Statement before the
Senate Select Committee on Intelligence
"Threats to US National Security: Countering PRC's Economic and Technological Plan for Dominance"

A Testimony by:

James Mulvenon, Ph.D.

March 11, 2022

216 Hart Senate Office Building

Introduction

Chairman Warner, Ranking Member Rubio, and distinguished members, thank you for inviting me to testify today.

My remarks today can be divided into three sections: (1) a summary of the Chinese Communist Party's economic and technological strategies; (2) the role of illicit technology acquisition in those strategies; and (3) the unique value of open-source intelligence to combat these problems.

The Chinese Communist Party's Economic and Technological Strategies

The Chinese government has a comprehensive strategy for national economic growth and technology modernization. This strategy has created an unfair, asymmetric business environment in China, sometimes forcing American companies, which need to be in the China market to grow and prosper, to make suboptimal decisions that are not always in the long-term interests of U.S. national security, but clearly benefit Chinese national security. Although American companies are one of Beijing's highest priority targets in the race to close the technological gap with the United States, the current tech transfer crisis is not entirely their fault. In the China market, American companies confront a comprehensive, state-directed economic and technological development strategy designed to promote technology transfer from foreign multinationals and elevate domestic companies to compete with those multinationals in the global market.[1] This strategy is one personally touted by President Xi Jinping, who declared at a recent Communist Party meeting that the Chinese state must determine which technologies to develop on its own, which to induce or co-opt from abroad, and which to develop in partnership with Chinese entities.[2] Xi's personal vision has been codified into a more concrete strategy with a number of key overt features:

- Promulgation of state industrial planning documents outlining how Beijing would use its substantial regulatory leverage and financial resources to promote technology transfer (e.g., "2006-2020 Mid-to-Long Range S&T Plan" and "Made in China 2025"[3])
- Implementation of the strategy of "military-civilian fusion" that expands "civil-military integration" of defense and civilian industrial bases to facilitate the "construction of a national infrastructure that connects the PLA, state-owned defense research,

---

[1] For an overview, see Jane Perlez, Paul Mozur And Jonathan Ansfield, "China's Technology Ambitions Could Upset the Global Trade Order," *New York Times*, 7 November 2017, accessed at:
https://www.nytimes.com/2017/11/07/business/made-in-china-technology-trade.html?_r=0

[2] https://chinacopyrightandmedia.wordpress.com/2016/04/19/xi-jinping-gives-speech-at-cybersecurity-and-informatization-work-conference/

[3] See U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections*, 2017, accessed at:
https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf

development, and manufacturing enterprises, government agencies under the State Council, universities, and private sector firms."[4]

- Provision of massive state subsidies (e.g., National Integrated Circuit Fund) to benefit Chinese companies, often masked in ways to skirt WTO prohibitions (according to the U.S Chamber's analysis of Made in China 2025, China will "provide preferential access to capital to domestic companies in order to promote their indigenous research and development capabilities, *support their ability to acquire technology from abroad*, and enhance their overall competitiveness"[5]). Other benefits include "fiscal stimulus, tax reductions and holidays, access to low-cost or free land, low-interest credit, easier access to securities markets, patent approvals, discriminatory technical standards, antitrust policy directed against disfavored competitors, privileged government procurement, limits on market access, and other preferential policies."[6]
- Promotion of "national champion" companies (e.g., Huawei) to supplant multinational companies in the China market and globally[7]
- Promulgation of laws and regulations codifying asymmetries in playing field for U.S. companies operating in China using a very broad definition for what constitutes national security (e.g., Anti-Monopoly Law,[8] Cybersecurity Law,[9] Counter-Espionage Law,[10] National Security Law,[11] Counter-Terrorism Law[12])
- The use of a domestic standards regime, especially with respect to information communication and telecommunications, as a trade weapon to advantage Chinese

---

[4] Greg Levesque and Mark Stokes, *Blurred Lines: Military-Civil Fusion and the "Going Out" of China's Defense Industry*, Pointe Bello, December 2016, accessed at: https://static1.squarespace.com/static/569925bfe0327c837e2e9a94/t/593dad0320099e64e1ca92a5/1497214574912/062017_Pointe+Bello_Military+Civil+Fusion+Report.pdf

