Independent Task Force Report No. 80

Confronting Reality in Cyberspace

Foreign Policy for a Fragmented Internet

Nathaniel Fick and Jami Miscik, *Chairs*
Adam Segal, *Project Director*
Gordon M. Goldstein, *Deputy Project Director*

ENDNOTES

1. Adam Satariano and Valerie Hopkins, “Russia, Blocked From the Global Internet, Plunges Into Digital Isolation,” *New York Times*, March 7, 2022, https://www.nytimes.com/2022/03/07/technology/russia-ukraine-internet-isolation.html; Joseph Menn, Ellen Nakashima, and Craig Timberg, “Lumen, a Second Major American Internet Carrier, Pulling Out of Russia,” *Washington Post*, March 8, 2022, https://www.washingtonpost.com/technology/2022/03/08/lumen-internet-russia-backbone-cut.

2. Adrian Shahbaz and Allie Funk, “Freedom on the Net 2021: The Global Drive to Control Big Tech,” Freedom House, September 21, 2021, https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech.

3. Gian M. Volpicelli, “The Draconian Rise of Internet Shutdowns,” *Wired*, February 9, 2021, https://www.wired.co.uk/article/internet-shutdowns; Access Now, *The Return of Digital Authoritarianism: Internet Shutdowns in 2021*, April 2022, https://www.accessnow.org/cms/assets/uploads/2022/04/2021-KeepItOn-Report-1.pdf.

4. BBC, “Ukraine Power Cut Was Cyber-Attack,” January 11, 2017, https://www.bbc.com/news/technology-38573074; Andy Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

5. Kate Conger, “Ukraine Says It Thwarted a Sophisticated Russian Cyberattack on Its Power Grid,” *New York Times*, April 12, 2022, https://www.nytimes.com/2022/04/12/us/politics/ukraine-russian-cyberattack.html; James Pearson, Raphael Satter, Christopher Bing, and Joel Schectman, “U.S. Spy Agency Probes Sabotage of Satellite Internet During Russian Invasion, Sources Say,” Reuters, March 11, 2022, https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/; CISA, FBI, Joint Cyber Adversary, “Destructive Malware Targeting Organizations in Ukraine,” CISA, March 1, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-057a; Gordon Corera, “Russia Hacked Ukrainian Satellite Communications, Officials Believe,” BBC, March 25, 2022, https://www.bbc.com/news/technology-60796079.

6. Tom Burt, “The Hybrid War in Ukraine,” *Microsoft on the Issues* (blog), April 27, 2022, https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks.

7. Alex Scroxton, “Conti Ransomware Syndicate Behind Attack on Irish Health Service,” *Computer Weekly*, May 17, 2021, https://www.computerweekly.com/news/252500905/Conti-ransomware-syndicate-behind-attack-on-Irish-health-service; Congressional Research Services, *Colonial Pipeline*: *The DarkSide Strikes*, May 11, 2021, https://crsreports.congress.gov/product/pdf/IN/IN11667; Jacob Bunge, “JBS Paid 11 Million to Resolve Ransomware Attack,” *Wall Street Journal,* June 9, 2021, https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781?mod=hp_lead_pos2; “Cyber Insurance Market Overview: Fourth Quarter 2021,” Marsh McLennan, 2021, https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-market-overview-q4-2021.html.

8. IT Army of Ukraine (@ITarmyUA), “Hackers all around the world: target #Belarus in the name of #Anonymous,” Twitter, February 28, 2022, https://twitter.com/ITarmyUA/status/1498287273581944843?s=20&t=fybBWPvIlxlNEnCm7ZD2ZA; Cyberknow, “2022 Russia-Ukraine War—Cyber Group Tracker,” Medium, February 27, 2022, https://cyberknow.medium.com/2022-russia-ukraine-war-cyber-group-tracker-6e08ef31c533.

9. Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert, *Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries*, Citizens Lab, September 18, 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries; Washington Post Staff, “Takeaways From the Pegasus Project,” *Washington Post*, August 2, 2021, https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project.

10. U.S. Cyberspace Solarium Commission, *A Warning From Tomorrow: Final Report*, March 11, 2020, https://www.solarium.gov.

11. Martin Matishak, “Biden Signs Cyber Incident Reporting Bill Into Law,” *The Record*, March 15, 2022, https://therecord.media/biden-signs-cyber-incident-reporting-bill-into-law.

12. Richard Lei, “Al Gore Takes a Spin on the Info Highway,” *Washington Post*, January 14, 1994, https://www.washingtonpost.com/archive/lifestyle/1994/01/14/al-gore-takes-a-spin-on-the-info-highway/2fa7774b-0cb4-45e2-87dc-dfe254001093; Michael L. Best and Keegan W. Wade, “The Internet and Democracy: Global Catalyst or Democratic Dud?” *Bulletin of Science, Technology, and Society* 29, no. 4 (2009): 255–56, doi: 10.1177/0270467609336304.

13. James A. Lewis, “Sovereignty and the Evolution of Internet Ideology,” Center for Strategic and International Studies, October 30, 2020, https://www.csis.org/analysis/sovereignty-and-evolution-internet-ideology; “Highlights of Clinton Speech on Internet Freedom,” Reuters, January 21, 2010, https://www.reuters.com/article/us-google-china-clinton-highlights/highlights-of-clinton-speech-on-internet-freedom-idUSTRE60K4R820100121.

