-Opinion. *SupChina*, 2019. november 26. <https://supchina.com/2019/11/26/distrust-but-verify-the-us-china-advanced-technology/>.

- Kynge, James, Yuan Yang és Sue-Lin Wong. "Huawei: Még mindig a túlélésért harcol a Trump-fegyvernység ellenére". *The Big Read - Huawei Technologies. Financial Times*, 2019. július 3. <https://www.ft.com/content/a6db14d8-9993-11e9-9573-ee5cbb98ed36>.
- Lahiri, Tripti és Mary Hui. "Kitiltva: Hogyan vált a Huawei Amerika első számú technológiai ellenségévé?" *Quartz*, május <https://qz.com/1627149/huaweis-journey-to-becoming-us-tech-28,enemy-no-1/2019..>
- Lairson, Thomas D., David Skidmore és Wu Xinbo. "Miért sült el visszafelé a Huawei elleni amerikai kampány." *Trans-Pacific View. The Diplomat*, 2020. május 13., <https://thediplomat.com/2020/05/why-the-us-campaign-against-huawei-backfired/>.
- Landau, Susan. "A biztonsági kudarc a Fehér Házban." *Cyber & Technology. Lawfare*, november 1, 2019. <https://www.lawfareblog.com/security-failure-white-house>.
- Lawson, Stephen. "A Nokia lezárja a felvásárlást, átnevezi Nokia Siemens Networks-re." *News-IT Leadership. ComputerWorld*, 2013. augusztus 7. <https://www.computerworld.com/article/2484790/nokia-closes-acquisition--renames-nokia-siemens-networks.html>.
- Le Maistre, Ray. "A Nokia feltárta az AlcaLu megfelelési időzített bombát." *Üzlet/foglalkoztatás. Light Reading*, 2019. március 22. <https://www.lightreading.com/business-employment/nokia-unearths-alcalu-compliance-timebomb/d/d-id/750356>.
- Le Maistre, Ray. "A Huawei Dingje elérzékenyül az 5G-vel kapcsolatban, 91 szerződéssel büszkélkedik." *5G. Light Reading*, 2020. február 20. <https://www.lightreading.com/5g/huaweis-ding-gets-emotional-about-5g-boasts-91-deals/d/d-id/757629>.
- Ledel, Johannes és Sam Kingsley. "Versenyezhet-e a Nokia, az Ericsson a Huawei-jel?". *Kína. Asia Times*, 2020. február 3. <https://asiatimes.com/2020/02/can-nokia-ericsson-compete-with-huawei/>.
- Lee, Jong-Wha és Ju Hyun Pyun. "Hozzájárul-e a kereskedelmi integráció a békéhez?". *Review of Development Economics* 20, no. 1 (2016. február): 327-344. <https://doi.org/10.1111/rode.12222>.
- Lee, Seungha. "Délkelet-ázsiai harc: Kína és az USA 5G rivalizálásában." *The SAIS China Studies Review*, 2020. május 1. <https://saicsr.org/2020/05/01/southeast-asian-struggle-caught-up-in-the-u-s-china-5g-rivalry/>.

- Leroux-Martin, Philippe és Vivienne O'Connor. "Rendszergondolkodás a béketeremtés és a jogállamiság érdekében: A konfliktus sújtotta környezetekben a komplex reformok támogatása." Jelentés. Peaceworks. United States Institute of Peace. Október 23, 2017. <https://www.usip.org/publications/2017/10/systems-thinking-peacebuilding-and-rule-law>.
- Levita, Ariel (Eli) [sic]. "Az IKT ellátási lánc integritásának alapelvei a kormányzati és vállalati politikákhoz". Papír. A Carnegie Endowment for International Peace. Október 4, 2019. <https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974>.
- Levy, Ian. "Biztonság, komplexitás és Huawei ; az Egyesült Királyság távközlési hálózatainak védelme". People. *NCSC Blog*, 2019. február 22. <https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks>.
- Levy, Ian. "A távközlés jövője az Egyesült Királyságban". NCSC Publications. *NCSC Blog*, január 28., 2020. <https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk>.
- Lewis, Ted G., Thomas J. Mackin és Rudy Darken. "A kritikus infrastruktúra mint komplexen kialakuló rendszer". *International Journal of Cyber Warfare and Terrorism* 1, no. 1 (2011): 1-12. DOI: 10.4018/ijcwt.201101010101.
- Lewis, James Andrew. "A ZTE, a távközlési háborúk és a kiberkémek". Jelentés - CSIS Briefs. CSIS, 201825. június. <https://www.csis.org/analysis/zte-telecom-wars-and-cyber-spies>.
- Lewis, James Andrew. "5G betiltani vagy nem betiltani? Ez nem fekete vagy fehér." Kommentár. CSIS. 2019. április 24. <https://www.csis.org/analysis/5g-ban-or-not-ban-its-not-black-or-white>.
- Lewis, James Andrew. "Statement Before the Senate Committee on the Judiciary - '5G: The Impact on National Security, Intellectual Property, and Competition' - A Testimony by: James A. Lewis." Tanúvallomás. CSIS. May 14, 2019. https://csis-prod.s3.amazonaws.com/s3fs-public/congressional_testimony/Jim%20Lewis%20Written%20Statement%203-4-20.pdf?j.NdIo307mIkIoIZ7sobLj5o088GC53m.
- Lewis, James Andrew, Clete Johnson és Denise E. Zheng. "5G innováció és biztonság: Az iparági és kormányzati vezetés perspektívái." Christopher Krebs, Kim Hart, Jason Boswell, John Godfrey, Susie Armstrong, Peter Lord, Robert Strayer, Eric Wagner, Kevin Linehan, Chris Boyer, Valerie J. Parker, Geoffrey Starks és Jennifer Lane. Esemény. CSIS. Július Audio31,2019., 2h:57m:40s. <https://www.csis.org/events/5g-innovation-and-security>.

- Lewis, James Andrew. "Mit döntött az Egyesült Királyság a Huawei-ről és az 5G-ről?". Kommentár. CSIS. January 28, 2020. <https://www.csis.org/analysis/what-did-united-kingdom-just-decide-huawei-and-5g>.
- Lewis, James Andrew. "Kompensálhatja-e a mesterséges intelligencia a stratégiai hiányosságokat?". Commentary. CSIS. January 29, 2020. <https://www.csis.org/analysis/can-artificial-intelligence-compensate-strategic-shortcomings>.
- Lewis, James Andrew. "A Szenátus Kereskedelmi, Tudományos és Közlekedési Bizottsága - 5G ellátási lánc biztonsága: Lewis szóbeli vallomása". Tanúvallomás. CSIS. March 4, 2020. https://csis-prod.s3.amazonaws.com/s3fs-public/congressional_testimony/200304_Oral_Testimony.pdf?eMPCUCg_p48O8hSNQR7AgV_b3pYHpBeP.
- Lewis, James Andrew. "Stratégia az elrettentés után." Kommentár. CSIS. Március 11,2020.<https://www.csis.org/analysis/strategy-after-deterrence>.
- Lewis, James Andrew. "Cyber Solarium és a kiberbiztonság naplementéje". Kommentár. CSIS. Március 13,2020.<https://www.csis.org/analysis/cyber-solarium-and-sunset-cybersecurity>.
- Lewis, James Andrew. "A Kínába irányuló félvezető-export irányítása." Kommentár. CSIS, május 5,2020.<https://www.csis.org/analysis/managing-semiconductor-exports-china>.
- Leffler, Melvyn P. "Kína nem a Társadalmi Unió. A kettő összekeverése veszélyes." Ideas. *The Atlantic*, 2019. december 2. <https://www.theatlantic.com/ideas/archive/2019/12/cold-war-china-purely-optional/601969/>.
- Liao, Rita. "A Huawei szerint a Kínán kívüli 5G-hálózatok kétharmada már az ő eszközeit használja". *TechCrunch*, 2019. június 25. <https://techcrunch.com/2019/06/25/huawei-wins-5g-szerzodesek/>.
- Lieberthal, Kenneth és Wang Jisi. "Az amerikai-kínai stratégiai bizalmatlanság kezelése". In *John L. Thornton China Center Monograph Series*, no. 4. Washington D.C.: The Brookings Institution, 2012. https://www.brookings.edu/wp-content/uploads/2016/06/0330_china_lieberthal.pdf.
- Lin, Justin Yifu. "A későn érkező előnye." Vélemény. *China Daily*, augusztus 7,2013.http://www.china.org.cn/opinion/2013-08/07/content_29646629.htm.

