High-Tech Friendly Fire: America's Technological Self-Sabotage in its Cold War with Beijing

Michael Sobolik

Three decades after winning the Cold War against the Soviet Union, the United States of America is locked in another twilight struggle with a different authoritarian regime. Many have accurately described the geopolitical dynamics between America and the Chinese Communist Party (CCP) as another cold war – one that is, in many ways, more complex than the last.[1] Even so, an abiding similarity is the centrality of technology. Throughout the second half of the twentieth century, American innovation led to superior weaponry that transformed the military domain and gave new political options to policymakers.[2] So it is in the twenty-first century. Although technological superiority is not a sufficient condition alone for victory, it remains a highly important one.

This reality separates the technological domain of the original Cold War from the U.S.-China competition today: unlike the Soviet Union, the People's Republic of China (PRC) has established market dominance in critical and emerging industries, from electric vehicles and biotechnology to telecommunications and unmanned aerial vehicles. Indeed, the U.S. government and policy experts have

Michael Sobolik is a senior fellow at Hudson Institute. He specializes in United States–China relations and great power competition with a focus on geopolitics, net assessments, and competitive strategies. He is the author of *Countering China's Great Game: A Strategy for American Dominance* (Naval Institute Press, 2024). Mr. Sobolik wrote this paper during his previous affiliation at the American Foreign Policy Council.

been warning private industry and the American people about CCP technological dominance, and the concomitant threats, for years.

Moreover, U.S. companies have knowingly and persistently handed critical technology to the CCP. Unlike the first Cold War between the United States and the Soviet Union, the ongoing competition between Washington and Beijing is marked by systemic economic integration. After all, U.S. companies enabled the PRC's internet access in the 1990s, and, importantly, built out the CCP's "Great Firewall" of censorship and surveillance. To be sure, decades of trade and investment enriched both nations, but they have also afforded considerable strategic advantages to the CCP. What started as largely PRC intellectual property theft eventually also morphed into willing technology transfer and U.S. compliance with PRC laws. U.S. firms have thus contributed—both unwittingly and in some cases willingly—to the technological development and dominance of America's greatest geopolitical and ideological adversary. The CCP leverages this advantage every day in ways that threaten critical U.S. interests and challenge American values in various industries and technologies, including commercial shipping, telecommunications and biotechnology. This reality also leaves the United States exposed to widespread technological sabotage in a moment of crisis. This paper will thus provide a series of concrete examples which all serve to highlight these troubling interconnections and growing vulnerabilities: from the sale of American-designed surveillance technologies or genetic mapping equipment to the Chinese state, to the ubiquity of ZPMC smart ship-to-shore cranes in American shipyards, and Huawei telecommunications infrastructure in proximity to sensitive US military installations.

"Imagine the Chaos": Turning the Lights Off in America

On September 17, 2024, the world witnessed the future of high-tech warfare play out in Lebanon. At 3:30 pm local time, hundreds of Hezbollah operatives received a notification on their pagers. The terrorist organization had recently downgraded their technological sophistication to avoid Israeli cyber penetration. In this instance, however, Israel was a step ahead of the Shi'ite militia. In what appears to have been a Mossad operation, the previously-rigged pagers detonated simultaneously across Lebanon, killing and injuring thousands of terrorists.[3]

The operation was remarkable in its discrimination and accuracy, but it also revealed a stunning Israeli infiltration of Hezbollah's supply chain. The pagers in question came from a Taiwanese company, but the manufacturing was outsourced to a Mossad-controlled facility in Israel. With remotely-detonated, undetectable explosives located in the pagers, Hezbollah operatives were carrying portable bombs in their pockets and backpacks for months.[4]