[5] See U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections*, 2017, accessed at: https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf

[6] Scott Kennedy, "Evaluating CFIUS: Challenges Posed by a Changing Global Economy," Statement Before the House Committee on Financial Services, Subcommittee on Monetary Policy and Trade, 9 January 2018, accessed at: https://financialservices.house.gov/uploadedfiles/hhrg-115-ba19-wstate-skennedy-20180109.pdf

[7] James McGregor, *China's Drive for 'Indigenous Innovation: A Web of Industrial Policies*, Washington, DC: US Chamber of Commerce, July 2010.

[8] U.S. Chamber of Commerce, *Competing Interests in China's Competition Law Enforcement: China's Anti-Monopoly Law Application and the Role of Industrial Policy*, accessed at: https://www.uschamber.com/sites/default/files/aml_final_090814_final_locked.pdf

[9] https://www.chinalawtranslate.com/cybersecuritylaw/?lang=en

[10] https://www.chinalawtranslate.com/anti-espionage/?lang=en

[11] http://www.chinalawtranslate.com/2015nsl/?lang=en

[12] https://www.chinalawtranslate.com/%E5%8F%8D%E6%81%90%E6%80%96%E4%B8%BB%E4%B9%89%E6%B3%95-%EF%BC%882015%EF%BC%89/?lang=en

companies (e.g., WLAN Authentication and Privacy Infrastructure or WAPI, draft China CPU/OS/computer standards, and the 5G cellular standard)[13]

- Promotion of "buy local" laws to disadvantage foreign firms, especially in information and communications technologies[14]
- Strategies to attract priority foreign investment in China, especially joint ventures and "greenfield" investments[15]
- Mercantilist investment structures globally designed to create infrastructure path dependencies for Chinese state-owned enterprises ("One Belt, One Road")[16] and quasi-private companies that China aims to ensure will provide the hardware and software that will underpin all critical infrastructure of the future, from power grids to telecom networks to e-payments infrastructure.

These activities have a direct and lasting negative impact on U.S. national security. As the Communist Party seeks to enhance all aspects of its national comprehensive power, U.S. comparative advantages will become even more paramount in sustaining U.S. leadership on the battlefield, including in advanced technologies. For example, the Pentagon's "third offset" strategy seeks to leverage current U.S. commercial technological advantages in key areas, such as artificial intelligence and machine learning, to enhance our war fighting capability vis-a-vis China and a resurgent Russia.[17] Yet if our porous investment security and export control regime is not improved, Beijing may be able to turn these current American advantages into their own by investing in, acquiring, or co-opting critical technology. This will allow China to deny the United States' ability to leverage critical technologies for its national security, and further close the gap with the U.S. in areas of key military systems and applications ranging from hypersonic glide vehicles to AI-enabled cyber defense systems.

---

[13] Dan Breznitz and Michael Murphree, "The Rise of China in Technology Standards: New Norms in Old Institutions," report prepared for the U.S.-China Economic and Security Review Commission, 16 January 2013, accessed at: https://www.uscc.gov/sites/default/files/Research/RiseofChinainTechnologyStandards.pdf

[14] U.S. Chamber of Commerce, *Preventing Deglobalization: An Economic and Security Argument for Free Trade and Investment in ICT*, 2016, accessed at: https://www.uschamber.com/sites/default/files/documents/files/preventing_deglobalization_1.pdf

[15] For the best data on the subject, see the American Enterprise Institute's China Global Investment Tracker at https://www.aei.org/china-global-investment-tracker/ and The Rhodium Group's China Investment Monitor at http://rhg.com/interactive/china-investment-monitor

[16] Christopher Johnson, *President Xi Jinping's "Belt and Road" Initiative: A Practical Assessment of the Chinese Communist Party's Roadmap for China's Global Resurgence,* Center for Strategic and International Studies, March 2016, accessed at: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160328_Johnson_PresidentXiJinping_Web.pdf

[17] https://www.defense.gov/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence/

