Testimony before the U.S. Senate Judiciary Subcommittee on Privacy, Technology, and the Law

Hearing on "Big Hacks & Big Tech: China's Cybersecurity Threat"

Sam Bresnick
Research Fellow
Center for Security and Emerging Technology (CSET), Georgetown University
November 19, 2024

Chair Blumenthal, Ranking Member Hawley, and members of the subcommittee: thank you for the opportunity to testify before you. Today, I will address a critical national security challenge—the extensive economic and technological interdependence between U.S. technology companies and China. This relationship has deepened amid an increasingly complex geopolitical landscape, and we must better understand the national security risks these ties present, as well as how they may impact corporate decision-making during future crises.

The historical, political, geographic, economic, and security dynamics of Russia-Ukraine and China-Taiwan relations differ significantly. However, the role U.S. tech companies have played in supporting Ukraine has sparked interest in how these and other firms might respond to potential Chinese aggression against Taiwan, whether military or otherwise.

My testimony draws on a CSET report published earlier this year that analyzes the impact of economic dependencies on corporate decision-making through two main case studies: U.S. technology companies' support for Ukraine against Russia in the aftermath of Moscow's full-scale invasion, and the anticipated complexities these same companies may face in a Taiwan contingency or other conflict with China.[1] Unlike in the Ukraine crisis, where U.S. technology firms had relatively limited exposure to Russia and acted quickly to defend Ukraine, a conflict with Beijing could present significant strategic challenges given these companies' deep economic and technological dependencies on China.

Corporate Involvement in the Russia-Ukraine War

During the early stages of the Russia-Ukraine conflict, U.S. technology companies showcased their capacity to shape conflict outcomes through swift, voluntary, and often unprecedented actions. These companies ranged from publicly traded big tech firms to privately held defense technology startups. Several of these companies acted as crucial enablers of the Ukrainian military and government in this conflict, lending their support in ways ranging from providing data and cybersecurity services to enhancing intelligence, surveillance, and reconnaissance (ISR) capabilities.[2] Still others reportedly facilitated targeting and satellite-enabled communications.[3] These companies, leveraging their advanced technologies and, in some cases, vast infrastructure, provided Ukraine with critical support to resist Russian aggression.

The absence of major economic or technological ties to Russia before the full-scale invasion simplified these companies' decisions to support Ukraine. Few, if any, of the firms depended heavily on Russia for revenue, manufacturing, or research and development (R&D) operations, thus allowing them a freer hand in aligning their actions with U.S. and allied interests.[4] Moreover, U.S. public support for Ukraine and disapproval of Russia further smoothed the way for their aiding Kyiv.[5] The companies that operated in Russia prior to February 2022, however, did suffer some costs, as many wound down their businesses in the country and were fined by the government.[6] But U.S. tech companies' flexibility in decision-making—without the risk of significant financial or technological losses or disruptions—may not apply as readily in a future crisis involving China, where economic and technological entanglements run far deeper.

Complexities in a China Conflict Scenario: Economic Interdependencies and Strategic Dilemmas

The situation with China, a global economic powerhouse and key trading partner, presents an entirely different challenge. Many of the same U.S. companies that played pivotal roles in Ukraine have substantial footprints in China, creating a complex web of mutual dependencies that could influence their responses in a conflict with China. These interdependencies fall into several distinct but interrelated categories, including revenue dependency, supply chain reliance, and research and development entanglement, among others. Each of these categories represents a potential vulnerability that could impact corporate decision-making in a crisis scenario.

Further complicating the picture is that China has a track record of leveraging economic coercion to advance its geopolitical objectives and respond to perceived threats to its territorial integrity, national security, or the Chinese Communist Party's legitimacy. Examples include barring rare earth mineral exports to Japan during a 2010 maritime dispute, restricting salmon imports from Norway after a Chinese activist won the Nobel Prize, and targeting fruit imports from the Philippines over a South China Sea dispute.[7] Additionally, Beijing has taken action against several U.S. technology companies. Google services like YouTube, Search, Gmail, and Maps are banned in China.[8] Recently, China restricted some government officials and state-owned enterprise employees from using Apple iPhones, and Tesla's electric vehicles have been banned from certain areas during events over concerns about sensitive data collection.[9] The following sections outline China-U.S. tech firm interdependencies in greater detail.

Revenue Dependency and Market Penetration

One of the primary areas of concern is the significant portion of revenue that some U.S. tech companies derive from the Chinese market. For a couple of these corporations, China has accounted for around 20 percent of their global revenue in recent years, and losing access to this market would represent a substantial financial blow. In comparison to the Russia-Ukraine crisis, where the financial cost of withdrawing from the Russian market was relatively low, the high stakes involved in losing the Chinese market could deter companies from taking actions perceived as antagonistic to Chinese interests. This dependency not only influences current business strategies but may also shape responses to U.S. government policies during a conflict, particularly if companies fear repercussions to their bottom line.