Some in America, however, sounded the alarm. "Look at the damage done by exploding pagers," warned former Congressman Mike Gallagher, "then imagine the chaos caused by haywire power grids, or the economic consequences of frozen ports." Of course, he was not referring to the Israeli-Iranian conflict. The former Chairman of the Select Committee on the Chinese Communist Party (CCP) was cautioning U.S. citizens that in the event of a future conflict, Beijing could throw their daily lives into unfathomable chaos. Blunting this threat, according to Gallagher, begins with an honest reckoning of the calculation of CCP General Secretary Xi Jinping: "He seeks a future where he could turn off the lights in Green Bay or Geneva knowing we could not do the same in Guangzhou."[5]

Policymakers must do more than grasp the scale and scope of these potential vulnerabilities. They must be more proactive, taking steps to mitigate and, wherever possible, eliminate them. Doing so, however, requires Americans to reckon with the origins of U.S. technological assistance to the CCP. The investments that leading American companies made in China three decades ago continue to haunt U.S. policymakers and the American people today.

With American Bricks: Building China's "Great Firewall"

The memory of the Tiananmen Square massacre on June 4, 1989 may be blocked within the People's Republic of China (PRC), but it is well-known in America and throughout the world. Even the most advanced censorship capabilities cannot erase the historical record. The account from the British embassy in Beijing was especially chilling: the People's Liberation Army (PLA) "ran over" civilians at 65 kilometers per hour "time and time again to make quote pie unquote," "collected [human bodies] by bulldozer," "incinerated [the remains] then hosed down drains," and "shot up" ambulances trying to save injured students.[6] To this day, the total number of casualties remains unknown. Most sources estimated a few thousand deaths, but some counts surpassed 10,000.[7]

There is one critical detail of the atrocity, however, that the West has memory-holed. Those the PLA couldn't kill immediately were subsequently rounded up and arrested with the aid of security cameras designed and manufactured by Pelco and Siemens Plessey—American and British tech companies, respectively.[8] At the time, international opprobrium of the CCP's response was nearly universal. Western governments suspended military assistance and temporarily halted high-level public diplomacy.

After a two-year hiatus, however, the West came back to Beijing. In particular, the World Bank funded the installation of the same security cameras that had tracked the Tiananmen protestors—only this time in Tibet, where the CCP was cracking down on Buddhism and sinicizing a region that was supposedly guaranteed semi-autonomy. The ostensible purpose for the cameras was traffic congestion, a problem with which Lhasa, Tibet's capital, had not previously struggled.[9]

The entire episode foreshadowed the posture that American companies and international institutions would adopt with regard to the CCP: elevate economic engagement over human rights concerns and prioritize monetary gain over strategic threats. U.S. corporations doubled down on this approach during the 1990s when they helped bring the People's Republic of China into the modern telecommunications age. Companies like AT&T provided rotary switches to PRC partners, only to discover that Chinese companies stopped purchases if surveillance components were not included.[10]

In AT&T's defense, this technology was the same capability the U.S. government relied on for lawful intercepts. Other companies, however, went far beyond American norms and helped the CCP build out its vast internet censorship capability. Colloquially called the "Great Firewall," this system operates at the PRC's borders and filters incoming internet traffic at fiber-optic choke points in Beijing, Shanghai, and Guangzhou.[11] According to journalist James Griffiths, "That the system works so well is in part thanks to U.S. corporations and engineers, particularly the Silicon Valley-based multinational Cisco, which began supplying filtering and surveillance equipment to Chinese censors in the early 1990s… In the words of internet historians Tim Wu and Jack Goldsmith, the Great Firewall was originally built 'with American bricks.'"[12]

Over time, however, Chinese companies shouldered their American competitors out of the market. China Telecom initially contracted with Sprint to build out the PRC's first commercial internet. After establishing U.S.-China internet connectivity and bringing dial-up access to various parts of the PRC, Sprint then moved to build a nation-wide network within China. Chinese scientists with PRC government backing, however, blocked Sprint and led the project.[13] The internet in China was built by American companies, but controlled by the Chinese Communist Party – and, importantly, maintained by PRC entities under the party's control.