The Role of Illicit Technology Acquisition in CCP Strategies

In 2013, two U.S. government colleagues and I published a book entitled *Chinese Industrial Espionage*, which documented the efforts, both quasi-legal and illegal, used by the Chinese government and state-owned entities to steal U.S. technology, intellectual property, and secrets.[18] For me, this culminated almost two decades of tracking Chinese cyber espionage and the PRC military and defense industrial base's efforts at illicit technology transfer. Beijing's illicit and non-traditional collection activities cover four main areas well known to this Committee:

- Beijing's well-documented, planetary-scale, government-directed cyber espionage program[19]
- Large-scale, government-directed technology espionage[20]
- Non-traditional collection (e.g., the "1000 Talents Program")[21]
- New types of hybrid cyber and human technology espionage (According to the 2016 U.S-China Economic and Security Review Commission report: "China appears to be conducting a campaign of commercial espionage against U.S. companies involving a combination of cyber espionage and human infiltration to systematically penetrate the

---

[18] William Hannas, James Mulvenon, and Anna Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, London: Routledge, May 2013.

[19] See *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, Office of the National Counterintelligence Executive, October 2011, at https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf; ThreatConnect, *CameraShy: Closing the Aperture on China's Unit 78020*, at https://www.threatconnect.com/camerashy/; Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, accessed at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf; Dmitri Alperovitch, *Revealed: Operation Shady RAT*, McAfee, August 2011; McAfee® Foundstone® Professional Services and McAfee Labs, Global Energy Cyberattacks: 'Night Dragon', 10 February 2011, accessed at: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf; Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, (report prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp), March 7, 2012; and *Operation SMN: Axiom Threat Actor Group Report*, accessed at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[20] Peter Mattis, "Testimony before the U.S.-China Economic and Security Review Commission: Chinese Human Intelligence Operations against the United States," 2 June 2016, accessed at: http://www.uscc.gov/sites/default/files/Peter%20Mattis_Written%20Testimony060916.pdf

[21] William Hannas, James Mulvenon, and Anna Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, London: Routledge, May 2013.

information systems of U.S. companies to steal their intellectual property, devalue them, and acquire them at dramatically reduced prices."[22])

Any one of these strategies or policies in isolation would be problematic for the U.S. government and American companies, but their simultaneous and often coordinated implementation with the explicit support of PRC government leadership presents an unprecedented challenge.

The Unique Value of Open-Source Intelligence to Countering the PRC's Strategies

I have spent the last 25 years building teams of cleared linguist-analysts, mainly Chinese and Russian, and cleared technical engineers, performing open-source collection, exploitation, and analysis for the US Government. As Members of the Committee know, some intelligence missions primarily require classified national technical means, while other intelligence missions lend themselves more easily to open-source collection and exploitation. I can confirm that open-source intelligence is particularly powerful for the topics I have been discussing. Most, if not all, of China's national level economic and technological development strategies are openly published, as are the accompanying implementation documents. This is also true of China's "military-civil fusion" strategy, as well as myriad laws and regulations that are promulgated to institutionalize the predatory system. All these documents are published in Chinese, and official translations are rare. Moreover, the core data required to track the implementation of the strategies (procurement bids and tenders, corporate records, investments records, patents, legal proceedings, and even résumés) are all available on public-facing Chinese databases, though again all in Chinese and often requiring moderately sophisticated tradecraft to access in a non-alerting way. With the passage of China's Data Security Law, it has recently become more difficult to access these datasets from outside of China, requiring more sophisticated methods. However, nearly all the information necessary for the US Government to gain deep and operationalizable insight into these CCP strategies and transactions remain available from open sources.

Conclusion

The People's Republic of China, through its economic and national security strategies, poses a serious threat to dominate key technologies and control key supply chains in ways that are inimical to American interests, though focused open-source intelligence could provide us with uniquely valuable and actionable insights. I look forward to your questions and again express my appreciation for the invitation to testify.

---

[22] *USCC 2016 Annual Report*, accessed at: https://www.uscc.gov/sites/default/files/annual_reports/2016%20Annual%20Report%20to%20Congress.pdf