- Lin, Zhang. "Az amerikai-kínai kereskedelmi háború valójában a civilizációk és ideológiák összecsapása". *Gazdaság-Opinion. South China Morning Post*, 2018. október 15. <https://www.scmp.com/economy/china-economy/article/2168492/us-china-trade-war-really-clash-civilizations-and-ideologies>.
- Lowsen, Ben. "A kínai-amerikai verseny zéróösszegű játékot jelent?: Lehet, de nem kell, hogy jelentsen". *The Diplomat*, 2019. január 3. <https://thediplomat.com/2019/01/does-sino-us-competition-mean-a-zero-sum-game/>.
- "A Lucent beismeri a vesztegetést." News Wire Feed. *Light Reading*, 2007. december 21. <https://www.lightreading.com/lucent-admits-to-bribery/d/d-id/650564>.
- Mares, Octavio. "A legveszélyesebb és legkémkedőbb televízió díját a TCL kapja". *Information Security Newspaper*, 2020. február 4. <https://www.securitynewspaper.com/2020/02/04/the-most-dangerous-spying-television-award-goes-to-tcl/>.
- Markey, Daniel. "Válasz Kína globális befolyásának új eszközeire". Kommentár. *War on the Rocks*, 2020. április 1. <https://warontherocks.com/2020/04/responding-to-chinas-new-tools-of-global-influence/>.
- Maxwell, Paul és Robert Barnsby. "Bizonytalan minden bitsebességen: Miért Ralph Nader a szoftvertervezési ipar igazi OG-je?". *Journal of Cyber Security* 4, no. 3 (2019): 346-361. <https://doi.org/10.1080/23738871.2019.1671471>.
- Medin, Milo, Gilman Louie, Kurt DelBene, Michael McQuade, Richard Murray és Mark Sirangelo. "Az 5G ökoszisztéma: Kockázatok és lehetőségek a Védelmi Minisztérium számára." Jelentés. Védelmi Innovációs Tanács. 2019. április 3. https://media.defense.gov/2019/Apr/04/2002109654/-1/-1/0/DIB_5G_STUDY_04.04.19.PDF.
- Mehta, Ishan. "Trump alatt a kiberbűnözés elleni küzdelem alábbhagyott". *Security-Opinion. WIRED*, 2019. június 20. <https://www.wired.com/story/under-trump-the-fight-against-cybercrime-has-waned/>.
- Meyer, David. "A Qualcommot 1,23 milliárd dollárra büntették az Apple-nek történő illegális kifizetések miatt." *Tech- Antitrust. Fortune*, 2018. január 24. <https://fortune.com/2018/01/24/qualcomm-apple-intel-antitrust-baseband-eu/>.

- Michta, Andrew A. "A globális átrendeződés: A kétpólusúság visszatért." *The American Interest*, 2020. január 17. <https://www.the-american-interest.com/2020/01/17/bipolarity-is-vissza/>.
- "Mérőkövek - A Huawei-ről." Hozzáférés: 2020. február 20. <https://www.huawei.com/en/about-huawei/corporate-information/milestone>.
- Miller, Greg. "'Az évszázad hírszerzési puccsa': For Decades, the CIA Read the Encrypted Communications of Allies and Adversaries." National Security. *The Washington Post*, 2020. február 11. <https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/>.
- Mishra, Yash. "A Huawei idén több mint 17 milliárd dollárt fektet K+F-be". Hírek. *Huawei Central*, 2019. július 30. <https://www.huaweicentral.com/huawei-will-invest-over-17-billion-in-rd-this-year/>.
- Mitchell, Melanie és Santiago Guisasola. "Bevezetés a komplexitásba." Tanfolyamok. Complexity Explorer. Santa Fe Institute. Hozzáférés 2020. február 23. <https://www.complexityexplorer.org/courses/104-introduction-to-complexity>.
- Moffat, James. *Komplexitáselmélet és hálózatközpontú hadviselés*. Information Age Transformation Series. Washington, D.C.: CCRP Publication Series, 2003. http://www.dodccrp.org/files/Moffat_Complexity.pdf.
- Mogull, Rich. "Az Apple biztonsági stratégiája: Make it Invisible." Business-Security-Opinion. *MacWorld*, június <https://www.macworld.com/article/2041724/apples-security-14-strategy-make-it-invisible2013.html>.
- Morris, Iain. "Where Huawei Fears to Tread to Tread." 5G. *Light Reading*, 2018. december 13. <https://www.lightreading.com/mobile/5g/where-huawei-fears-to-tread/d/d-id/748266>.
- Morris, Iain. "Huawei Muscle Puts Ericsson, Nokia on 5G Back Foot in Europe - Források." 5G. *Light Reading*, 2019. február 14. <https://www.lightreading.com/mobile/5g/huawei-muscle-puts-ericsson-nokia-on-5g-back-foot-in-europe---sources/d/d/d-id/749474>.
- Morris, Iain. "A Huawei a 6G-sztárságot tűzte ki célul az 5G-csatározások közepette". 5G. *Light Reading*, 2019. február. <https://www.lightreading.com/mobile/5g/huawei-sets-sights-on-6g-stardom-amid-5g-strife/d/d/d-id/74949497>.