As the CCP's economy grew, it replicated this playbook across critical industries by leveraging U.S. technology in ways that threatened American interests and challenged Western values. Telecommunications, commercial infrastructure, and biotechnology are particularly compromised – and American individuals and companies are largely to blame.

CCP-Controlled Cranes: Shutting Off U.S. Commerce

Founded in 1992, Chinese company Shanghai Zhenhua Port Machinery Co. (ZPMC) took merely six years to dominate the global market in ship-to-shore (STS) cranes. By virtue of underselling its competitors and hiring local advocates to build connections, ZPMC crowded out its competitors in short order. Low prices were worth initial issues with product quality, problems that the company seems to have largely overcome.

There was an additional element to ZPMC's shocking success: intellectual property theft. According to a *Los Angeles Times* report from 2002, "In Florida, a competitor accused ZPMC of stealing its design, and ZPMC's partner was indicted on unrelated corruption charges."[14] Nearly a decade later, *The Wire China* referenced an interview in which ZPMC founder Guan Tongxian admitted that ZPMC's early designs were largely borrowed from other firms.[15]

Questionable business practices did not stop ZPMC from dominating global markets, including the United States. ZPMC smart cranes line American ports in Seattle, Tacoma, Oakland, Los Angeles, Long Beach, Gulfport, Tampa Bay, Miami, Jacksonville, Charleston, Wilmington, Portsmouth, Philadelphia, and Elizabeth.[16] According to congressional estimates, ZMPC cranes account for 80% of ship-to-shore transfer capacity in U.S. ports. In 2020, the risk consulting group Pointe Bello warned of potential national security risks with a PRC state-owned company's presence in U.S. commercial networks: "Port equipment is embedded with digital components that integrate cranes into U.S. port digital infrastructure, creating surveillance capabilities and possible disruption vulnerabilities at U.S. strategic locations."[17] This concern is not without merit. ZPMC's primary shareholder, China Communications Construction Company, is primarily responsible for constructing the CCP's artificial atolls in the South China Sea. ZPMC crane-delivery ships also reportedly train with the People's Liberation Army in amphibious landing operations likely connected to a Taiwan scenario.[18]

In 2024, the House Select Committee on the Chinese Communist Party and the House Committee on Homeland Security released a joint investigation into ZPMC and issued the following warnings:

> ZPMC has repeatedly requested remote access to its STS cranes operating at various U.S. ports… If granted, this access could potentially be extended to other PRC government entities, posing a significant risk due to the PRC's national security laws that mandate cooperation with state intelligence agencies.[19]
>
> ZPMC and other PRC [state-owned enterprises] are not contractually barred from installing backdoors into equipment or modifying technology in ways that could allow unauthorized access or remote control, enabling them to compromise sensitive data or disrupt operations within the U.S. maritime sector at a later time.[20]
>
> In a potential future dispute with the United States over Taiwan, the PRC could restrict or manipulate the supply of critical components or materials essential to U.S. maritime infrastructure, including STS cranes. Such actions could severely disrupt U.S. commercial activities and hinder the DoD's ability to deploy supplies and resources to the Indo-Pacific region.[21]

The final warning is particularly ominous. American security analyst Ian Easton put it in even starker terms in 2022: "What if smart gantry cranes used to load and unload container ships at major port facilities refused to work? Or worse, what if they stacked containers in the wrong places, capsizing ships and snarling port traffic?"[22]

CCP-Controlled Networks: Compromised Operational Security

In 1983, Ren Zhengfei, a member of the PLA engineering corps, retired from military service. After brief employment at state-owned Shenzhen Electronics Corp., Ren left and founded Huawei with an $8.5 million loan from a state bank. By 1993, Huawei had secured a contract with the PLA and sourced indigenously-produced components directly to the army. The following year, Ren scored a meeting with Communist Party General Secretary Jiang Zemin and pushed him to close China's market to foreign telecommunications companies, a step that Jiang took in 1996. Thereafter, Huawei dominated the market in China by offering steep discounts and undercutting its competition, in some cases offering free services to government entities.