Supply Chain and Manufacturing Reliance

Supply chain entanglement with China is another critical area where U.S. tech companies face substantial risks. In some cases, over 80 percent of a company's suppliers operate in China, and large proportions of product assembly for certain high-demand technologies is conducted within the country. Given ongoing de-risking efforts, however, corporate reliance on China for manufacturing is in some cases decreasing.[10] But a potential Taiwan conflict could have sweeping implications for U.S. technology firms' supply chains, triggering disruptions that might extend beyond the immediate conflict zone. Companies with a high degree of reliance on Chinese factories face particular risks, as production delays or supply chain shutdowns could create significant barriers to maintaining operations. U.S. tech companies could find themselves in a position where they must weigh the risk of disrupted supply chains against support for U.S. or allied strategic objectives. This dependency underscores the importance of a resilient supply chain strategy that mitigates risk by diversifying beyond China. That said, China's advanced infrastructure—spanning road, rail, ports, and utilities—has streamlined manufacturing and logistics. Additionally, China's vast workforce and abundance of skilled engineers have solidified its status as a global manufacturing leader. Thus, these advantages are unlikely to diminish in the short to medium term, as no other country will likely be able to rival China's manufacturing advantages.

Research and Development Activities

The entanglement extends beyond revenue and supply chains to R&D operations, which are important factors in U.S. technology companies' innovation ecosystems. China serves as a significant base for R&D activities for some of these companies, particularly in fields such as artificial intelligence (AI) and hardware design. However, this reliance on Chinese R&D resources could lead to challenges in balancing commercial imperatives with national security interests. In a conflict with Beijing, Chinese authorities could impose restrictions on R&D activities, constraining corporate innovation strategies. This could not only affect ongoing projects but also damage the competitiveness of U.S. tech companies in global markets. A reduction in R&D output, due to regulatory or operational constraints imposed by China, could ultimately weaken U.S. innovation in critical technology sectors.

Other Dependencies

Aside from revenue, supply chains, and R&D operations, several U.S. technology companies conduct supplemental activities that could expose them to Chinese coercion. Some of these companies have injected a significant amount of capital into China through foreign direct investment (FDI), both in sheer dollar terms and as a proportion of their global FDI expenditures. The prospects for recovering those investments amid a conflict are unclear. Furthermore, several U.S. technology companies maintain data centers or cloud computing infrastructure in China, the closure of which could negatively impact their ability to continue operating or making money in the country. Finally, though employment data is difficult to access, some companies maintain thousands of international and Chinese employees in China. Protecting these people amid a conflict could prove difficult.

The Implications of Chinese Coercive Leverage

The economic entanglements of U.S. tech companies with China present not only a source of financial risk but also potential channels for Chinese coercive leverage. In a conflict with China, Chinese authorities could impose regulatory restrictions, threaten market access, or disrupt supply chains to dissuade U.S. companies from taking actions that align with U.S. government objectives. The threat of such repercussions could create significant pressure on U.S. companies, potentially undermining their willingness to support U.S. strategic goals in future crises.

That said, China also relies heavily on U.S. tech companies, and their exit would pose significant challenges to Beijing. A reduction in their operations or complete departure could result in millions of job losses, disrupt value chains, and destabilize local economies in the short term. Their withdrawal would hinder China's access to global science and technology networks, chill FDI, and potentially trigger capital flight. Such factors underscore the critical role these companies play in China's economic and technological landscape, as well as why China may be reluctant to coerce these companies, especially given its ongoing economic slowdown.

Policy Recommendations

The U.S. government has a critical role to play in mitigating the vulnerabilities of U.S. corporations operating in China and ensuring that they can respond effectively to potential future conflicts. I have several policy recommendations for Congress as a whole to consider:

1. **Identify the Optimal De-Risking Balance**

    - Incentives to support supply chain diversification could reduce corporate reliance on China-based manufacturing. Programs that facilitate partnerships with alternative suppliers or business associations in third-party nations, or that encourage reshoring of critical production activities, could help build a more resilient manufacturing base that is less vulnerable to coercive pressures from geopolitical rivals. This strategy should encourage the deepening of electronics manufacturing outside of China, which currently dominates much of the electronics supply chain.
    - It would be unwise, however, to move from de-risking toward full decoupling; mutual interdependence can stabilize bilateral ties and act as a brake on conflict.

2. **Enhance Reporting Requirements and Transparency**

    - U.S. companies should be required to disclose detailed information on their foreign dependencies, including revenue shares, supply chain sources, and R&D investments and activities, particularly in nations that may pose strategic risks. Supply chain analysis is particularly difficult, as companies are not always aware of their first-order suppliers' dependencies on those further down the chain. Increased transparency in these areas would allow policymakers to make informed decisions and develop targeted responses that mitigate potential adversarial coercive leverage.