- Morris, Iain. "Az Ericsson és a Nokia felkészült a Kínában gyártott eszközökre vonatkozó amerikai tilalomra." 5G. *Light Reading*, 2019. június 24.
<https://www.lightreading.com/mobile/5g/ericsson-nokia-prepared-for-any-us-banant-on-china-made-gear/d/d/d-id/752342>.
- Morris, Iain. "A Nokia 5G chipválasztása kiteszi magát." 5G. *Light Reading*, október 28.,
<https://www.lightreading.com/5g/nokias-5g-chip-choice-leaves-it-exposed/d/d-2019.id/755184>.
- Morris, Iain. "A Nokia 350 K+F-szakértőt alkalmaz az 5G-problémák megoldására". 5G. *Light Reading*, 2019. október. <https://www.lightreading.com/5g/nokia-hires-350-randd-experts-to-fix-5g-problems/d/d/d-id/755257>.
- Morris, Iain. "A Nokia akár 2,2 milliárd dollár értékű 5G-szerződésekért áll sorba a kínai távközlési vállalatokkal". Ázsia. *Light Reading*, 2019. november 11.
[https://www.lightreading.com/asia-pacific/nokia-in-line-for-5g-contracts-worth-up-to-\\$22b-with-chinese-telcos/d/d-id/755523](https://www.lightreading.com/asia-pacific/nokia-in-line-for-5g-contracts-worth-up-to-$22b-with-chinese-telcos/d/d-id/755523).
- Morris, Iain. "A 6G fegyverkezési verseny meghatározhatja a 2020-as éveket." 6G. *Light Reading*, 2020. február 4. <https://www.lightreading.com/6g/a-6g-arms-race-may-define-the-2020s/a/d-id/757268>.
- Morris, Iain. "A Huawei "18 hónapos előnye" az 5G-ben a telekommunikáció leghamisabb állítása." 5G. *Light Reading*, 2020. március 9.
<https://www.lightreading.com/5g/huaweis-18-month-lead-in-5g-is-telecoms-most-spurious-claim/a/d-id/758064>.
- Nakashima, Ellen, Jeanne Whalen és David J. Lynch. "A Pentagon ejti az ellenállást az új szabályokkal szemben, amelyek tovább korlátoznák a Huawei-nek történő technológiai értékesítést." Technológia. *The Washington Post*, 2020. február 15.
<https://www.washingtonpost.com/technology/2020/02/14/pentagon-drops-opposition-new-rules-that-wat-wurth-restrict-tech-sales-huawei/>.
- Naim, Moises. "A korrupciós kitörés." *The Brown Journal of World Affairs* 2, no. 2 (1995 tavasz/nyár): 245-261. <http://bjwa.brown.edu/2-2/the-corruption-eruption/>.
- "Nemzeti kiberbiztonsági stratégia 2016-2021". Policy Paper. HM Government. November 1, 2016. <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-2021>.
- "Nemzeti kiberbiztonsági stratégia 2016-2021: Jelentés az elért eredményekről." Policy Paper. Cabinet Office. HM Government. May 31, 2019.
<https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021-progress-so-far>.

- "Az Amerikai Egyesült Államok nemzeti hírszerzési stratégiája 2019". A Nemzeti Hírszerzés Igazgatójának Hivatala. 2019.
https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf?utm_source=Press%20Release&utm_medium=Email&utm_campaign=NIS_2019.
- Naughton, John. "Azt hiszed, hogy az iPhone biztonságban van a hackerektől?: That's What They Want You to Think." Technology-Opinion. *The Guardian*, 2019. szeptember 8.
<https://www.theguardian.com/technology/commentisfree/2019/sep/08/iphone-safe-from-hackers-think-again-ios-android-zero-day-exploit-zero-dium-google-threat-analysis>.
- Newman, Lily Hay. "Az 5G biztonságosabb, mint a 4G és a 3G - kivéve, ha nem az." Biztonság. *WIRED*, 2019. december 15. <https://www.wired.com/story/5g-more-secure-4g-except-when-not/>.
- Nichols, Shaun. "Ha kétségbeesik a személyzet admin jelszavainak megosztásán, nézze a jó oldalát. Ez a CIA-Grad Security." Biztonság. *The Register*, 2020. június 16.
https://www.theregister.com/2020/06/16/cia_report_vault_7_leak/.
- Nichols, Philip M. "Kinek tartozik egy védelmi vállalkozás kötelességgel, ha lehetőség van kenőpénz fizetésére?". In *Ethical Dilemmas in the Global Defense Industry*, szerkesztette Claire Finkelstein, Kevin Govern és Daniel Schoeni, (tba oldalak). New York: Oxford University Press, 2020 (megjelenés előtt).
- Nietsche, Carisa és Bolton Smith. "Miért nem fog Európa harcolni a Huawei trójai technológiája ellen." Nemzetbiztonság. *The National Interest*, 2019. október 2.
<https://nationalinterest.org/feature/why-europe-wont-combat-huaweis-trojan-tech-85041>.
- Nietsche, Carisa és Martijn Rasser. "Washington Huawei-ellenes taktikájának újraindítására van szükség Európában". *Argument. Foreign Policy*, 2020. április 30.
<https://foreignpolicy.com/2020/04/30/huawei-5g-europe-united-states-china/>.
- Nietzel, Michael T. "Az Egyesült Államok a K+F finanszírozás terén lemarad a világ többi részével szemben". Leadership. *Forbes*, 2019. október 22.
<https://www.forbes.com/sites/michaelt Nietzel/2019/10/22/the-us-loses-ground-to-the-rest-of-the-world-in-r-and-d-funding/#637c3864202d>.
- "No Pay, No Gain: Huawei Outspends Apple on R&D for a 5G Edge". Új Gazdaság. *Bloomberg News*, 2019. április 25. <https://www.bloomberg.com/news/articles/2019-04-25/huawei-s-r-d-spending-balloons-as-u-s-tensions-flare-over-5g>.

- Nuttall, Chris. "Az Ericsson az 5G vezető szerepét követeli a Huawei felett." Technológiai ágazat. *Financial Times*, 2020. február 13. <https://www.ft.com/content/9cdf33f0-4e8e-11ea-95a0-43d18ec715f5>.
- O'Hanlon, Michael E. "A katonai technológia változásának előrejelzése, 2020-2040". Kutatási jelentés. The Brookings Institution. 2018. szeptember. <https://www.brookings.edu/research/forecasting-change-in-military-technology-2020-2040/>.
- O'Neill, Patrick Howell. "Az Apple szerint a kínai ujjur muszlimok voltak a legutóbbi iPhone-hackelési kampány célpontjai". Computing. *MIT Technology Review*, 2019. szeptember 6. <https://www.technologyreview.com/2019/09/06/133138/apple-says-chinas-ujgur-muslims-were-targeted-in-iphone-hacking-campaign/>.
- "Az O-RAN szövetség áttekintése." O-RAN Szövetség. Hozzáférés április 2, 2020. <https://www.o-ran.org/>.
- Olenick, Doug. "A Brexit kiberbiztonsági hatásai stabilan tartják magukat az átmeneti időszakban". Security News. *SC Magazine*, 2020. január 31. <https://www.scmagazine.com/home/security-news/brexit-cybersecurity-implications-hold-steady-during-transition-period/>.
- Oliver, Richard. "Partnerség és biztonság: Az USA és az Egyesült Királyság védelmi technológiai kapcsolatának előmozdítása a globalizáció korában". Esemény-összefoglaló átirat. Szerkesztette Peter Bean. Wilson Center. July 12, 2005. <https://www.wilsoncenter.org/event/partnership-and-security-advancing-the-usuk-defense-technology-relationship-the-era>.
- "A nyílt szabványok, nem pedig a szankciók Amerika legjobb fegyvere a Huawei ellen." Vezetők - 5Geopolitika. *The Economist*, 2020. április 8. <https://www.economist.com/leaders/2020/04/08/open-standards-not-sanctions-are-americas-best-weapon-against-huawei>.
- Orr, Gordon. "Mire számíthatunk Kínában 2020-ban?". Featured Insights - Commentary. McKinsey and Company. December 2019. <https://www.mckinsey.com/featured-insights/china/what-can-we-expect-in-china-in-2020>.
- Osnos, Evan. "Amerika és Kína versengésének jövője". A Reporter at Large. *The New Yorker*, 2020. január 6. <https://www.newyorker.com/magazine/2020/01/13/the-future-of-americas-contest-with-china>.

