PREVENTING CHINESE SABOTAGE IN A CRISIS

RISKS OF INTERDEPENDENCE

The Biden and Trump administrations both have warned that China could sabotage critical U.S. systems during a bilateral crisis and that technological interdependence heightens this risk.[301] Beijing has the legal and political tools to compel private Chinese companies to offer up any privileged access they may have to software or hardware systems used in the United States. Such access could facilitate actual attacks, as well as threats (either explicit or implicit), against U.S. infrastructure. During peacetime, China's interest in stable commercial and diplomatic relations generally outweighs any benefits of digital sabotage or saber-rattling. But in extreme circumstances, like the cusp of war, China would have strong reason to consider all its options. There are two broad scenarios.

In extreme circumstances, Beijing would consider digital sabotage to paralyze the U.S. military or dissuade American leaders from confronting China forcefully.

First, China could attempt a counterforce operation to paralyze the U.S. military and prevent American units from responding to a bilateral crisis. For example, Beijing might want to stop key U.S. military assets from promptly reinforcing or resupplying American or allied forces abroad. The scenario has parallels with Japan's 1941 surprise attack on Pearl Harbor, which sought to buy time for Tokyo to act freely in the Pacific.[302] In a modern digital version of such an attack, China could try to subvert unclassified and/or commercially operated infrastructure that the U.S. military relies

on—such as core telecommunications systems, private logistics companies, off-base electric power sources, undersea cables, commercial satellites, and cloud services.

Second, Beijing could carry out a countervalue operation that harms U.S. civilians, hoping to demoralize them and thereby dissuade American political leaders from confronting China forcefully. This might involve disruptions of the U.S. power grid, financial sector, healthcare systems, emergency services, telecommunications, or transportation networks. Britain briefly tried (and soon abandoned) a countervalue strategy at the outset of World War I, seeking to exploit its centrality in international communications and financial networks to isolate the German economy and force Berlin to quickly sue for peace.[303] A Chinese version of this gambit could cause significant blowback—harming the Chinese economy and turning Chinese tech companies into international pariahs, among other consequences. But in a major crisis, Beijing might discount or accept this risk, seeing digital subversion as less dangerous and provocative than more overt forms of disruption.

The danger posed by these scenarios is difficult to assess. On the one hand, they are premised on a hypothetical, high-stakes crisis that may never come to pass. China's calculus for when and how to exploit its companies' access to adversary systems is unknown; Beijing's concern for Chinese firms' commercial reputations may create a state of deterrence. And the ultimate impact of any Chinese sabotage is uncertain, in part because U.S. critical infrastructure systems are so complicated and decentralized. On the other hand, the long-term risk of such a crisis seems to be trending upward as bilateral relations deteriorate. And all governments, including the United States, are willing to exploit domestic companies for national security purposes under various circumstances. Finally, a crisis is no time to test the consequences of critical U.S. system outages.

RISKS AND LIMITATIONS OF DEFENSIVE MEASURES

U.S. restrictive measures can help to reduce the risks of actual or threatened Chinese technological sabotage. But such measures also have practical limits. Understanding these limits can help to focus U.S. action on the most important areas while preventing futile and costly overreach elsewhere.

To begin with, Beijing's counterforce and countervalue options in a crisis do not all require insider access to U.S. systems. According to the U.S. Intelligence Community, "China can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States."[304] Such cyber attacks most frequently involve remote hacking; built-in backdoors are rare. In extremis, China could also do things like physically cutting undersea cables (including those that are not operated by or connected to China), disrupting U.S. satellites (through physical or cyber means that do not require

supply chain access), or ordering intelligence agents or co-optees inside the United States to carry out physical sabotage of critical infrastructure (whether Chinese-made or otherwise). Some of these actions are potentially deniable. In other words, U.S. tech restrictions can curb a few of China's sabotage options, but it isn't clear that PLA military planners need or prefer those particular options.