The venture was never primarily economic in nature. At one point Ren reportedly told Jiang Zemin "that switching equipment was related to international security, and that a nation that did not have its own switching equipment was like one that lacked its own military." According to Ren, China's paramount leader tersely replied, "Well said."[23]

Huawei set about targeting proven technologies and appropriating them. In 2003, Cisco executives accused Huawei of copying their routers and manuals. When confronted with this evidence, Ren casually responded, "Coincidence."[24] In 2010, Motorola brought a lawsuit against Huawei for stealing base station technology – something that Huawei employees had in fact done seven years prior.[25] In 2013, a Huawei employee absconded with a T-Mobile robotic arm used to test devices.[26] Even with prosecution from the Department of Justice, however, Huawei's market dominance was beginning to solidify. Aided by $3 billion in grants from the CCP and $25 billion in tax benefits from Beijing, Huawei surpassed Nokia and Erickson in 2015 as the world's leading provider of telecommunications equipment.[27]

In Europe, this reality introduced particularly grave national security concerns. In April 2019, the Washington Post reported that the U.S. Embassy in Germany had warned Berlin that Huawei's presence in German 5G networks "could in the future jeopardize nimble cooperation and joint mobilization, particularly in times of crisis."[28] The Department of State has relayed these concerns to Capitol Hill as well. After Britain announced its initial decision to limit Huawei equipment to the random access network, Senator Ted Cruz (R-TX) cautioned that doing so "will not succeed in limiting Huawei's ability to conduct espionage, interfere with critical infrastructure or mobilization, or even access more sensitive nodes in the telecom network."[29] Secretary of Defense Mark Esper echoed these assessments in testimony before the Senate Armed Services Committee in March 2020. "If our NATO allies incorporate Huawei technology," Esper noted, "it may very well have a severe impact on our ability to share information, to share intelligence, to share operational plans, and for the alliance to conduct itself as an alliance."[30]

Huawei infrastructure has the ability to detect early warning indicators of military mobilization, and could sabotage active operations in a host nation. These concerns are present in the United States as well. According to an FBI investigation, the location of rural Huawei equipment in America eerily coincides with military bases housing nuclear weapons.[31]

CCP-Dominated Biotechnology: Genocide At Home, Biowarfare Abroad

In 2021, the National Counterintelligence and Security Center (NCSC) previewed the promises of biotechnology. "Your DNA," the NSCS advised, "is the most valuable thing you own. It holds the most intimate details of your past, present and potential future—whether you are prone to addiction or high-risk for cancer. It is your unique genetic code and can enable tailored healthcare delivery to you."[32] This potential is already spreading beyond healthcare into agriculture, energy production, and warfighting. According to the National Security Commission on Emerging Biotechnology (NSCEB), "We can imagine a future in which our warfighters are fed, fueled, equipped, protected, and healed on the battlefield, all

thanks in part to biotechnology."[33] Such a future is not far off, and it is embedded within a human's unique genetic code.

It is for this exact reason that the NCSC also warned of biotechnology's perils: "Losing your DNA is not like losing a credit card. You can order a new credit card, but you cannot replace your DNA. The loss of your DNA not only affects you, but your relatives and, potentially, generations to come."[34] Unfortunately for Americans, the PRC has been collecting genetic information on Americans for years. Beijing's ultimate goal is not to cure longstanding diseases, but to develop new pressure points to silence, intimidate, and extort key individuals.[35] The CCP's ongoing genocide of Uyghurs in the PRC evinces Beijing's intent to leverage biotechnology for nefarious ends. By building a comprehensive DNA databank of Uyghurs, the CCP has built the capacity to locate, track, and apprehend Uyghurs around the world.[36]