- Owen, Malcolm. "A Foxconn 43 millió dolláros csalási hálózatot vizsgál hibás iPhone-alkatrészekkel kapcsolatban". Cikkek. Apple Insider. December 18. <https://appleinsider.com/articles/19/12/18/foxconn-investigating-43m-fraud-ring-2019.involving-faulty-iphone-parts>.
- Pandey, Erica. "Az amerikai tilalmak erősebbé tehetik a Huaweiit." Technológia. *Axios*, 2020. március 5. <https://www.axios.com/huawei-cybersecurity-china-decoupling-5g-11034740-797b-4f00-a17e-7b3265d8bbcd.html>.
- Pancevski, Bojan. "U.S. Officials Say Huawei Can Covertly Access Telecom Networks". *World. The Wall Street Journal*, 2020. február 12. <https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256>.
- Panettieri, Joe. "Huawei: Melyik országban tilos és melyikben engedélyezett? Lista és GYIK." ChannelE2E és After Nines Inc. Hozzáférés 2020. március 10. <https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/>.
- Park, Ju-min. "A Samsung befejezi a mobiltelefon-gyártást Kínában." Technológiai hírek. *Reuters*, 2019. október 2. <https://www.reuters.com/article/us-samsung-elec-china/samsung-ends-mobile-phone-production-in-china-idUSKBN1WH0LR>.
- Parker, George és Daniel Thomas. "UK Looks to Wean Itself Off Chinese Imports" (Az Egyesült Királyság igyekszik leszoktatni magát a kínai importról). UK Trade. *Financial Times*, 2020. június 9. <https://www.ft.com/content/dc22913c-4abd-4258-89fb-e45a4342e2a6>.
- Pawlak, Patryk és Panagiota-Nayia Barmaliou. "A kiberbiztonsági kapacitásépítés politikája: rejtély és lehetőség". *Journal of Cyber Policy* 2, no. 1 (2017): 123-144. <https://doi.org/10.1080/23738871.2017.1294610>.
- Pawlyk, Oriana és Richard Sisk. "A törvényhozók fontolóra veszik egyes F-35 telepítések blokkolását a Huawei 5G hálózatán keresztül: Jelentések." Hírek. *Military.com*, 2020. május 13. <https://www.military.com/daily-news/2020/05/13/lawmakers-consider-blocking-some-f-35-deployments-over-huawei-5g-network-reports.html>.
- Pearlstine, Norman, David Pierson, Robyn Dixon, David S. Cloud, Alice Su és Max Hao Lu. "Az ember a Huawei mögött". *The Los Angeles Times*, 2019. április 10. <https://www.latimes.com/projects/la-fi-tn-huawei-5g-trade-war/>.

- Pearson, Erin. "Melbourne Teen Hacked into Apple's Secure Computer Network, Court Told". Crime. *The Age*, 2018. augusztus 16.
<https://www.theage.com.au/national/victoria/melbourne-teen-hacked-into-apple-s-secure-computer-network-court-told-20180816-p4zxwu.html>.
- Peeters, Christian. "Huawei Ban Creates Challenge for Int'l Antitrust Enforcement." Szakértői elemzés - vélemény. *Law360*, 2019. május 30.
<https://www.law360.com/articles/1164251/huawei-ban-creates-challenge-for-int-l-antitrust-enforcement>.
- Perlow, Jason. "A paranoia elpusztít minket: Miért nem kémkedik a Huawei és más kínai tech cégek az amerikaiak után." Tech Broiler. *ZDNet*, 2019. május 20.
<https://www.zdnet.com/article/paranoia-will-destroy-you-why-chinese-tech-isnt-spying-on-us/>.
- Pfefferkorn, Riana. "A kormányzati hackerek biztonsági kockázatai". The Center for Internet and Society, Stanford Law School. September 2018.
https://cyberlaw.stanford.edu/files/publication/files/2018.09.04_Security_Risks_of_Government_Hacking_Whitepaper.pdf.
- Pomerleau, Mark. "Két év elteltével hogyan változtatta meg az új stratégia a kiberműveleteket?". CyberCon. *Fifth Domain*, 2019. november 11.
<https://www.fifthdomain.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations/>.
- Pomerleau, Mark. "A Pentagon következetlenül kezeli a kibersebezhetőségeket". DoD. *Fifth Domain*, 2020. március 17. <https://www.fifthdomain.com/dod/2020/03/17/the-pentagon-is-handling-cyber-vulnerabilities-inconsistently/>.
- Poon, Kos. "Tajvanon öt volt Foxconn-alkalmazott ellen emeltek vádat." Business. *The Wall Street Journal*, 2014. május 21. <https://www.wsj.com/articles/five-former-foxconn-employees-indicted-for-accepting-bribes-1400651370?tesla=y>.
- Pothier, Fabrice és David Fernandez. "Kína-EU: A tíz intézkedés megvalósítása?". Ramussen Global. Május 2020. https://rasmussenglobal.com/wp-content/uploads/2020/05/EU-China-audit_Rasmussen_Global.pdf.
- Prince, Conrad. "A koronavírus-járvány és a kibertér." Kommentár. RUSI. Április h20,2020. <https://rusi.org/commentary/coronavirus-pandemic-and-cyber-landscape>.

- Prince, Conrad és James Sullivan. "Az Egyesült Királyság kiberstratégiája: Kihívások a következő fázisban." Briefing Papers. RUSI. June 27, 2019.
<https://rusi.org/publication/briefing-papers/uk-cyber-strategy-challenges-next-phase>.
- Rasser, Martijn. "Az Egyesült Államok vezető szerepének megteremtése a 6G területén". Cyber & Technology. *Lawfare*, augusztus h13,2019.<https://www.lawfareblog.com/setting-stage-us-leadership-6g>.
- Rasser, Martijn. "A technológiai szövetségek segítenek a járvány utáni jövőnk alakításában." Vélemény. *C\$ISRNET*, 2020. április 14.
<https://www.c4isrnet.com/opinion/2020/04/14/technology-alliances-will-help-shape-our-post-pandemic-future/>.
- Raymond, Mark és Laura Denardis. "Multistakeholderizmus: Egy kialakulatlan globális intézmény anatómiája." *International Theory* 7, no. 3 (2015): 572-616.
<https://doi.org/10.1017/S1752971915000081>.
- Rayner, Gordon. "Boris Johnson az eddigi legegységesebb jelzést adta, hogy a választások után betiltja a Huawei-t." Politika. *The Telegraph*, 2019. december 4.
<https://www.telegraph.co.uk/politics/2019/12/04/boris-johnson-gives-clearest-indication-yet-will-ban-huawei/>.
- Reardon, Marguerite. "A Nokia és az Ericsson a Huawei 5G alternatívájaként kínálja magát". *CNET*, 2020. március 4. <https://www.cnet.com/news/nokia-and-ericsson-pitch-themselves-as-huawei-5g-alternative/>.
- Reichert, Corinne. "A Huawei újabb 45 napos haladékot kapott a Kereskedelmi Minisztériumtól." *CNET*, február <https://www.cnet.com/news/huawei-gets-another-45-day-14-reprieve-from-commerce-department/2020..>
- Reichert, Corinne és Marguerite Reardon. "Huawei Says US Ban Will 'Significantly Harm' American Jobs, Companies." *CNET*, 2019. május 16.
<https://www.cnet.com/news/huawei-says-blacklisting-will-significantly-harm-american-companies-jobs/>.
- Reichert, Corinne és Sean Keane. "A Huawei szerint Trump tiltása árt az amerikai 5G kiépítésének." *CNET*, 2019. május 16. <https://www.cnet.com/news/trump-effectively-bans-huawei-with-national-security-order/>.
- Reinsch, William Alan. "Walk the Line." Kommentár. CSIS. February 3, 2020.
<https://www.csis.org/analysis/walk-line>.