14. European Union Parliament and Council of the European Union, “General Data Protection Regulation,” April 27, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679; EY Americas, “How To Prepare for Global Data Compliance,” EY, May 4, 2021, https://www.ey.com/en_us/consulting/how-to-prepare-for-global-data-compliance; Madalina Murariu, *Data Sharing Between the United States and European Union: Impact of the Schrems II Decision*, Belfer Center, July 2021, https://www.belfercenter.org/publication/data-sharing-between-united-states-and-european-union.

15. Foo Yun Chee, “EU Plans ‘Chip Act’ To Promote Semiconductor Self-Sufficiency,” Reuters, September 15, 2021, https://www.reuters.com/world/europe/tech-is-make-or-break-issue-eu-chief-executive-says-2021-09-15/.

16. “Versailles Declaration: Strengthening European Sovereignty and Reducing Strategic Dependencies,” March 11, 2022, https://www.consilium.europa.eu/media/54773/20220311-versailles-declaration-en.pdf.

17. Graham Webster, “A Brief History of the Chinese Internet,” *Logic*, May 1, 2019, https://logicmag.io/china/a-brief-history-of-the-chinese-internet; Qijia Zhou, “Building the (Fire) Wall: Internet Censorship in the United States and China,” *Harvard International Review*, December 28, 2020, https://hir.harvard.edu/building-the-fire-wall; Gary King, Jennifer Pan, and Margaret E. Roberts, “How Censorship in China Allows Government Criticism but Silences Collective Expression,” *American Political Science Review*, 107, no. 2 (2013): 1–18, https://j.mp/2nxNUhk.

18. Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia’s Digital Dictators and the New Online Revolutionaries* (New York: PublicAffairs, 2015); Nick Macfie and Alexander Marrow, “Russia Disconnects From Internet in Tests as It Bolsters Security,” Reuters, July 22, 2021, https://www.reuters.com/technology/russia-disconnected-global-internet-tests-rbc-daily-2021-07-22; Merrit Kennedy, “Russia’s ‘Sovereign Internet’ Law Gives Government Sweeping Power Over Internet,” NPR, November 1, 2019, https://www.npr.org/2019/11/01/775366588/russian-law-takes-effect-that-gives-government-sweeping-power-over-internet; Adam Satariano and Paul Mozur, “Russia Is Censoring the Internet, With Coercion and Black Boxes,” *New York Times*, October 22, 2021, https://www.nytimes.com/2021/10/22/technology/russia-internet-censorship-putin.html; Craig Timberg, Cat Zakrzewski, and Joseph Menn, “A New Iron Curtain Is Descending Across Russia’s Internet,” *Washington Post*, March 4, 2022, https://www.washingtonpost.com/technology/2022/03/04/russia-ukraine-internet-cogent-cutoff.

19. Jacob Berntsson and Maygane Janin, “Online Regulation of Terrorist and Harmful Content,” *Lawfare* (blog), October 14, 2021, https://www.lawfareblog.com/online-regulation-terrorist-and-harmful-content; Janosch Delcker, “Germany’s Balancing Act: Fighting Online Hate While Protecting Free Speech,” *Politico*, October 1, 2020, https://www.politico.eu/article/germany-hate-speech-internet-netzdg-controversial-legislation; Ashley Westerman, “‘Fake News’ Law Goes Into Effect in Singapore, Worrying Free Speech Advocates,” NPR, October 2, 2019, https://www.npr.org/2019/10/02/766399689/fake-news-law-goes-into-effect-in-singapore-worrying-free-speech-advocates.

20. Marianne Diaz Hernandez, Rafael Nunes, Felicia Anthonio, and Sage Cheng, “#KeepItOn Update: Who Is Shutting Down the Internet in 2021?,” Accessnow, June 7, 2021, https://www.accessnow.org/who-is-shutting-down-the-internet-in-2021; Peter Guest, “In the Dark: Seven Years, 60 Countries, 935 Internet Shutdowns: How Authoritarian Regimes Found an Off Switch for Dissent,” Rest of the World, April 26, 2022, https://restofworld.org/2022/blackouts.

21. Mehab Qureshi, “Decoding India’s Dubious Distinction as World’s ‘Internet Shutdown Capital,’” *Indian Express*, December 4, 2021, https://indianexpress.com/article/technology/tech-news-technology/india-ranks-highest-in-internet-suspensions-7654773.

22. “Blockchain Technologies Could Boost the Global Economy U.S.$1.76 Trillion by 2030 Through Raising Levels of Tracking, Tracing and Trust,” PwC, October 13, 2020, https://www.pwc.com/gx/en/news-room/press-releases/2020/blockchain-boost-global-economy-track-trace-trust.html.

23. Michael Chui, Mark Collins, and Mark Patel, “IoT Value Set to Accelerate Through 2030: Where and How to Capture It,” McKinsey & Company, November 9, 2021, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it.