Beijing, however, did not construct its impressive DNA repository alone. Thermo Fisher, a Massachusetts-based company, sold genetic-mapping equipment to government authorities in Xinjiang, the PRC territory where Uyghurs overwhelmingly live. According to a 2021 report from the *New York Times*, "The authorities there said in the documents that the machines were important for DNA inspections in criminal cases and had 'no substitutes in China.'"[37] When members of Congress and advocacy groups raised concerns about human rights, Thermo Fisher announced it would cut off future sales in Xinjiang.[38] Such a move, while commendable, risks overlooking the broader ways the CCP is leveraging biotechnology outside of the Uyghur region – and, indeed, outside of China.[39]

China's National Genebank is the most impressive of its kind. It is the manifestation of the CCP's quest to obtain DNA samples of humans around the world. The COVID-19 pandemic presented a ready-made opportunity to do so. According to the National Security Commission on Emerging Biotechnology, "The BGI Group, which has a demonstrated history of collaboration with the PRC military, collected massive amounts of genetic information from around the world" during the pandemic. "Stakeholders and U.S. Government officials note that it is difficult, if not impossible, to know how these data are being used and combined with other data by the PRC."[40] The risk of targeted diseases and tailored blackmail are well known but not well understood, given the technology's developmental stage. It appears, though, that the CCP is testing the possibility of biologically enhancing warfighters and developing mind-reading software to test ideological loyalty.[41]

Stemming the Tide

The three industries discussed here are representative of a broader strategic predicament facing the United States. What began as PRC companies stealing intellectual property from American competitors has morphed into a dynamic wherein Americans willingly hand over information to CCP-controlled entities in the form of joint ventures, commercial transactions, corporate acquisitions, and data transfers. That this problem has persisted and grown over thirty years suggests a widespread culture of myopia among U.S. companies that downplays geopolitical risk and overlooks complicity in human rights abuses.

It also reveals political unseriousness in Washington. Policymakers have been largely aware of these problems since 2015, when Ret. General Keith Alexander called Beijing's theft of American intellectual property "the single greatest transfer of wealth in history."[42] Governmental efforts to adjust market incentives and protect U.S. technology have not been lacking, but the requisite political will to enact and implement them has not yet fully materialized.

To be sure, policymakers have made limited gains. For instance, the U.S. Government and its closest allies and partners successfully blunted Huawei's dominance in next-generation telecommunications technology. Haphazardly enforced export controls on Huawei, however, have allowed the company to survive, retrench, and invest in new technologies that could threaten America's partners.[43] Moreover, Washington's efforts to "rip-and-

replace" legacy Huawei components in rural networks throughout America have stalled, due largely to funding issues.[44]

The broader problem remains: American complicity in PRC technological dominance has both enriched and strengthened Beijing. The acme of sound strategy is crafting asymmetric policies that force adversaries to compete on weak terrain.[45] Washington could do this easily by targeting the very capability it helped build decades ago: China's "Great Firewall." Beijing's censorship and surveillance apparatus is not a sign of strength, but an indicator of insecurity. Complicating the CCP's ability to control information within the PRC's borders would also serve as a sort of redemption for America, targeting the very threat it helped construct so many years ago.

Unfortunately, Washington is still struggling to master a more basic strategic tenant: do no harm. U.S. companies continue to transfer know-how and data to Beijing, and policymakers remain divided on how to respond. Until bipartisan political will emerges, the United States risks losing this new cold war with the CCP.