- Rempfer, Kyle. "A DoD Kínában gyártott hamis katonai felszerelést vásárolt, beleértve az éjjellátó ruházatot, amely valójában nem is működött." News-Your Military. *Military Times*, May 30, 2019. <https://www.militarytimes.com/news/your-air-force/2019/05/30/dod-bought-phony-military-gear-made-in-china-including-counter-night-vision-clothing-that-didnt-actually-work/>.
- Renard, Thomas. "Az EU kiberpartnerségei: Az EU stratégiai partnerségeinek értékelése harmadik országokkal a kibertérben". *European Politics and Society* 19, no. 3 (2018). <https://doi.org/10.1080/23745118.2018.1430720>.
- "Kötelező olvasmányok." Konferenciák - Etikai dilemmák a globális védelmi iparban. Center for Ethics and the Rule of Law. University of Pennsylvania Law School. April 9, 2015. <https://www.law.upenn.edu/institutes/cerl/conferences/ethicaldilemmas/required-readings.php>.
- Ribeiro, John. "Az USA több millió dolláros bírságot szabott ki a Qualcommra a kínai korrupciós vádak miatt". News-Legal. *PCWorld*, 2016. március 2. <https://www.pcworld.com/article/3040157/qualcomm-fined-in-the-us-over-china-corruption-allegations.html>.
- "A hírszerzési patológiák kockázatai Dél-Koreában". Ázsia, 259. jelentés. International Crisis Group. 2014. augusztus 5. <https://www.crisisgroup.org/asia/north-east-asia/korean-peninsula/risks-intelligence-pathologies-south-korea>.
- Roberts, Peter és Sidharth Kaushal. "Versenyelőny és szabályok a tartós versenyben". Occasional Papers. RUSI. April 29, 2020. <https://www.rusi.org/publication/occasional-papers/competitive-advantage-and-rules-persistent-competitions>.
- Rodrik, Dani. "Az amerikai és kínai jellemzőkkel bíró kapitalizmus békésen együtt tud létezni - ha lemondunk a 'hiperglobalizmusról'". Comment-Opinion. *South China Morning Post*, 2019. április 12. <https://www.scmp.com/comment/insight-opinion/article/3005674/capitalism-us-and-chinese-characteristics-can-peacefully>.
- Rodrik, Dani. "A globalizáció rossz irányba fordult és hogyan ártott Amerikának". *Foreign Affairs* 98, no. 4 (2019. július/augusztus): 26-33. https://drodrik.scholar.harvard.edu/files/dani-rodrik/files/globalizations_wrong_turn.pdf.

- Rogers, James, Andrew Foxall, Matthew Henderson, Sam Armstrong, Gisela Stuart, Michael Danby, Andrew Hastie, Peter Mackay, Marco Rubio és Bob Seely. "A kínai ellátási lánc megtörése: Hogyan tud az "öt szem" függetleníteni a stratégiai függőségtől". Fehér könyv. Henry Jackson Society. Május 2020. <https://henryjacksonsociety.org/wp-content/uploads/2020/05/Breaking-the-China-Chain-Chain-Chain.pdf>.
- Rosenberg, Mark Y. "A szakértők tévednek a többpólusúsággal kapcsolatban". *Foreign Policy*, 2019. június 24. <https://foreignpolicy.com/2019/06/24/experts-get-multipolarity-all-wrong/>.
- Rosenberg, Matt. "A világ országainak száma". Földrajz. *ThoughtCo*. DotDash Publishing Company, 2020. február 27. <https://www.thoughtco.com/number-of-countries-in-the-world-1433445>.
- Samuel, Juliet. "Bocs Boris, Franciaország megmutatja, hogy mégis van alternatíva a Huawei-nek". Hírek. *The Telegraph*, február 2020. <https://www.telegraph.co.uk/news/2020/02/01/sorry-boris-france-shows-alternative-huawei/>.
- Sandle, Paul és Jack Stubbs. "Dacolva Trumppal, a brit Johnson nem tiltja meg a Huawei-t az 5G-től". Technológiai hírek. *Reuters*, 2020. január 27. <https://www.reuters.com/article/us-britain-usa-huawei/defying-trump-uks-johnson-refuses-to-ban-huawei-from-5g-idUSKBN1ZR02G>.
- Sanger, David E. és Nicole Perloth. "Az NSA által feltört kínai szerverek biztonsági fenyegetésnek számítanak." Asia Pacific. *The New York Times*, 2014. március 22. <https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?partner=rss&emc=rss&r=1>.
- Sanger, David E. és David McCabe. "A Huawei nyeri a vitát Európában, miközben az Egyesült Államok botladozik az alternatívák kidolgozásában". Politika. *The New York Times*, 2020. február 17. <https://www.nytimes.com/2020/02/17/us/politics/us-huawei-5g.html>.
- Sanger, David E. és Nicole Perloth. "U.S. Accuses North Korea of Cyberattacks, a Sign of Deterrence is Failing." (Az USA kibertámadásokkal vádolja Észak-Koreát, ami annak a jele, hogy az elrettentés kudarcot vall.) Asia Pacific. *The New York Times*, 2020. április 15. <https://www.nytimes.com/2020/04/15/world/asia/north-korea-cyber.html>.
- Satariano, Adam. "Nagy-Britannia szembeszáll Trump kérésével, hogy tiltsa ki a Huawei-t az 5G hálózattól." Technológia. *The New York Times*, 2020. január 28. <https://www.nytimes.com/2020/01/28/technology/britain-huawei-5g.html>.