Technology controls also cannot eliminate China's low-tech or no-tech sources of leverage over the United States. During peacetime, Beijing's demonstrated coercive tool kit includes halting key exports, imports, and people-to-people exchanges in an effort to inflict economic damage.[305] Such actions do not necessarily target technology industries or rely on technological links. Instead, China has previously targeted sectors (including agriculture, tourism, and education) where it can impose asymmetric economic costs and maximize political pressure on a rival country's government. Again, more extreme options also exist. At the threshold of war, Beijing could choose to seize U.S.-owned assets in China or carry out mass arrests of American citizens. Such leverage points are inherent to a U.S.-China relationship; they cannot be eliminated so long as the two countries do business.

The fact is that any bilateral relationship provides both countries with some access to and influence over the other. Unless the United States seeks a Cold War–style separation from China, Beijing will retain significant avenues for coercion and disruption. Of course, Washington wants to design a relationship that maximizes U.S. leverage over China while minimizing Chinese leverage over America. This is a fine aspiration in theory, but often unattainable in practice, especially in the long run. One-sided dynamics will become harder to sustain over time as China continues to grow in economic heft and international influence relative to the United States.[306]

Any bilateral relationship provides both countries with some influence over the other. Barring a Cold War–style separation, Beijing will retain significant avenues for coercion and disruption.

Finally, potential Chinese sabotage should be placed in the context of other threats to U.S. infrastructure.[307] While American policymakers worry about what Beijing might do in future crises, a diverse array of non-Chinese actors have already caused actual disruptions to U.S. infrastructure during peacetime, or demonstrated the capability to do so. In 2021, a criminal ransomware attack led to the lengthy shutdown of America's largest petroleum pipeline, helping trigger fuel shortages throughout the East Coast.[308] The year prior, a domestic suicide bombing near an AT&T facility in Nashville caused prolonged telecommunications outages across multiple states.[309] Russia has twice caused power outages in Ukraine, and in 2014 it emerged that unknown cyber actors had severely damaged a German steel mill.[310]

The biggest threat to critical infrastructure, arguably, comes from non-intentional disruptions. Episodes like the Texas freeze (2021), Hurricane Maria (2017), and the Northeast blackout (2003) illustrate a basic problem: First, inadequate investments in infrastructure capacity, maintenance, and resilience create systemic fragility. Then, semi-random shocks—such as weather events, demand surges, equipment malfunctions, or counterfeit parts—destabilize the system and lead to large-scale outages.[311] Non-intentional infrastructure failures have been far more frequent and damaging than intentional wrongdoing by any actor. Non-intentional disruptions might even happen to coincide with an international crisis and thereby hamper U.S. military forces, although such a convergence is unlikely.

Unfortunately, China-focused restrictions can sometimes divert resources from broader efforts to shore up U.S. critical infrastructure against all hazards. Consider a hypothetical federal mandate to remove all Chinese equipment from the electrical grid. To pay for this expensive initiative, utilities would need to defer other planned investments in security and resilience, raise rates on consumers and businesses, or secure large government subsidies. Congress recently bumbled through a very similar situation. In March 2020, it passed a law requiring U.S. telecoms to "remove and replace" Huawei and ZTE equipment due to national security concerns.[312] Small rural carriers warned that this unfunded mandate would "devastate" them financially. Congress eventually provided subsidies to offset carriers' costs, but it took nine months and a fortuitous legislative vehicle—the $900 billion COVID-19 relief package—to do so.[313] Meanwhile the industry was forced to endure what one top lobbyist described as a lengthy "cliffhanger," during which two small carriers shut down.[314]

To be sure, U.S. policymakers cannot ignore the risk of China sabotaging American systems in a crisis. The risk is real, and technological interdependence provides Beijing with additional means (though perhaps lower motivation) to subvert U.S. infrastructure. Washington should take targeted, cost-effective actions to address the problem. But restrictive measures should focus on the highest-risk areas, where Chinese technological influence within the United States could grant Beijing a particularly effective capability to paralyze key U.S. forces or coerce U.S. political leadership at a critical moment. Even then, technology controls should be aligned with a comprehensive national plan to protect U.S. critical infrastructure from all digital and physical hazards.