24. Jack Goldsmith, “The Failure of Internet Freedom,” Knight Institute at Columbia University, June 13, 2018, https://knightcolumbia.org/content/failure-internet-freedom; Jack Goldsmith and Andrew Keane Woods, “Internet Speech Will Never Go Back to Normal,” *The Atlantic*, April 25, 2020, https://www.theatlantic.com/ideas/archive/2020/04/what-covid-revealed-about-internet/610549.

25. Adrian Shahbaz, “Freedom on the Net 2018: The Rise of Digital Authoritarianism,” Freedom House, October 2018, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism; Jessica Chen Weiss, “Understanding and Rolling Back Digital Authoritarianism,” *War on the Rocks*, February 17, 2020, https:// warontherocks.com/2020/02/understanding-and-rolling-back-digital-authoritarianism; Prak Chun Thul, “Cambodia Adopts China-style Internet Gateway Amid Opposition Crackdown,” Reuters, February 17, 2021, https://www.reuters.com/business/media-telecom/cambodia-adopts-china-style-internet-gateway-amid-opposition-crackdown-2021-02-17/.

26. Adam Segal, “Peering Into the Future of Sino-Russian Cyber Security Cooperation,” *War on the Rocks*, August 10, 2020, https://warontherocks.com/2020/08/peering-into-the-future-of-sino-russian-cyber-security-cooperation; Sino-Russian Cybersecurity Agreement art. 3, April 30, 2015, no. 788-p. https://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf; Luca Belli, “Cybersecurity Convergence in the BRICS Countries,” *Directions*, September 17, 2021, https://directionsblog.eu/cybersecurity-convergence-in-the-brics-countries.

27. “A Declaration for the Future of the Internet,” April 28, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf.

28. Matthew Slaughter and David McCormick, “Data Is Power,” *Foreign Affairs*, April 16, 2021, https://www.foreignaffairs.com/articles/united-states/2021-04-16/data-power-new-rules-digital-age.

29. A zettabyte is one sextillion bytes or 10^{21} (1,000,000,000,000,000,000,000).

30. WEF, “Shaping the Future of Digital Economy and New Value Creation,” accessed May 18, 2022, https://www.weforum.org/platforms/shaping-the-future-of-digital-economy-and-new-value-creation.

31. Eric Schmidt, Robert Work, et al., *Final Report: The Beginning of the Beginning* (Washington, D.C.: National Security Commission on Artificial Intelligence, 2021), https://www.nscai.gov/2021-final-report/.

32. Amy Zegart, “Intelligence Isn’t Just for Government Anymore,” *Foreign Affairs*, November 2, 2020, https://www.foreignaffairs.com/articles/united-states/2020-11-02/intelligence-isnt-just-government-anymore.

33. Lizhi Liu, “The Rise of Data Politics: Digital China and the World,” *Studies in Comparative International Development* 56, no. 1 (2021): 45–67, doi: 10.1007/s12116-021-09319-8.

34. “Opinion of the Central Committee of the Communist Party of China and the State Council on Building a More Perfect Market-Based Allocation System and Mechanism for Factors of Production,” April 9, 2020, http://www.gov.cn/zhengce/2020-04/09/content_5500622.htm; Rogier Creemers, Johanna Costigan, and Graham Webster, “Translation: Xi Jinping’s Speech to the Politburo Study Session on the Digital Economy—Oct. 2021,” DigiChina, January 28, 2022, https://digichina.stanford.edu/work/translation-xi-jinpings-speech-to-the-politburo-study-session-on-the-digital-economy-oct-2021.

35. Jake Sullivan, “Remarks at the National Security Commission on Artificial Intelligence Global Emerging Technology Summit,” White House press release, July 13, 2021, https://www.whitehouse.gov/nsc/briefing-room/2021/07/13/remarks-by-national-security-advisor-jake-sullivan-at-the-national-security-commission-on-artificial-intelligence-global-emerging-technology-summit.

36. Matt Burgess, “Ignore China’s New Data Privacy Law at Your Peril,” *Wired*, November 5, 2021, https://www.wired.com/story/china-personal-data-law-pipl; Jack Wagner, “China’s Cybersecurity Law: What You Need to Know,” *The Diplomat*, June 1, 2017, https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know.

37. Gary Clyde Hufbauer and Megan Hogan, “Digital Agreements: What’s Covered, What’s Possible,” Peterson Institute for International Economics policy brief, October 2021, https://www.piie.com/reader/publications/policy-briefs/digital-agreements-whats-covered-whats-possible.

38. White House, “Readout of President Biden’s Participation in the East Asia Summit,” October 27, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/27/readout-of-president-bidens-participation-in-the-east-asia-summit.

39. Joshua David, “Hackers Take Down the Most Wired Country in Europe,” *Wired*, August 21, 2007, https://www.wired.com/2007/08/ff-estonia/; Elisabeth Bumiller and Thom Shanker, “Panetta Warns of Dire Threat of Cyberattack on U.S.,” *New York Times*, October 11, 2012, https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

40. David Sanger, “Obama Ordered Wave of Cyberattacks Against Iran,” *New York Times*, June 1, 2012, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html; Thom Shanker and David Sanger, “U.S. Suspects Iran Was Behind a Wave of Cyberattacks,” *New York Times*, October 13, 2012, https://www.nytimes.com/2012/10/14/world/middleeast/us-suspects-iranians-were-behind-a-wave-of-cyberattacks.html; Peter Elkind, “Sony Pictures: Inside the Hack of the Century,” *Fortune*, June 25, 2016.