- Schaake, Marietje és Mathias Vermeulen. "A kiberbiztonság értékalapú európai külpolitikája felé". *Journal of Cyber Policy* 1, no. 1 (2016): 75-84.
<https://doi.org/10.1080/23738871.2016.1157617>.
- Schiavenza, Matt. "Kína dominanciája a feldolgozóiparban - egy táblázatban." Kína. *The Atlantic*, 2013. augusztus 5. <https://www.theatlantic.com/china/archive/2013/08/china-dominance-in-manufacturing-in-one-chart/278366/>.
- Schmitz Jr., James A. "The Cost of Monopoly: A New View" (A monopólium költségei: új nézőpont). Cikk. Federal Reserve Bank of Minneapolis, 2016. július 12.
<https://www.minneapolisfed.org/article/2016/the-costs-of-monopoly-a-new-view>.
- Schneier, Bruce. "Nem Kína az egyetlen probléma az 5G-vel". Érv. *Foreign Policy*, 2020. január 10. <https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/>.
- Schneider Jr, William. "Miért nagy dolog az 5G a világ hadseregei számára". Vélemény. *C4ISRNET*, 2019. február 5. <https://www.c4isrnet.com/opinion/2019/02/05/why-5g-is-a-big-deal-for-militaries-throughout-the-world/>.
- Schousboe, Laura. "A forradalmi védelmi technológiáról való írás buktatói". Commentary. *War on the Rocks*, 2019. július 15. <https://warontherocks.com/2019/07/the-pitfalls-of-writing-about-revolutionary-defense-technology/>.
- Seaman, John. (Szerkesztő.). "Covid-19 és Európa kínai kapcsolatai: A Country-Level Analysis." Különjelentés. European Think-Tank Network on China. Francia Nemzetközi Kapcsolatok Intézete. April 29, 2020. <https://merics.org/en/report/covid-19-and-europe-china-relations>.
- "Keresés: Huawei Cyber Security Evaluation Centre Oversight Board". Gov.uk. Hozzáférés 2020. március 30.
<https://www.gov.uk/search/all?keywords=%22Huawei+Cyber+Security+Evaluation+Centre+Oversight+Board%22&order=relevance>.
- Sears, Nathan A. "Kína, Oroszország és a hosszú 'egypólusú pillanat': How Balancing Failures are Actually Extending US Hegemony" (Hogyan bővítik ki az USA hegemoniáját a kiegyensúlyozás kudarcai). *The Diplomat*, 2016. április 27.
<https://thediplomat.com/2016/04/china-russia-and-the-unipolar-moment/>.

- "Security-by-Design keretrendszer verzió: 1.0." Szingapúri Kiberbiztonsági Ügynökség.
Hozzáférés: 2019. július 20. https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/security_by_design_framework.pdf.
- Seely, Bob, Peter Varnish Obe és John Hemmings. "Adataink védelme: Huawei, 5G és az öt szem". Ázsiai Tanulmányok Központja. Henry Jackson Society. May 2019.
<https://henryjacksonsociety.org/wp-content/uploads/2019/05/HJS-Huawei-Report-A1.pdf>.
- Shi, Wei. "A Nokia márkájú telefonok személyes adatokat küldtek Norvégiából Kínába". Hírek. *Telecoms.com*, 2019. március 22. <https://telecoms.com/496471/nokia-branded-phones-sent-personal-data-from-norway-to-china/>.
- Shi, Wei. "A HMD Finnországba költözteti a Nokia telefonok felhasználói adatainak tárolását." Hírek. *Telecoms.com*, 2019. június 19. <https://telecoms.com/498007/hmd-moves-nokia-phone-user-data-storage-to-finland/>.
- Shipman, Tim. "Ben Wallace interjú: Wallace: Nem támaszkodhatunk az USA-ra." News. *The Sunday Times*, 2020. január 12. https://www.thetimes.co.uk/edition/news/ben-wallace-interview-we-cant-rely-on-us-pmwgcgv398?wgu=270525_54264_15817040629028_276d8c4cf9&wgexpiry=1589480062&utm_source=planit&utm_medium=affiliate&utm_content=22278.
- Silver, Laura, Kat Devlin és Christine Huang. "Kína gazdasági növekedése többnyire üdvözlendő a feltörekvő piacokon, de a szomszédok óvakodnak a befolyásától". Pew Research Center: Global Attitudes and Trends. The Pew Charitable Trusts, 2019. december 5. <https://www.pewresearch.org/global/2019/12/05/chinas-economic-growth-mostly-welcome-in-emerging-markets-but-neighbors-wary-of-its-influence/>.
- Simpson, David. "FCC Fehér Könyv: Cybersecurity Risk Reduction." Jelentés. Közbiztonsági és belbiztonsági iroda - Szövetségi Hírközlési Bizottság. Január 18, 2017. <https://www.fcc.gov/document/fcc-white-paper-cybersecurity-risk-reduction>.
- Smeets, Max. "A kiberparancsnokság stratégiája súrlódást kockáztat a szövetségeseikkel." Kiberbiztonság és elrettetés. *Lawfare*, 2019. május 28.
<https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies>.

Smith, Julianne és Garima Mohan. "A válságban a botladozó Amerika megerősíti Európa legrosszabb félelmeit". Kommentár. *War on the Rocks*, április 23., <https://warontherocks.com/2020/04/in-a-crisis-a-fumbling-america-confirms-europes-2020-worst-fears/>.

Smith, Norman. "Huawei: a kormány szavazást nyert a hátsó padosorok lázadása után". Politika. *BBC News*, 2020. március 10. <https://www.bbc.com/news/uk-politics-51806704>.

Soderpalm, Helana és Olof Swahnberg. "'Az Ericsson elbocsátotta a dolgozókat50 az alábbiakat követően

U.S. Corruption Probe." Üzleti hírek. *Reuters*, 2018. október 18. <https://www.reuters.com/article/us-ericsson-probe/ericsson-has-dismissed-50-employees-following-u-s-corruption-probe-idUSKCN1MS1R4>.

Solon, Olivia. "Az iPhone Spyware lehetővé teszi a rendőrség számára, hogy a gyanúsítottak jelszavait naplózza, ha a feltörés nem működik." Tech-Security. *NBC News*, 2020. május 18. <https://www.nbcnews.com/tech/security/iphone-spyware-lets-cops-log-suspects-passcodes-when-cracking-doesn-n1209296>.

Soo, Zen, Zheping Huang, Sarah Dai és Li Tao. "SCMP sorozat: A csata az 5G-ért." *South China Morning Post*, 2019. február-június. <https://series.scmp.com/5g/>.

"Különszám: Különszám: Összehasonlító iparpolitika és kiberbiztonság." *Journal of Cyber Policy* no3., 3 (2018): 287-469. <https://www.tandfonline.com/toc/rcyb20/3/3>.

Statt, Nick. "Az USA a Huawei 5G alternatívájának kiépítésére ösztönzi a technológiai és távközlési iparágakat". Policy. *The Verge*, 2020. február 5. <https://www.theverge.com/2020/2/5/21124888/us-5g-huawei-white-house-trump-china-alternative-telecom-standard>.

Stecklow, Steve. "Exkluzív: Huawei szerepe a tiltott amerikai felszerelések Iránba szállításában." Technology News. *Reuters*, 2020. március 2. <https://www.reuters.com/article/us-huawei-iran-sanctions-exclusive/exclusive-newly-obtained-documents-show-huawei-role-in-shipping-prohibited-u-s-gear-to-iran-idUSKBN20P1VA>.

Suciu, Peter. "Tom Cotton megpróbálja megakadályozni az F-35-ösök telepítését az Egyesült Királyságba (a Huawei aggodalmai miatt)". Blog-The Buzz. *The National Interest*, 2020. május 8. <https://nationalinterest.org/blog/buzz/tom-cotton-trying-block-f-35-deployment-uk-due-huawei-worries-152251>.