RECOMMENDED POLICIES AND PROCESSES

The U.S. government should identify the most consequential Chinese sabotage scenarios, map the specific technological dependencies that would enable them, and design targeted controls to curb such risks.

The Department of Defense should take the lead on counterforce analysis. Approved defense planning scenarios can serve as the starting point. For each planning scenario, DOD

could list the individual U.S. military assets or networks essential to achieving mission objectives, perhaps based on Time-Phased Force Deployment Data.[315] It could then determine where these military assets have critical dependencies on unclassified and/or commercial U.S. networks. Finally, DOD could evaluate such networks for the presence of Chinese-origin software or hardware that Beijing could exploit to alter military outcomes. The acid test would be whether Chinese technological sabotage could significantly increase the likelihood of U.S. mission failure.

While DOD is leading the counterforce analysis, DHS should assess countervalue sabotage. To build a set of scenarios, DHS might start with existing frameworks such as the National Critical Functions—a list of fifty-five government and private sector activities "so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[316] These functions include such elemental tasks as "Manage Hazardous Materials," "Generate Electricity," and "Provide Positioning, Navigation, and Timing Services." DHS could survey major stakeholders for each function to identify Chinese commercial presence in the supply chain that could be exploited for disruptive purposes. This could leverage and complement the department's ongoing Systemic Cyber Risk Reduction Venture, which has a similar purpose but is not China-specific.[317]

DHS should set a high threshold of criticality before it recommends that regulators impose new China-related technology controls. It might, for example, consider only those sabotage scenarios that could plausibly exert a coercive effect on U.S. political leadership during a crisis. This would likely involve mass casualties and/or mass evacuations. As a point of comparison, the Federal Emergency Management Agency's National Threat and Hazard Identification and Risk Assessment provides a list of seven scenarios with that level of severity, including earthquakes, hurricanes, space weather events, and concurrent natural disasters.[318] To justify new government technology controls, a Chinese countervalue sabotage scenario might need to threaten damage on the same order of magnitude.

Any Chinese sabotage scenario should be vetted for plausibility. The Intelligence Community could provide an independent assessment that considers China's technology subversion capabilities, military doctrines, and national leadership intentions during the expected lifecycle of the U.S. systems at issue. In assessing China's plans and intentions, intelligence analysts should consider what other counterforce or countervalue options Beijing may have in a crisis, and whether Chinese leaders may be deterred by the risks of economic blowback or U.S. reprisals.

CASE STUDIES

Bulk power. The Trump administration's regulation of bulk power systems was a good example of tailored tech restrictions designed to thwart Chinese sabotage. In May 2020,

Trump signed an executive order restricting usage of bulk power equipment sourced from "foreign adversary" countries such as China.[319] Bulk power systems are ideal targets for sabotage because their failure can cause massive electricity outages that cannot easily be remediated. Large power transformers, for example, can take more than twenty months to replace.[320] These transformers are increasingly—though not exclusively—sourced from China and contain smart components potentially susceptible to manipulation.[321]

Trump's action focused specifically on counterforce scenarios. The administration assessed that the PLA "is equipped and actively planning to undermine" the bulk power system and that "such attacks are most likely during crises abroad where Chinese military planning envisions early cyber attacks against the electric power grids . . . in the U.S. to prevent the deployment of military forces and to incur domestic turmoil." Accordingly, the Department of Energy applied the ban on Chinese bulk power equipment only to "Defense Critical Electric Infrastructure"—that is, civilian-owned or -operated power infrastructure serving certain military facilities designated by DOD as "critical to the defense of the United States."[322]

The Department of Energy was right to bar China from supplying highly critical, difficult-to-replace bulk power equipment that directly supports military operations.