41. Neal Pollard, Adam Segal, and Matthew Devost, “Trust War: Dangerous Trends in Cyber Conflict,” *War on the Rocks*, January 16, 2018, https://warontherocks.com/2018/01/trust-war-dangerous-trends-cyber-conflict; Jacquelyn Schneider, “A World Without Trust,” *Foreign Affairs*, December 14, 2021, https://www.foreignaffairs.com/articles/world/2021-12-14/world-without-trust.

42. Director of National Intelligence, “Assessing Russian Activities and Intentions in Recent US Elections,” January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf; U.S. Department of Justice, “Report on the Investigation Into Russian Interference in the 2016 Presidential Election,” March 2019, https://www.justice.gov/archives/sco/file/1373816/download.

43. Dustin Voltz, “U.S. Spy Agency Warns That Chinese Hackers Target Military, Defense Industry,” *Wall Street Journal*, October 20, 2020, https://www.wsj.com/articles/u-s-spy-agency-warns-beijing-s-hackers-aiming-at-u-s-defense-industry-military-11603206459; Brian Naylor, “One Year After OPM Data Breach, What Has the Government Learned?,” NPR, June 6, 2016, https://www.npr.org/sections/alltechconsidered/2016/06/06/480968999/one-year-after-opm-data-breach-what-has-the-government-learned; Office of the National Counterintelligence Executive, “Foreign Spies Stealing U.S. Economic Secrets in Cyberspace,” October 2011, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf.

44. Kevin Mandia, “FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community,” FireEye, December 8, 2020, https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html; Gordon Corera, “China Accused of Cyber-Attack on Microsoft Exchange Servers,” BBC, July 19, 2021, https://www.bbc.com/news/world-asia-china-57889981.

45. Kim Parker, Juliana Menasce Horowitz, and Rachel Minkin, "How the Coronavirus Outbreak Has—and Hasn't—Changed the Way Americans Work," Pew Research Center, December 9, 2020, https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work; Dan Patterson, "Cybercrime Is Thriving During the Pandemic, Driven by Surge in Phishing and Ransomware," CBS News, May 19, 2021, https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic.

46. Ransomware Task Force, "Combatting Ransomware," Institute for Security and Technology, last updated September 23, 2021, https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf; Ellen Nakashima, "Cyber Command Has Sought to Disrupt the World's Largest Botnet, Hoping to Reduce Its Potential Impact on the Election," *Washington Post*, October 9, 2020, https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html; Javier Cordoba and Christopher Sherman, "Cyber Attack Causes Chaos in Costa Rica Government Systems," Associated Press, April 22, 2022, https://apnews.com/article/russia-ukraine-technology-business-gangs-costa-rica-9b2fe3c5a1fba7aa7010eade96a086ea.

47. Davis Hake and Vishaal Hariprasad, "Ransomware's Path to Product/Market Fit," *Net Politics* (blog), September 2, 2021, https://www.cfr.org/blog/ransomwares-path-productmarket-fit; Anthony M. Freed, "How Do Initial Access Brokers Enable Ransomware Attacks?" Cybereason, October 5, 2021, https://www.cybereason.com/blog/how-do-initial-access-brokers-enable-ransomware-attacks.

48. Patrick Howell O'Neill, "Wealthy Cybercriminals Are Using Zero-Day Hacks More Than Ever," *Technology Review*, April 21, 2022, https://www.technologyreview.com/2022/04/21/1050747/cybercriminals-zero-day-hacks.

49. WION Web Team, "Russia Responsible for 74% of Ransomware Attacks in World, Hackers Bagged $400mn in Crypto: Report," WION, last updated February 17, 2022, https://www.wionews.com/world/russia-responsible-for-74-of-ransomware-attacks-in-world-hackers-bagged-400mn-in-crypto-report-453867.

50. U.S. Department of the Treasury, "Treasury Takes Robust Actions to Counter Ransomware," news release, September 21, 2021, https://home.treasury.gov/news/press-releases/jy0364; Alexander Osipovich, "Global Regulators Back Tougher Rules to Prevent Criminals From Using Crypto," *Wall Street Journal*, October 28, 2021, https://www.wsj.com/articles/global-regulators-back-tougher-rules-to-prevent-criminals-from-using-crypto-11635413402?reflink=desktopwebshare_permalink; David Uberti, "How the FBI Got the Colonial Pipeline's Ransom Money Back," *Wall Street Journal*, June 11, 2021, https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981.

51. AJ Vicens, "Conti Ransomware Group Announces Support of Russia, Threatens Retaliatory Attacks," CyberScoop, February 25, 2022, https://www.cyberscoop.com/conti-ransomware-russia-ukraine-critical-infrastructure; Catalin Cimpanu, "Conti Ransomware Gang Chats Leaked by Pro-Ukraine Member," *The Record*, February 27, 2022, https://therecord.media/conti-ransomware-gang-chats-leaked-by-pro-ukraine-member.