Endnotes

1 For the "cold war" framing to describe current U.S.-China great power competition, see Dmitri Alperovitch, World On the Brink: How America Can Beat China in the Race for the Twenty-First Century (New York: Public Affairs, 2024). See also Michael Sobolik, *Countering China's Great Game: A Strategy for American Dominance* (Anapolis: Naval Institute Press, 2024).
2 For a historical analysis of the role of technology in the Cold War, see Thomas Mahnken, *Technology and the American Way of War Since 1945* (New York: Columbia University Press, 2008).
3 Matt Murphy and Joe Tiddy, "What we know about the Hezbollah device explosions," BBC, September 20, 2024, https://www.bbc.com/news/articles/cz04m913m49o.
4 Souad Mekhennet and Joby Warrick, "Mossad's pager operation: Inside Israel's penetration of Hezbollah," *Washington Post*, October 5, 2024, https://www.washingtonpost.com/world/2024/10/05/israel-mossad-hezbollah-pagers-nasrallah/.
5 Mike Gallagher, "Exploding Pagers and the Tech Race with China," *Wall Street Journal*, September 22, 2024, https://www.wsj.com/opinion/exploding-pagers-and-the-tech-race-with-china-5e9b7a6e.
6 Adam Lusher, "At Least 10,000 People Died in Tiananmen Square Massacre, Secret British Cable from the Time Alleged," *Independent*, December 23, 2017, https://www.independent.co.uk/news/world/asia/tiananmen-square-massacre-death-toll-secret-cable-british-ambassador-1989-alan-donald-a8126461.html.
7 Ibid.
8 Steve Wright, "An Appraisal of Technologies for Political Control," European Parliament (Directorate General for Research, Directorate B, the STOA Programme), January 6, 1998, https://www.statewatch.org/media/documents/news/2005/may/steve-wright-stoa-rep.pdf.
9 Ibid.
10 Jon Pelson, *Wireless Wars: China's Dangerous Domination of 5G and How We're Fighting Back* (Dallas: BenBella Books, 2021), 54-55
11 James Griffiths, *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet* (London: Zed Books, 2019), 29.
12 Ibid, 29-30.
13 Ibid, 29-31.
14 Tim Reiterman, "Cranes Lift Upstart Above Competition," *Los Angeles Times*, January 27, 2002, https://www.latimes.com/archives/la-xpm-2002-jan-27-fi-cranes27-story.html.
15 Grady McGregor, "China's Crane Reign," *The Wire China*, March 26, 2023, https://www.thewirechina.com/2023/03/26/chinas-crane-reign-zpmc/.
16 Ian Easton, *The Final Struggle*: Inside China's Global Strategy (Manchester, UK: Eastbridge Books, 2023), 174.
17 "Beijing-controlled Enterprises Little Hindered by U.S. Sanctions Aimed at Specific Subsidiaries," Pointe Bello, November 2020, https://www.pointebello.com/insights/beijing-controlled-enterprises-little-hindered-by-us-sanctions.
18 Easton, *The Final Struggle*, 174.
19 House Committee on Homeland Security and House Select Committee on the Chinese Communist Party: Majority Staff, Committee report, "Handling Our Cargo: How the People's Republic of China Invests Strategically in the U.S. Maritime Industry," September 2024, https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/Joint%20Homeland-China%20Select%20Port%20Security%20Report-compressed.pdf, 7.
20 Ibid.
21 Ibid, 8.
22 Ian Easton, *The Final Struggle*, 196.
23 Pelson, *Wireless Wars*, 61.
24 Chuin-Wei Yap, Dan Strumpf, Dustin Volz, Kate O'Keeffe, and Aruna Viswanatha, "Huawei's Yearslong Rise Is Littered With Accusations of Theft and Dubious Ethics," *Wall Street Journal*, March 25, 2019, https://www.wsj.com/articles/huaweis-yearslong-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858.
25 Ibid