The Department of Energy was right to impose this restriction on a select subset of highly critical, difficult-to-replace equipment that directly supports military operations. However, Biden has rescinded the new rule and asked the Energy Department to consider what, if anything, should replace it.[323] The department invited public comment on potential approaches, including whether it should issue a new, even broader ban to cover countervalue scenarios and other types of power infrastructure. Any such expansion should remain focused on a very high threshold of sabotage impact and be rooted in rigorous cost-benefit analysis.

ICTS supply chain security rule. Not every U.S. action aimed at preventing Chinese technological sabotage has been so targeted. A particularly troubling case is the Commerce Department's new rule on ICTS supply chain security, which was first developed by the Trump administration, then allowed by Biden to come into effect in March 2021. Like the bulk power regulation, this rule warns that China and other foreign adversaries could sabotage the U.S. supply chain—"fully or partially shutting down critical networks or functions at key times," among many other cited dangers.[324] But the ICTS supply chain rule is far more sweeping in its scope and implications.

The ICTS rule allows the Commerce Department to review and ban virtually any China-sourced technology that is widely used in the United States. The potential scope of review includes—but is not limited to—all software (including mobile apps and web apps), internet hosting services, home networking devices, and Internet of Things devices used by or process-

ing data on more than 1 million Americans.[325] Considering the U.S. population and the scale of many digital markets, this is a low threshold. A transaction need not have any connection to critical infrastructure sectors or critical national functions to trigger review. The law firm Morrison & Foerster observed that "almost any ICTS-related activity in the United States connected to China is now subject to regulatory review by the U.S. government."[326]

Covered transactions are not automatically banned. Instead, the rule establishes a review system analogous to CFIUS. The Department of Commerce, in consultation with other agencies, will judge each transaction using a wide range of factors, including the likelihood and severity of potential harms and the efficacy of mitigation options, to determine whether "undue or unacceptable risks" exist. The publicly stated decisionmaking criteria are quite vague. Biden and the Commerce Department have taken laudable initial steps to clarify and refine these criteria, but it remains to be seen what implementation will actually look like. If Commerce follows the standard model of U.S. national security regulation (exemplified by CFIUS), it will either develop a more detailed list of internal criteria, or else make decisions on an ad hoc basis.[327] Both options would leave outside stakeholders—such as U.S. businesses—in the dark.

U.S. national security officials and political leaders traditionally prefer opaque regulatory processes for several reasons. By declining to commit publicly (or sometimes even privately) to a detailed and predictable decision framework, they seek to maximize the U.S. government's enforcement discretion. The all-encompassing ICTS supply chain rule means that Washington can adjust its interpretation from day to day based on its evolving needs and beliefs. Trump's Commerce Department also explained that clearer public criteria "would [have] allow[ed] foreign adversaries to pinpoint certain types of ICTS Transactions that would more easily escape Departmental oversight and, therefore, threaten U.S. national security."

Biden should substantially narrow the ICTS rule, instituting a clear and high threshold for technology bans and declaring specific safe harbors for noncritical tech areas.

But too much discretion comes with costs of its own, especially when a large portion of the U.S. digital economy and global technology supply chain is at stake. Without more clarity and predictability, some U.S. businesses will simply choose to avoid China-related technology transactions, including many that pose little national security risk and are economically beneficial. Likewise, global investors will pull back support from some projects—many of them benign—whose viability depends on a long-term U.S.-China technology supply chain.[328] The Biden administration should substantially narrow the ICTS supply chain rule, instituting a clear and high threshold for technology bans and declaring specific safe harbors for noncritical technology areas. It should also continue working to develop and publicize a more detailed and explicit set of enforcement criteria, along the lines suggested throughout this report.