52. C. Todd Lopez, "In Cyber, Differentiating Between State Actors, Criminals Is a Blur," U.S. Department of Defense, May 14, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur.

53. Kate Conger, "Hackers' Fake Claims of Ukrainian Surrender Aren't Fooling Anyone. So What's Their Goal?," *New York Times*, April 5, 2022, https://www.nytimes.com/2022/04/05/us/politics/ukraine-russia-hackers.html.

54. Margarita Levin Jaitner, "Russian Information Warfare: Lessons From Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015), https://ccdcoe.org/uploads/2018/10/Ch10_CyberWarinPerspective_Jaitner.pdf, quoted in Eric Rosenbach and Sue Gordon, "America's Cyber Reckoning," *Foreign Affairs*, December 14, 2021, https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning.

55. Quoted in Alyza Sebinius, "Cyber Command's Annual Legal Conference," *Lawfare* (blog), April 18, 2022, https://www.lawfareblog.com/cyber-commands-annual-legal-conference.

56. Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3(2017): 72–109, doi: 10.1162/ISEC_a_00267; Brandon Valeriano, "Does the Cyber Offense Have the Advantage?," Cato Institute, December 20, 2021, https://www.cato.org/commentary/does-cyber-offense-have-advantage.

57. Micah Musser and Ashton Garriott, "Machine Learning and Cybersecurity: Hype and Reality," Center for Security and Emerging Technology, June 2021, https://cset.georgetown.edu/publication/machine-learning-and-cybersecurity.

58. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2013).

59. Michael P. Fischerkeller and Richard Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2017): 381–93, doi: 10.1016/j.orbis.2017.05.003.

60. Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/2017): 44–71, doi: 10.1162/ISEC_a_00266.

61. U.S. Cyberspace Solarium Commission, *A Warning From Tomorrow*.

62. U.S. Cyber Command, "Achieve and Maintain Cyberspace Superiority," Cyber Command, 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

63. Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92, no. 1 (2019): 10–14, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1736950/a-cyber-force-for-persistent-operations.

64. Ellen Nakashima, "White House Authorizes Offensive Cyber Operations to Deter Foreign Adversaries," *Washington Post*, September 20, 2018, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

65. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636–2423 (2018), https://www.govinfo.gov/content/pkg/PLAW-115publ232/pdf/PLAW-115publ232.pdf.

66. Zach Dorfman et al., "Exclusive: Secret Trump Order Gives CIA More Powers to Launch Cyberattacks," Yahoo News, July 15, 2020, https://www.yahoo.com/video/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html.

67. Brad D. Williams, "CYBERCOM Has Conducted 'Hunt-Forward' Ops in 14 Countries, Deputy Says," *Breaking Defense*, November 10, 2021, https://breakingdefense.com/2021/11/cybercoms-no-2-discusses-hunt-forward-space-cybersecurity-china; Martin Matishak, "Cyber Command Sent a 'Hunt Forward' Team to Help Lithuania Harden Its Systems," *The Record*, May 4, 2022, https://therecord.media/cyber-command-sent-a-hunt-forward-team-to-help-lithuania-harden-its-systems.

68. Ellen Nakashima and Dalton Bennet, "A Ransomware Gang Shut Down After Cybercom Hijacked Its Site and It Discovered It Had Been Hacked," *Washington Post*, November 3, 2021, https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html.

69. AJ Vicens, "U.S. Cyber Command Shares New Samples of Suspected Iranian Hacking Software," CyberScoop, January 12, 2022, https://www.cyberscoop.com/u-s-cyber-command-iranian-hacking-malware-virustotal.

70. Mehul Srivastava et al., "The Secret U.S. Mission to Bolster Ukraine's Cyber Defenses Ahead of Russia's Invasion," *Financial Times*, March 9, 2022, https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471.

71. Julian Barnes, "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections," *New York Times*, October 23, 2018, https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html; Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

72. Christopher A. Ford "The Trouble With Cyber Arms Control," *New Atlantis*, no. 29 (Fall 2010): 52–67; Herb Lin, "Arms Control in Cyberspace: Challenges and Opportunities," *World Politics Review*, March 6, 2012.

73. United Nations Office for Disarmament Affairs, "Group of Governmental Experts," United Nations, accessed May 19, 2022, https://www.un.org/disarmament/group-of-governmental-experts.

74. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (July 22, 2015), https://undocs.org/A/70/174.

75. United Nations General Assembly, Resolution 70/237, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/70/237 (December 23, 2015), https://undocs.org/A/RES/70/237.

76. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/76/135 (July 14, 2021), https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf; Josh Gold, "Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?" *Net Politics* (blog), March 18, 2021, https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what.