Sullivan, James és Rebecca Lucas. "5G kiberbiztonság: A Risk Management Approach." The Globalisation of Technology Occasional Paper. RUSI. 2020. február 14.
<https://rusi.org/publication/occasional-papers/5g-cyber-security-risk-management-megközelítés>.

"Ellátási lánc kockázatkezelés." A Nemzeti Kémelhárítási és Biztonsági Központ. A Nemzeti Hírszerzés Igazgatójának Hivatala. Hozzáférés 2020. március 15. <https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats>.

Sutherland, Ewan. "Az USA kontra ZTE különös esete: vádemelés, betiltás, bírság és elnöki beavatkozás". *Digital Policy, Regulation and Governance* 21, no. 6 (2019): 550-573.
<https://doi.org/10.1108/DPRG-04-2019-0029>. <https://doi.org/10.1108/DPRG-04-2019-0029>.

Swaine, Michael D. "Egy kapcsolat extrém kényszer alatt: Kína és az Egyesült Államok kapcsolatai válaszüton." The Carter Center, 2019. január 16.
<https://www.cartercenter.org/resources/pdfs/peace/china/china-program-2019/swaine.pdf>.

Taylor, Trevor és Rebecca Lucas. "A kiberbiztonság kezelése a védelmi ellátási láncokban". *RUSI News Brief*, 2020. április 24. <https://www.rusi.org/publication/rusi-newsbrief/management-cyber-security-defence-supply-chains>.

Telegraph riporterek. "Donald Trump korlátozhatja az amerikai hírszerzés megosztását az Egyesült Királysággal, ha Nagy-Britannia nem tiltja be a Huawei-t". Technológiai hírszerzés. *The Telegraph*, 2019. május 31.
<https://www.telegraph.co.uk/technology/2019/05/31/donald-trump-could-limit-sharing-us-intelligence-uk-britain/>.

Thayer, Bradley A. és John M. Friend. "A világ Kína szerint: A világ megértése, amelyet Kína 2049-re, a KNK 100. születésnapjára szeretne létrehozni". *The Diplomat*, október 3, 2018. <https://thediplomat.com/2018/10/the-world-according-to-china/>.

"A prágai javaslatok." A Cseh Köztársaság kormánya. March 5, 2019.
<https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/>.

"Az Egyesült Államok hadseregének kibertéri műveleti koncepciójának 2016-2028-as képességterve". TRADOC Pamphlet 525-7-8. A hadügyminisztérium. 2010. február 22. <https://fas.org/irp/doddir/army/pam525-7-8.pdf>.

- Thompson, Loren. "A Qualcomm trösztellenes ügy messzemenő nemzetbiztonsági aggályokat vet fel". *Business. Forbes*, 2020. január 28.
<https://www.forbes.com/sites/lorenthompson/2020/01/28/qualcomm-antitrust-case-raises-far-reaching-national-security-concerns/#1d9399f669ea>.
- Ting-Fang, Cheng és Lauly Li. "Chip Titan TSMC Caught in Crossfire between US and China." *Business-Company in Focus. Nikkei Asian Review*, 2020. május 15.
<https://asia.nikkei.com/Business/Company-in-focus/Chip-titan-TSMC-caught-in-crossfire-between-US-and-China>.
- Tisdale, Susan M. "Kiberbiztonság: Kihívások a rendszerek, a komplexitás, a tudásmenedzsment és az üzleti intelligencia szemszögéből". *Issues in Information Systems* no16., 3 (2015): 191-198. https://iacis.org/iis/2015/3_iis_2015_191-198.pdf.
- Tisdale, Susan M. "Architecting a Cybersecurity Management Framework" (A kiberbiztonsági irányítási keretrendszer felépítése). *Issues in Information Systems* 17, no. 4 (2016): 227-236. https://iacis.org/iis/2016/4_iis_2016_227-236.pdf.
- Townsend, Will. "Ki a "valódi" vezető a mobil 5G-ben, 6. rész: politika, szabályozás és konzorciumok". *Forbes*, 2019. október 12.
<https://www.forbes.com/sites/moorinsights/2019/10/12/who-is-really-leading-in-mobile-5g-part-6-policy-regulation-and-consortia/#6f08dff2755>.
- Trump, Donald J. "Végrehajtási rendelet az információs és kommunikációs technológiák és szolgáltatások ellátási láncának biztosításáról". Végrehajtási rendeletek - Infrastruktúra és technológia. A Fehér Ház. May 15, 2019. <https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/>.
- Trump, Donald J. "Nemzeti stratégia az Amerikai Egyesült Államok 5G-jének biztosítására". A Fehér Ház. Március 2020. <https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf>.
- Turner Lee, Nicol. "Navigálás az amerikai-kínai 5G versenyben". Jelentés. Globális Kína. The Brookings Institution. April 2020. <https://www.brookings.edu/research/navigating-the-us-china-5g-competition/>.
- Tzogopoulos, George N. "Coronavírus, biztonság és a kiberrend." *Perspectives Papers. Begin-Sadat Stratégiai Tanulmányok Központja*. April 21, 2020.
<https://besacenter.org/perspectives-papers/coronavirus-security-and-the-cyber-order/>.

"Az Egyesült Királyság telekommunikációs ellátási láncának felülvizsgálati jelentése." Értesítés. Digitális, Kulturális, Média- és Sportminisztérium. HM Government. 2019. július 22. <https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-hivatkozás>.

Amerikai kibertér-szolárium bizottság. Elnökei Angus King és Mike Gallagher. "Jelentés." Amerikai Kongresszus. Március 11., 2020. <https://www.solarium.gov/report>.

Vaswani, Karishma. "Huawei: Egy ellentmondásos vállalat története". *BBC News*, Március 6, 2019. <https://www.bbc.co.uk/news/resources/idt-sh/Huawei>.

Venard, Bertrand. "A Siemens hatalmas korrupciós botrányának tanulságai egy évtizeddel később". *Gazdaság + Üzlet. The Conversation*, 2018. december 13. <https://theconversation.com/lessons-from-the-massive-siemens-corruption-scandal-one-decade-later-108694>.

Voo, Julia és Cindy Gao. "USA-Kína kiberverseny és együttműködés Julia Voo-val". Joanna Chiu. Podcasts-NuVoices. *SupChina*, 2020. április 3. Audio, 54m:33s. <https://supchina.com/podcast/u-s-china-cyber-competition-and-cooperation-with-julia-voo/>.

Weber, Valentin. "A technológiai befolyási szférák értelmezése". Stratégiai frissítések. LSE IDEAS. 2020. március 31. <http://www.lse.ac.uk/ideas/publications/updates/technological-spheres-of-influence>.

Weiss, Jessica Chen. "A digitális tekintélyelvűség megértése és visszaszorítása". Commentary. *War on the Rocks*, 2020. február 17. <https://warontherocks.com/2020/02/understanding-and-rolling-back-digital-authoritarianism/>.

Wheeler, Tom és Robert D. Williams. "A Huawei hardverének az Egyesült Államokon kívül tartása nem elég az 5G biztonságához". Huawei. *Lawfare*, 2019. február 20. <https://www.lawfareblog.com/keeping-huawei-hardware-out-us-not-enough-secure-5g>.