In its current form, the ICTS supply chain rule is an invitation for overuse—if not by this administration, then by a future one. For example, restrictionist politicians and national security analysts have long campaigned for broad-based bans on computers, printers, and other devices sold by the Chinese companies Lenovo and Lexmark. The proposed bans would apply even in lower-risk settings, like noncritical state and local government offices.[329] Banning these cheap IT commodities would make it harder for cash-strapped public entities to address more pressing cybersecurity concerns, such as ransomware. Yet the ICTS supply chain rule provides a clear regulatory basis for such a ban, setting the stage for a concerted lobbying push in the future.

KEY OFFENSIVE POLICIES

The U.S. government has numerous options for directly bolstering the cybersecurity and resilience of critical military and civilian systems, which would mitigate not only the risk of Chinese sabotage but also other serious threats, like weather-related outages. With the electrical grid, for example, the Federal Energy Regulatory Commission could apply stronger mandatory cybersecurity standards to a larger number of entities and enforce them more vigorously.[330] The Department of Energy could establish a strategic reserve of large power transformers.[331] Congress could allocate federal money to shore up grid vulnerabilities.[332] Investments in disaster recovery capabilities at the federal, state, and local levels would also help mitigate the economic and societal damage caused by infrastructure outages once they occur. Any of these efforts might be expensive, so the federal government could focus first on a small subset of assets, like Defense Critical Electric Infrastructure, that face greatest risk from Chinese sabotage.

301 "Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure," Department of Energy, 86 Fed. Reg. 21,309 (April 22, 2021), https://www.federalregister.gov/documents/2021/04/22/2021-08482/notice-of-request-for-information-rfi-on-ensuring-the-continued-security-of-the-united-states; and "Prohibition Order Securing Critical Defense Facilities," Department of Energy, 86 Fed. Reg. 533 (January 6, 2021), https://www.federalregister.gov/documents/2021/01/06/2020-28773/prohibition-order-securing-critical-defense-facilities.

302 Emily O. Goldman and Michael Warner, "Why a Digital Pearl Harbor Makes Sense . . . and Is Possible," Carnegie Endowment for International Peace, October 16, 2017, https://carnegieendowment.org/2017/10/16/why-digital-pearl-harbor-makes-sense-.-.-.-and-is-possible-pub-73405.

303 Britain quickly abandoned this strategy due to its large costs. But that does not mean that China would never consider its own similar strategy in a future Sino-U.S. crisis. If Beijing implemented such a strategy, it might once again turn out to be a mistake. But an initial blow against the United States could nevertheless be powerful, justifying U.S. efforts to prevent and mitigate such a scenario. Nicholas Lambert, "Brits-Krieg: The Strategy of Economic Warfare," Carnegie Endowment for International Peace, October 16, 2017, https://carnegieendowment.org/2017/10/16/brits-krieg-strategy-of-economic-warfare-pub-73403.

304 "Annual Threat Assessment of the US Intelligence Community," Director of National Intelligence, April 9, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

305 Peter Harrell, Elizabeth Rosenberg, and Edoardo Saravalle, "China's Use of Coercive Economic Measures," Center for a New American Security, June 2018, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/China_Use_FINAL-1.pdf; and Evan A. Feigenbaum, "Is Coercion the New Normal in China's Economic Statecraft?," Macro Polo, July 25, 2017, https://carnegieendowment.org/2017/07/25/is-coercion-new-normal-in-china-s-economic-statecraft-pub-72632.

306 For example, the Lowy Institute's most recent Asia Power Index identified "a short-term reprieve from an established pattern of relative US decline" compared to China. Hervé Lemahieu and Alyssa Leng, "Asia Power Index: Key Findings 2021," Lowy Institute, 2021, https://power.lowyinstitute.org/downloads/lowy-institute-2021-asia-power-index-key-findings-report.pdf. See also James Dobbins, Gabrielle Tarini, and Ali Wyne, "The Lost Generation in American Foreign Policy," RAND Corporation, 2020, https://www.rand.org/pubs/perspectives/PEA232-1.html.