77. Department of Justice, Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," press release no. 14-528, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor; Barack Obama and Xi Jinping, "Remarks by President Obama and President Xi Jinping of the People's Republic of China in Joint Press Conference," White House, September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

78. FireEye, "Red Line Drawn: China Recalculates Its Use of Cyber Espionage," June 2016, https://www.mandiant.com/media/11416/download; Daniel Paltiel, "G20 Communiqué Agrees on Language to Not Conduct Cyber Economic Espionage," Center for Strategic and International Studies, November 16, 2015, https://www.csis.org/blogs/strategic-technologies-blog/g20-communiqu%C3%A9-agrees-language-not-conduct-cyber-economic; "G7 Declaration on Responsible States Behavior in Cyberspace," Group of Seven, April 11, 2017, https://ccdcoe.org/uploads/2018/11/G7-170411-LuccaDeclaration-1.pdf.

79. Department of Justice, Office of Public Affairs, "Two Chinese Hackers Associated With the Ministry of State Security Charged With Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," press release no. 18-1673, December 20, 2018, https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion; Christopher Bing, Joseph Menn, and Jack Stubbs, "Inside the West's Failed Fight Against China's 'Cloud Hopper' Hackers," Reuters, June 26, 2019, https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper; Lucian Constantin, "'Five Eyes' Countries Attribute APT10 Attacks to Chinese Intelligence Service," *Security Boulevard*, December 21, 2018, https://securityboulevard.com/2018/12/five-eyes-countries-attribute-apt10-attacks-to-chinese-intelligence-service.

80. White House, "Imposing Costs for Harmful Foreign Activities by the Russian Government," April 15, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government; U.S. Department of the Treasury, "Treasury Sanctions Russia With Sweeping New Sanctions Authority," press release, April 15, 2021, https://home.treasury.gov/news/press-releases/jy0127; Kristen Eichensehr, "SolarWinds: Accountability, Attribution, and Advancing the Ball," Just Security, April 16, 2021, https://www.justsecurity.org/75779/solarwinds-accountability-attribution-and-advancing-the-ball.

81. Garret Hinck and Tim Maurer, “Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity,” *Journal of National Security Law & Policy* 10, no. 525 (2019–2020): 525–61, quoted in William Akoto, “Hackers for Hire: Proxy Warfare in the Cyber Realm,” Modern War Institute, January 31, 2022, https://mwi.usma.edu/hackers-for-hire-proxy-warfare-in-the-cyber-realm/.

82. Department of Justice, Office of Public Affairs, “Six Russian GRU Officers Charged in Connection With Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace,” press release no. 20-1117, October 19, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

83. Exec. Order No. 13694, “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,” 3 C.F.R. 13694 (2015), https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

84. Jason Bartlett and Megan Ophel, “Sanctions by the Numbers: Spotlight on Cyber Sanctions,” Center for a New American Security, May 4, 2021, https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber.

85. Exec. Order No. 14024, “Blocking Property With Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation,” 86 Fed. Reg. 73 (April 19, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/04/15/executive-order-on-blocking-property-with-respect-to-specified-harmful-foreign-activities-of-the-government-of-the-russian-federation.

86. Trevor Logan, “U.S. Should Indict and Sanction Cyber Adversaries,” Foundation for Defense of Democracies, February 27, 2019, https://www.fdd.org/analysis/2019/02/27/u-s-should-indict-and-sanction-cyber-adversaries.

87. Jared Cohen and Richard Fontaine, “Uniting the Techno-Democracies: How to Build Digital Cooperation,” *Foreign Affairs*, October 13, 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies; Martijin Rasser, “The Case for an Alliance of Techno-Democracies,” Observer Research Foundation, October 19, 2021, https://www.orfonline.org/expert-speak/the-case-for-an-alliance-of-techno-democracies.

88. Shinzo Abe, “Defeatism About Japan Is Now Defeated,” speech delivered at WEF, January 23, 2019, https://www.weforum.org/agenda/2019/01/abe-speech-transcript.

89. U.S. Department of Commerce, “Global Cross-Border Privacy Rules Declaration,” accessed May 19, 2022, https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

90. Jay Heisler, “Smaller Economies See Big Opportunities in Digital Trade Pact,” Voice of America, April 21, 2021, https://www.voanews.com/a/economy-business_smaller-economies-see-big-opportunities-digital-trade-pact/6204836.html.

91. Nigel Cory, “U.S. Options to Engage on Digital Trade and Economic Issues in the Asia-Pacific,” Information Technology and Innovation Foundation, February 8, 2022, https://itif.org/publications/2022/02/08/us-options-engage-digital-trade-and-economic-issues-asia-pacific.

92. Joshua P. Meltzer, “Why Schrems II Requires US-EU Agreement on Surveillance and Privacy,” Brookings TechStream, December 8, 2020, https://www.brookings.edu/techstream/why-schrems-ii-requires-us-eu-agreement-on-surveillance-and-privacy; Kenneth Propp, “Transatlanic Data Transfers: The Slow Motion Crisis,” Council on Foreign Relations, January 13, 2021, https://www.cfr.org/report/transatlantic-data-transfers; Matt Burgess, “Europe’s Move Against Google Analytics Is Just the Beginning,” *Wired*, January 19, 2022, https://www.wired.com/story/google-analytics-europe-austria-privacy-shield/?bxid=5bea07d724c17c6adf15204d&cndid=31936551.

93. White House, “Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework,” March 25, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework.