26 Laurel Wamsley, “A Robot Named ‘Tappy’: Huawei Conspired To Steal T-Mobile’s Trade Secrets, Says DOJ,” NPR, January 29, 2019, https://www.npr.org/2019/01/29/689663720/a-robot-named-tappy-huawei-conspired-to-steal-t-mobile-s-trade-secrets-says-doj.
27 Michael Sobolik, “Mend the Gap: 5G, the US-UK Split over Huawei, and National Security Implications,” American Foreign Policy Council, March 2020, https://www.afpc.org/uploads/documents/Defense_Technology_Briefing_-_Issue_19.pdf, 5.
28 Griff Witte and Luisa Beck, “When hunger for fast Internet collides with U.S. concerns about Chinese spying,” *Washington Post*, April 23, 2019, https://www.washingtonpost.com/world/europe/when-hunger-for-fast-internet-collides-with-us-concerns-about-chinese-spying/2019/04/22/20bf17f6-5d29-11e9-98d4-844088d135f2_story.html.
29 Office of Senator Ted Cruz, “Sen. Cruz: Huawei Decision Will Endanger National Security of Britain, United States, and Our Allies, for Generations to Come,” January 28, 2020, https://www.cruz.senate.gov/?p=press_release&id=4898.
30 Eli Lake, “The U.S.-U.K. Alliance Could Soon Get Much Weaker,” Bloomberg, March 5, 2020, https://www. bloomberg.com/opinion/articles/2020-03-05/u-k-huawei-decision-prompts-u-s-review-of-intelligence-assets.
31 Pelson, *Wireless Wars*, 156-158.
32 National Counterintelligence and Security Center, “China’s Collection of Genomic and Other Healthcare Data from America: Risks to Privacy and U.S. Economic and National Security,” February 2021, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf.
33 National Security Commission on Emerging Biotechnology, “Interim Report,” December 2023, https://www.biotech.senate.gov/wp-content/uploads/2024/01/NSCEB-December-2023-Interim-Report.pdf.
34 National Counterintelligence and Security Center, “China’s Collection of Genomic and Other Healthcare Data from America.”
35 Greg Myer, “China Wants Your Data – And May Already Have It,” NPR, February 24, 2021, https://www.npr.org/2021/02/24/969532277/china-wants-your-data-and-may-already-have-it.
36 Sui-Lee Wee, “China Uses DNA to Track Its People, With the Help of American Expertise,” *New York Times*, February 21, 2019, https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html?module=inline.
37 Ibid.
38 Ibid.
39 China human rights advocates at Human Rights Watch initially made this point. See “Thermo Fisher’s Necessary, But Insufficient, Step in China,” Human Rights Watch, February 22, 2019, https://www.hrw.org/news/2019/02/22/thermo-fishers-necessary-insufficient-step-china.
40 National Security Commission on Emerging Biotechnology, “Biological Data as a Strategic Asset,” April 2024, https://www.biotech.senate.gov/wp-content/uploads/2024/04/NSCEB_WP_Biological-Data-as-a-Strategic-Asset.pdf, 25.
41 House Select Committee on the Chinese Communist Party: Democrats, “Transcript of Ranking Member Krishnamoorthi’s Opening Statement from Hearing on The Bioeconomy and American National Security,” March 7, 2024, https://democrats-selectcommitteeontheccp.house.gov/media/press-releases/transcript-ranking-member-krishnamoorthis-opening-statement-hearing-0.
42 GEN (Ret) Keith B. Alexander, Prepared Statement on the Future of Warfare before the Senate Armed Services Committee, November 3, 2015, https://www.armed-services.senate.gov/imo/media/doc/Alexander_11-03-15.pdf.
43 “Biden admin defends approving licenses for auto chips for Huawei,” Reuters, August 27, 2021, https://www.reuters.com/business/autos-transportation/biden-admin-defends-approving-licenses-auto-chips-huawei-2021-08-27/.
44 David Shepardson, “More funds needed for US telecoms to remove Chinese equipment, says FCC,” Reuters, May 2, 2024, https://www.reuters.com/business/media-telecom/many-us-telecom-firms-need-more-funding-replace-huawei-zte-equipment-fcc-says-2024-05-02/.
45 See Sobolik, *Countering China’s Great Game*.

SALVE
THE PELL CENTER

About the Pell Center

The Pell Center for International Relations and Public Policy at Salve Regina University is a multi-disciplinary research center focused at the intersection of politics, policies, and ideas. Dedicated to honoring Senator Claiborne Pell's legacy, the Pell Center promotes American engagement in the world, effective government at home, and civic particpation by all Americans.

www.pellcenter.org