307 The Biden administration's 100-day review of the U.S. supply chain makes this point elegantly. Though not focused on critical infrastructure per se, it outlines a range of domestic and international risks to U.S. resilience in key sectors, and wisely treats hostile subversion from China as just one of many challenges. "Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth," White House, June 2020, https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.

308 Ken Dilanian and Kelly O'Donnell, "Russian Criminal Group Suspected in Colonial Pipeline Ransomware Attack," NBC News, May 10, 2021, https://www.nbcnews.com/politics/national-security/russian-criminal-group-may-be-responsible-colonial-pipeline-ransomware-attack-n1266793.

309 Adi Robertson, "AT&T Recovers From Multi-state Outage After Nashville Bombing," The Verge, December 28, 2020, https://www.theverge.com/2020/12/28/22202822/att-outage-nashville-christmas-bombing.

310 "Hack Attack Causes 'Massive Damage' at Steel Works," BBC, December 22, 2014, https://www.bbc.com/news/technology-30575104.

311 Nick Thieme, "After Hurricane Maria, Puerto Rico's Internet Problems Go From Bad to Worse," PBS, October 23, 2018, https://www.pbs.org/wgbh/nova/article/puerto-rico-hurricane-maria-internet/.

312 William Yuen Ye, "With U.S. Restrictions on Huawei and ZTE, Where Will Rural America Turn?," Center for Strategic and International Studies, December 10, 2020, https://www.csis.org/blogs/new-perspectives-asia/us-restrictions-huawei-and-zte-where-will-rural-america-turn.

313 Matt Kapko, "Rural US Carriers Secure $1.9B to Rip Out Chinese Equipment," SDxCentral, December 23, 2020, https://www.sdxcentral.com/articles/news/rural-us-carriers-secure-1-9b-to-rip-out-chinese-equipment/2020/12/.

314 William Yuen Ye, "With U.S. Restrictions on Huawei and ZTE, Where Will Rural America Turn?," Center for Strategic and International Studies, December 10, 2020, https://www.csis.org/blogs/new-perspectives-asia/us-restrictions-huawei-and-zte-where-will-rural-america-turn.

315 Joint Chiefs of Staff, "Joint Publication 5-0: Joint Planning," December 1, 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0.pdf.

316 "National Critical Functions Set," Cybersecurity and Infrastructure Security Agency (CISA), April 2019, https://www.cisa.gov/national-critical-functions-set.

317 "Systemic Cyber Risk Reduction Venture," CISA, https://www.cisa.gov/systemic-cyber-risk-reduction.

318 "2019 National Threat and Hazard Identification and Risk Assessment (THIRA): Overview and Methodology," Federal Emergency Management Agency, July 25, 2019, https://www.fema.gov/sites/default/files/2020-06/fema_national-thira-overview-methodology_2019_0.pdf; and "Homeland Security Planning Scenarios and Summary Descriptions," Brookings Institution, https://www.brookings.edu/wp-content/uploads/2016/06/20051026_3-1.pdf.

319 Executive Order 13920, "Securing the United States Bulk-Power System," 85 Fed. Reg. 26595 (May 1, 2020), https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system.

320 "Large Power Transformers and the U.S. Electric Grid," Department of Energy, June 2021, https://www.energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf.

321 Black Sobczak and Peter Behr, "Security – China and America's 400-Ton Electric Albatross," E&E News, April 25, 2019, https://www.eenews.net/stories/1060216451/.

322 "Prohibition Order Securing Critical Defense Facilities," Department of Energy, 86 Fed. Reg. 533 (January 6, 2021), https://www.federalregister.gov/documents/2021/01/06/2020-28773/prohibition-order-securing-critical-defense-facilities.

323 "Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure," Department of Energy, 86 Fed. Reg. 21,309 (April 22, 2021), https://www.federalregister.gov/documents/2021/04/22/2021-08482/notice-of-request-for-information-rfi-on-ensuring-the-continued-security-of-the-united-states.