94. Paul Karp, “Australia and US Sign Cloud Act Deal to Help Law Enforcement Agencies Demand Data From Tech Giants,” *The Guardian*, December 15, 2021, https://www.theguardian.com/technology/2021/dec/16/australia-and-us-sign-cloud-act-deal-to-help-law-enforcement-agencies-demand-data-from-tech-giants.

95. Stewart Baker, “How Can the U.S. Respond to Schrems II?” *Lawfare* (blog), July 21, 2020, https://www.lawfareblog.com/how-can-us-respond-schrems-ii.

96. Department of Justice, Office of Public Affairs, “U.S. Leads Multi-National Action Against ‘Gameover Zeus’ Botnet and ‘Cryptolocker’ Ransomware, Charges Botnet Administrator,” press release no. 14-584, June 2, 2014, https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware; Andy Greenberg, “Cops Disrupt Emotet, the Internet’s ‘Most Dangerous Malware,’” *Wired*, January 27, 2021, https://www.wired.com/story/emotet-botnet-takedown.

97. U.S. Department of Treasury, “U.S. Department of the Treasury Announces Partnership With Israel to Combat Ransomware,” press release, November 14, 2021, https://home.treasury.gov/news/press-releases/jy0479.

98. Jonathan Hillman, *The Digital Silk Road: China’s Quest to Wire the World and Win the Future* (New York: HarperCollins, 2021); Council on Foreign Relations, *China’s Belt and Road: Implications for the United States* (New York: Council on Foreign Relations, 2021).

99. U.S. Cyberspace Solarium Commission, *A Warning From Tomorrow*.

100. “US, Australia and Japan to Fund Undersea Cable in the Pacific,” Reuters, December 11, 2021, https://www.voanews.com/a/us-australia-and-japan-to-fund-undersea-cable-in-the-pacific/6350792.html.

101. Annie Njanja, “Google Confirms $1B Investment Into Africa, Including Subsea Cable for Faster Internet,” *TechCrunch*, October 6, 2021, https://techcrunch.com/2021/10/06/google-confirms-1b-investment-into-africa-including-subsea-cable-for-faster-internet.

102. “CISA Director Says the LOG4J Security Flaw Is the ‘Most Serious’ She’s Seen in Her Career,” CNBC, December 16, 2021, https://www.cnbc.com/video/2021/12/16/cisa-director-says-the-log4j-security-flaw-is-the-most-serious-shes-seen-in-her-career.html.

103. Derek Johnson, “Chinese APT Leveraged Zero Days—Including Log4j—to Compromise U.S. State Governments,” *SC Magazine*, March 8, 2022, https://www.

scmagazine.com/analysis/application-security/chinese-apt-leveraged-zero-days-including-log4j-to-compromise-u-s-state-governments.

104. White House, “Readout of White House Meeting on Software Security,” January 13, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security.

105. Schmidt, Work, et al., *Final Report*.

106. White House, “Readout of AUKUS Joint Steering Group Meetings,” December 17, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/17/readout-of-aukus-joint-steering-group-meetings.

107. Director of National Intelligence, “Assessing Russian Activities and Intentions in Recent US Elections,” January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf; Select Comm. on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, S. Rep. No. 116-XX, vol. 1 (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf; Department of Homeland Security, “Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector,” January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

108. Michael Schmitt and Tim Maurer, “Protecting Financial Data in Cyberspace: Precedent for Further Progress on Cyber Norms?,” Just Security, August 24, 2017, https://www.justsecurity.org/44411/protecting-financial-data-cyberspace-precedent-progress-cyber-norms; Tim Maurer, Ariel Levite, and George Perkovich, “Toward a Global Norm Against Manipulating the Integrity of Financial Data,” Carnegie White Paper, March 27, 2021, https://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403.

109. Sarah Kreps and Jacquelyn Schneider, “Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics,” *Journal of Cybersecurity* 5, no. 1 (2019); Page O. Stoutland and Samantha Pitts-Kiefer, *Nuclear Weapons in the New Cyber Age: Report of Cyber-Nuclear Weapons Study Group*, Nuclear Threat Initiative, September 2018; James M. Acton, “Cyber Warfare & Inadvertent Escalation,” *Daedalus* 149, no. 2 (2020): 133–49.

110. Arms Control Association, “U.S. Nuclear Modernization Programs,” last updated January 2022, https://www.armscontrol.org/factsheets/USNuclearModernization; Erin D. Dumbacher and Page O. Stoutland, “U.S. Nuclear Weapons Modernization Security and Policy Implications of Integrating Digital Technology,” Nuclear Threat Initiative, November 2020, https://media.nti.org/documents/NTI_Modernization2020_FNL-web.pdf.

111. Kim Zetter, “When Russia Helped the U.S. Nab Cybercriminals,” Zero Day, November 30, 2021, https://zetter.substack.com/p/when-russia-helped-the-us-nab-cybercriminals.

112. James M. Acton, “Cyber Warfare & Inadvertent Escalation”; Rebecca K.C. Hersman, Eric Brewer, and Suzanne Claeys, “NC3: Challenges Facing the Future System,” Center

for International and Strategic Studies, July 9, 2020, https://www.csis.org/analysis/nc3-challenges-facing-future-system; George Perkovich and Ariel Levite, "How Cyber Ops Increase the Risk of Accidental Nuclear War," *DefenseOne*, April 21, 2021, https://www.defenseone.com/ideas/2021/04/how-cyber-ops-increase-risk-accidental-nuclear-war/173523.