3. **Develop Contingency Plans for High-Stakes Scenarios**

    - To prepare for potential crises, companies with significant dependencies in China should be encouraged to develop contingency plans that address scenarios like a potential Taiwan crisis. These plans could outline alternative supply chains, potential relocation strategies for R&D operations, and fallback options for capital assets, ensuring, as much as possible, that corporate interests remain aligned with U.S. national security objectives. The companies should communicate these plans and the difficulties they present to the U.S. government.

Conclusion

In summary, this testimony underscores the profound entanglements of U.S. technology companies with China and the potential impact of these ties on their response to a Taiwan contingency. While these companies demonstrated a strong capacity to support U.S. and allied interests in Ukraine, their dependencies on China present a far more complex and potentially constraining scenario.

As the U.S. faces an evolving global landscape where national security and economic interests increasingly intersect, it is essential for policymakers to address these vulnerabilities proactively. Implementing strategic policies that enhance corporate resilience can help align U.S. technology companies' interests with national security goals, even in challenging circumstances.

Thank you for your attention to these critical issues. I am available to answer any questions you may have.

[1] Sam Bresnick, Ngor Luong, and Kathleen Curlee, "Which Ties Will Bind?" (Center for Security and Emerging Technology, February 2024). https://cset.georgetown.edu/publication/which-ties-will-bind/.
[2] Erik Lin-Greenberg and Theo Milonopoulos, "Boots on the Ground, Eyes in the Sky," *Foreign Affairs*, May 30, 2022, https://www.foreignaffairs.com/articles/ukraine/2022-05-30/boots-ground-eyes-sky; Cisco "Supporting Ukraine: Cisco Response to the War in Ukraine," March 27, 2023, https://perma.cc/45ZN-9MH6; David E. Sanger, Julian E. Barnes and Kate Conger, "As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War," *The New York Times*, February 28, 2022, https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html.
[3] Jeffrey Dastin, "Ukraine is using Palantir software for 'targeting,' CEO says," *Reuters*, February 1, 2023, https://www.reuters.com/technology/ukraine-is-using-palantirs-software-targeting-ceo-says-2023-02- 02/; Alex Marquardt, "Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab," *CNN*, October 14, 2022, https://www.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html.
[4] Bresnick, Luong, and Curlee, "Which Ties Will Bind?"
[5] Gallup, "Russia | Gallup Historical Trends," https://news.gallup.com/poll/1642/russia.aspx.
[6] Bresnick, Luong, and Curlee, "Which Ties Will Bind?"
[7] Keith Bradsher, "Amid Tension, China Blocks Vital Exports to Japan," *The New York Times*, September 22, 2010, https://www.nytimes.com/2010/09/23/business/global/23rare.html; Echo Huang and Isabella Steger, "Norway wants China to forget about the human rights thing and eat salmon instead," *Quartz*, June 14, 2017, https://qz.com/1000541/norway-wants-china-to-forget-about-the-human-rights-thingand-eat-salmon-instead; Andrew Higgins, "In Philippines, banana growers feel effect of South China Sea dispute," *The Washington Post*, June 10, 2012, https://www.washingtonpost.com/world/asia_pacific/in-philippinesbanana-growers-feel-effect-of-south-china-sea-dispute/2012/06/10/gJQA47WVTV_story.html.
[8] Rob Binns, "Websites banned in China: Access, alternatives and unblocked sites," *The Independent*, November 6, 2023, https://www.independent.co.uk/advisor/vpn/websites-banned-in-china; Matt Sheehan, "How Google took on China—and lost," *MIT Technology Review*, December 19, 2018, https://www.technologyreview.com/2018/12/19/138307/how-google-took-on-china-and-lost/.
[9] *Bloomberg*, "China's iPhone Ban Accelerates Across Government and State Firms," December 15, 2023, https://www.bloomberg.com/news/articles/2023-12-15/china-s-apple-iphone-ban-acceleratesacross-state-firms-government; *Reuters*, "Tesla cars barred for 2 months in Beidaihe, site of China leadership meet," June 20, 2022, https://www.reuters.com/business/autos-transportation/chinasbeidaihe-district-bar-tesla-cars-driving-july-local-police-2022-06-20/; *Bloomberg*, "Tesla Cars Barred From World University Games Ahead of Xi Visit," July 26, 2023, https://www.bloomberg.com/news/articles/2023-07-26/tesla-cars-barred-from-world-university-games-ahead-of-xi-visit.
[10] Ashley Capoot, "Apple doubles India iPhone production to $14 billion as it shifts from China: Report," *CNBC*, April 10, 2024, https://www.cnbc.com/2024/04/10/apple-made-14-billion-worth-of-iphones-in-india-in-shift-from-china.html.