Wheeler, Tom. "5G öt (nem is olyan) egyszerű darabban". Jelentés. The Brookings Institution. Július 9. 2019. <https://www.brookings.edu/research/5g-in-five-not-so-easy-pieces/>.

Wheeler, Tom és David Simpson. "Miért igényel az 5G új megközelítést a kiberbiztonsághoz: A 21st. század legfontosabb hálózatának védelméért folytatott verseny." Jelentés. The Brookings Institution. September 3, 2019. <https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/>.

- Wheeler, Tom. "A "titkos szósztól" az 5G nyílt szabványok felé való elmozdulás". TechTank. The Brookings Institution. February 18, 2020.
<https://www.brookings.edu/blog/techtank/2020/02/18/moving-from-secret-sauce-to-open-standards-for-5g/>.
- "Miért fontos a verseny és a fogyasztóvédelem". Nemzetközi Kereskedelmi és Áruügyi Tanszék - Versenyjog. Az Egyesült Nemzetek Kereskedelmi és Fejlesztési Konferenciája. Hozzáférés 2020. április 17.
<https://unctad.org/en/Pages/DITC/CompetitionLaw/why-competition-matters.aspx>.
- Widener, Laura. "Trump azt mondja: 'Megszakíthatnánk az egész kapcsolatot' Kínával; a lehetőségek között". *American Military News*, 2020. május 14.
<https://americanmilitarynews.com/2020/05/trump-says-we-could-cut-off-whole-relationship-with-china-among-opciók/>.
- Williams, Darrell. "Az amerikai logisztikai főnök az ellátási láncot fenyegető kockázatokról és a védelmi intézkedésekről beszél". Jill Aitoro. Interjúk. *DefenseNews*, 2019. október 28.
<https://www.defensenews.com/interviews/2019/10/28/us-logistics-boss-talks-risks-to-the-supply-chain-and-protective-measures/>.
- Wilson, Clay és Nicole Drumhiller. "USA-Kína kapcsolatok: Kiberkémkedés és kulturális elfogultság." In: *Nemzetbiztonság és kémelhárítás a kiberkémkedés korában*, szerkesztette: Eugenie de Silva, 28-47. Hershey, PA, USA: Information Science Reference, 2016.
- Wong, Catherine. "A Thuküdidész-csapda szerzője, Graham Allison szerint Kínának és az USA-nak együtt kell működnie, és nem szabad háborúhoz vezető útra térnie." Diplomacy. *South China Morning Post*, 2018. december 20.
<https://www.scmp.com/news/china/diplomacy/article/2178905/thucydides-trap-author-says-china-and-us-must-work-together-and>.
- Woo, Stu és Dustin Volz. "Az USA fontolgatja, hogy a hazai használatra szánt 5G berendezéseket Kínán kívül kell gyártani." Tech. *The Wall Street Journal*, 2019. június 23. <https://www.wsj.com/articles/u-s-considers-requiring-5g-equipment-for-domestic-use-be-made-outside-china-11561313072>.
- Wu, Tim. "Az oligopólium problémája." *Annals of Technology*. *The New Yorker*, 2013. április 15. <https://www.newyorker.com/tech/annals-of-technology/the-oligopoly-problem>.

- X., Z. (szerkesztő). "A norvég Telenor azt mondja, hogy továbbra is a Huawei berendezéseit használja az 5G-hez". *XinHuaNet*, 2019. december 14.
http://www.xinhuanet.com/english/2019-12/14/c_138631613.htm.
- Xinbo, Wu. "Az Egyesült Államok biztonságpolitikája Ázsiában: A kínai-amerikai kapcsolatokra gyakorolt hatásai." Jelentés. The Brookings Institution. September 1, 2000. <https://www.brookings.edu/research/u-s-security-policy-in-asia-implications-for-china-u-s-relations/>.
- Yang, Heekyong. "A Samsung felállítja a korrupcióellenes testületet, mivel a vezetője perrel néz szembe." Technology News. *Reuters*, 2020. január 8.
<https://www.reuters.com/article/us-samsung-group-compliance/samsung-sets-up-anti-corruption-panel-as-chief-faces-trials-idUSKBN1Z80DR>.
- Yap, Chuin-Wei, Dan Strumpf, Dustin Volz, Kate O'Keeffe és Aruna Viswanatha. "A Huawei évek óta tartó felemelkedése tele van lopás és kétes etika vádjaival." Tech. *The Wall Street Journal*, 2019. május 25. <https://www.wsj.com/articles/huaweis-years-long-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858>.
- Yap, Chuin-Wei. "Az állami támogatás segítette a Huawei globális felemelkedését." Tech. *The Wall Street Journal*, 2019. december 25. <https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736>.
- Yu, Eileen. "Huawei: Könnyebb megvesztegetni a távközlési cégek munkatársait, mint hátsó ajtókat építeni." Blog-By the Way. *ZDNet*, 2019. október 23.
<https://www.zdnet.com/article/huawei-easier-to-bribe-telco-staff-then-build-backdoors/>.
- Zacks, Aviva. "Mi az a hátsó ajtó és hogyan védekezhetünk ellene." Blog. Biztonsági nyomozók. September 2, 2018. <https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/>.
- Zenko, Micah. *Vörös csapat: Hogyan lehetsz sikeres, ha úgy gondolkodsz, mint az ellenség*. New York: Basic Books, 2015.
- Zetter, Kim. "A támadók tanúsítványt loptak a Foxconn-tól, hogy Duqu 2.0-val feltörjék a Kaspersky-t." *WIRED*, június 15, <https://www.wired.com/2015/06/foxconn-hack-kaspersky-duqu-2/2015..>
- Zhou, Amy. "Huawei vagy az autópálya." Világ. *Harvard Political Review*, március 15, 2020. <https://harvardpolitics.com/world/huawei-or-the-highway/>.

Zibreg, Christian. "Korrupst Apple-menedzser, aki megrendelési titkokat szivárogtatott ki ázsiai beszállítóknak, bíróság elé került". Apple. *Geek.com*, 2010. augusztus 16.
<https://www.geek.com/apple/corrupt-apple-manager-who-leaked-order-secrets-to-asian-suppliers-brought-to-justice-1277412/>.

Zoellick, Robert B. "Lehet-e Amerika és Kína érdekelt felek?". Átirat - USA-Kína Üzleti Tanács. The Carnegie Endowment for International Peace, 2019. december 4.
<https://carnegieendowment.org/2019/12/04/can-america-and-china-be-stakeholders-pub->
<https://carnegieendowment.org/2019/12/04/can-america-and-china-be-stakeholders-pub->. [80510](#).

"ZTE." Hír-témák: Hírek. Korrupcióellenes összefoglaló. Hozzáférés
2020. március 3. <https://anticorruptiondigest.com/news-topics/zte/#axzz6Hk3lZgYv>.

Zweig, David és Siqin Kang. "Amerika kihívást jelent Kína nemzeti tehetségprogramjainak."
Jelentés.
CSIS. May 5, 2020. <https://www.csis.org/analysis/america-challenges-chinas-national-talent-programok>.