113. Nicole Perlroth, *This is How They Tell Me the World Ends: The Cyber Weapons Arms Race* (New York: Bloomsbury, 2021).

114. Ellen Nakashima and Craig Timberg, "NSA Officials Worried About the Day Its Potent Hacking Tool Would Get Loose. Then It Did," *Washington Post*, May 16, 2017, https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.

115. Ari Schwartz and Rob Knake, *Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerabilities Equities Process* (Cambridge, MA: Belfer Center, 2016); Michael Daniel, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities," *White House Blog*, April 28, 2014, https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

116. *China's Capabilities for State-Sponsored Cyber Espionage: Testimony Before the U.S.-China Economic and Security Review Commission*, 117th Cong. (February 17, 2022) (statement of Kelli Vanderlee, Senior Manager, Strategic Analysis, Mandiant Threat Intelligence), https://www.uscc.gov/sites/default/files/2022-02/Kelli_Vanderlee_Testimony.pdf; Zeyi Yang, "Beijing Punishes Alibaba for Not Reporting Log4j Loophole Fast Enough," *Protocol*, December 22, 2021, https://www.protocol.com/bulletins/alibaba-cloud-log4j#.

117. Lily Hay Newman, "Hackers Are Getting Caught Exploiting New Bugs More Than Ever," *Wired*, April 21, 2022, https://www.wired.com/story/zero-day-exploits-vulnerabilities-google-mandiant.

118. Australian Signals Directorate, "Responsible Release Principles for Cyber Security Vulnerabilities," accessed May 20, 2022, https://www.asd.gov.au/responsible-release-principles-cyber-security-vulnerabilities; Communication Security Establishment, "CSE's Equities Management Framework," last updated March 11, 2019, https://cse-cst.gc.ca/en/information-and-resources/announcements/cses-equities-management-framework; National Cyber Security Centre, "Equities Process," November 29, 2018, https://www.ncsc.gov.uk/blog-post/equities-process; Marietje Schaake, *Software Vulnerability Disclosure in Europe: Technology, Policies, and Legal Challenges* (Brussels: CEPS, 2018), https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges.

119. Ellen Nakashima, "Cyber Command Has Sought To Disrupt the World's Largest Botnet, Hoping To Reduce Its Potential Impact on the Election," *Washington Post*, October 9, 2020, https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html; Andy Greenberg, "A Trickbot Assault Shows US Military Hackers' Growing Reach," *Wired*, October 14, 2020, https://www.wired.com/story/cyber-command-hackers-trickbot-botnet-precedent.

120. Ines Kagubare, “U.S., EU Cyber Investments in Ukraine Pay Off Amid War,” *The Hill*, March 13, 2022, https://thehill.com/policy/technology/597921-us-eu-cyber-investments-in-ukraine-pay-off-amid-war.

121. Amy Zegart, “The Weapon the West Used Against Putin,” *The Atlantic*, March 5, 2022, https://www.theatlantic.com/ideas/archive/2022/03/russia-ukraine-invasion-classified-intelligence/626557.

122. Michael Schmitt, “Three International Law Rules for Responding Effectively to Cyber Operations,” Just Security, July 13, 2021, https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations.

123. Dmitri Alperovitch, “The Case for Cyber Realism,” *Foreign Affairs*, December 14, 2021, https://www.foreignaffairs.com/articles/united-states/2021-12-14/case-cyber-realism.

124. Danny Palmer, “The FBI Removed Hacker Backdoors From Vulnerable Microsoft Exchange Servers. Not Everyone Likes the Idea,” *ZDNet*, April 19, 2021, https://www.zdnet.com/article/the-fbi-removed-hacker-backdoors-from-vulnerable-microsoft-exchange-servers-not-everyone-likes-the-idea.

125. National Initiative for Cybersecurity Education, “Cybersecurity Workforce Demand,” accessed May 20, 2022, https://www.nist.gov/document/workforcedemandonepager2021finalpdf.

126. White House, “Indo-Pacific Strategy of the United States,” February 2022, https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf.

127. Patrick Howell O’Neill, “Tillerson to Officially Eliminate Cyber Coordinator Office,” CyberScoop, August 29, 2017, https://www.cyberscoop.com/state-department-cyber-office-eliminated-rex-tillerson/; State Department, Establishment of the Bureau of Cyberspace and Digital Policy, April 4, 2022, https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy.

128. Suzanne Smalley, “State to Gain More Ability to Monitor DOD Cyber Ops Under White House Agreement,” CyberScoop, May 10, 2022, https://www.cyberscoop.com/state-to-gain-authorities-to-monitor-dod-cyber-ops-under-new-white-house-agreement.

129. Kevin Childs and Amy Zegart, “The Divide Between Silicon Valley and Washington Is a National-Security Threat,” *The Atlantic*, December 13, 2018, https://www.theatlantic.com/ideas/archive/2018/12/growing-gulf-between-silicon-valley-and-washington/577963.