324 "Securing the Information and Communications Technology and Services Supply Chain," Commerce Department, 86 Fed. Reg. 4909 (January 19, 2021), https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain.

325 "Securing the Information and Communications Technology and Services Supply Chain," Commerce Department, 86 Fed. Reg. 4909 (January 19, 2021), https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain.

326 Brandon L. Van Grack, Charles L. Capito, and Joseph A. Benkert, "Biden Administration Carries Forward Trump Era Executive Order Scrutinizing Imports and Sales of Certain Communications Technology and Services," Morrison Foerster, April 1, 2021, https://www.mofo.com/resources/insights/210401-trump-executive-order.html.

327 As discussed earlier, Biden issued an executive order outlining "a criteria-based decision framework and rigorous, evidence-based analysis" to help guide the rule's application to internet-connected software. The Commerce Department subsequently proposed to incorporate this guidance into the ICTS rule, and invited comment on whether Biden's criteria should also govern reviews of other kinds of software and hardware. Executive Order 14034, "Protecting Americans' Sensitive Data From Foreign Adversaries," 86 Fed. Reg. 31,423 (June 9, 2021), https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries; and "Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications," Commerce Department, 86 Fed. Reg. 67,379 (November 26, 2021), https://www.federalregister.gov/documents/2021/11/26/2021-25329/securing-the-information-and-communications-technology-and-services-supply-chain-connected-software.

328 Francesca M.S. Guerrero and Jennifer L. Parry, "Veritas, a U.S. Genetic Sequencing Company, Suspends U.S. Operations Due to Decreased Funding; CFIUS Thought to Be Leading Cause," Winston & Strawn, December 23, 2019, https://www.winston.com/en/global-trade-and-foreign-policy-insights/veritas-a-us-genetic-sequencing-company-suspends-us-operations-due-to-decreased-funding-cfius-thought-to-be-leading-cause.html.

329 Bill Gertz, "Lexmark, Lenovo Tech Funnels Data to China Intelligence Services," *Washington Times*, February 24, 2020, https://www.washingtontimes.com/news/2020/feb/24/lexmark-lenovo-tech-funnels-data-china-intelligenc/; Roslyn Layton, "Why Is U.S. Policy Tough on Huawei and TikTok but Not Lenovo?," *Forbes*, June 26, 2020, https://www.forbes.com/sites/roslynlayton/2020/06/26/why-is-us-policy-tough-on-huawei-and-tiktok-but-not-lenovo/?sh=3cdcb5cc7b6e; James Marks, "The Chinese Threat That's Hiding in Plain Sight," The Bulwark, September 12, 2019, https://thebulwark.com/the-chinese-threat-thats-hiding-in-plain-sight/; Roslyn Layton, "Stealing From the States: China's Power Play in IT Contracts," China Tech Threat, March 2020, https://chinatechthreat.com/wp-content/uploads/2020/02/CTT-Report-Stealing-From-States-Chinas-Power-Play-in-IT-Contracts.pdf; Ryan McMorrow and Kathrin Hille, "Lenovo's Sales Strong Despite Growing Threat of US Sanctions," *Financial Times*, August 13, 2020, https://www.ft.com/content/a5f5f290-04c9-4776-ae8d-ee881b13bb3a.

330 Robert K. Knake, "A Cyberattack on the U.S. Power Grid," Council on Foreign Relations, April 3, 2017, https://www.cfr.org/report/cyberattack-us-power-grid.

331 "Strategic Transformer Reserve," Department of Energy, March 2017, https://www.energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf.

332 Robert K. Knake, "A Cyberattack on the U.S. Power Grid," Council on Foreign Relations, April 3, 2017, https://www.cfr.org/report/cyberattack-us-power-grid; and "Strategic Transformer Reserve," Department of Energy, March 2017, https://www.energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf.