INSTITUTE FOR DEFENSE ANALYSES

Opportunity Seldom Knocks Twice: Influencing China's Trajectory via Defend Forward / Persistent Engagement in Cyberspace

Michael P. Fischerkeller, *Project Leader*

April 2020

IDA Non-Standard
NS D-13135

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-14-D-0001, Project C5107, "Cyberspace Operations Working Group," for the IDA. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgements

Laura A. Odell, Emily Goldman, Keith W. Crane, Thomas C. Greenwood, Paul A. Mancinelli

For More Information

Michael P. Fischerkeller, Project Leader
mfischer@ida.org, 703-845-6784

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Rigorous Analysis | Trusted Expertise | Service to the Nation

INSTITUTE FOR DEFENSE ANALYSES

IDA Non-Standard NS D-13135

Opportunity Seldom Knocks Twice: Influencing China's Trajectory via Defend Forward / Persistent Engagement in Cyberspace

Michael P. Fischerkeller, *Project Leader*

Opportunity Seldom Knocks Twice:

Influencing China's Trajectory via Defend Forward / Persistent Engagement in Cyberspace

Michael P. Fischerkeller, Institute for Defense Analyses

Introduction

Through its long march to a "moderately prosperous society" and global technological supremacy, China has encountered significant hurdles.[1] In 2010, for example, after years of significant economic growth, the Chinese Communist Party (CCP) leadership was publicly expressing concerns about slowing economic growth and social unrest—conditions CCP leadership associated with the middle-income trap (MIT).[2] As part of a multi-faceted strategy to mitigate the MIT and stave off impending calamity, China launched a campaign of cyber-enabled theft of U.S. intellectual property (IP). Evidence of successfully re-innovating illicitly acquired IP was arguably behind President Xi's confident exclamation in 2015 that growth would average 6.5% from 2015–2020, a target necessary for keeping the MIT at bay.[3] Although the United States attempted to abate China's campaign of cyber-enabled IP theft through diplomatic means, the Chinese ignored U.S. requests, resulting in a lost opportunity to shape China's rise when its economy was in a vulnerable state.[4]

Opportunity is knocking again. Current U.S. tariff policy began placing downward pressure on China's economy in 2018 that was not anticipated when President Xi made his 2015 proclamation.[5] Not coincidentally, the CCP again ramped up cyber-enabled IP theft in 2018, possibly to help mitigate that pressure by jump-starting additional innovation-based growth, just as it did in 2010–2013.[6] The first

---

[1] Julian Baird Gewirtz, "China's Long March to Technological Supremacy: The Roots of Xi Jinping's Ambition to "Catch Up and Surpass," *Foreign Affairs*, August 27, 2019, https://www.foreignaffairs.com/articles/china/2019-08-27/chinas-long-march-technological-supremacy.

[2] The MIT describes a condition resulting from policy misdiagnosis when countries fail to match their growth strategies with prevailing structural characteristics of their economies. The economies to which the MIT applies are those being "squeezed between the low-wage poor country competitors that dominate in mature industries and the rich-country innovators that dominate in industries undergoing rapid technological change." Indermit S. Gill and Homi Kharas, "The Middle Income Trap Turns 10," World Bank Group, August 2015, http://documents.worldbank.org/curated/en/291521468179640202/pdf/WPS7403.pdf.

[3] Edward Wong, "China Aims for 6.5% Economic Growth Over Next 5 Years, Xi Says," *The New York Times*, November 3, 2015, https://www.nytimes.com/2015/11/04/world/asia/china-economic-growth-xi.html.

[4] See Eric Chabrow, "Obama Raises IP Theft with New China Leader," *Bankinfosecurity*, March 14, 2013, https://www.bankinfosecurity.com/obama-raises-ip-theft-new-china-leader-a-5610 and Eric Chabrow, "U.S. Asks China to Probe, Stop Cyber-Intrusions," *Bankinfosecurity*, March 11, 2013, https://www.govinfosecurity.com/us-asks-china-to-probe-stop-cyber-intrusions-a-5594.

[5] A conservative estimate of the impact of U.S. tariffs on China's GDP is a 1% decline. While a small value, when considered against the fact that Xi's growth targets were the minimum required to avoid the MIT, the consequences of falling short of those targets by 1% could be severe. See Nicholas R. Lardy, "China's Growth Is Slowing, but not Because of the Trade War", August 21, 2019, Peterson Institute for International Economics, https://www.piie.com/blogs/china-economic-watch/chinas-growth-slowing-not-because-trade-war.

[6] See, "Observations from the Front Lines of Threat Hunting: A 2018 Mid-year Review" from Falcon OverWatch, CrowdStrike, October, 2018, https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018OverwatchReport.pdf?mkt_tok=eyJpIjoiWWpWa1lqUTRNelF3Wm1GbSIsInQiOiJEbHNkNVEyenppYjRvWHNtcllGS0VtMHJ3ZVZETStrdVRwXC9veWVoUXE0c2ZlWU5KSDdqUkpLVWkxRkhsREpuXC9HNjV4VWN

time around, the U.S. Department of Defense's (DoD) 2011 Strategy for Operating in Cyberspace was misaligned against the IP-theft campaign and U.S. Cyber Command's (USCYBERCOM) capabilities were not matched to the challenge. Today, USCYBERCOM is a mature combatant command with 133 Fully Operationally Capable teams, and DoD is implementing a new cyber strategy of Defend Forward, including an operational approach of persistent engagement to inhibit adversary strategic gains through such cyber operations short of armed conflict. This second time around, the U.S. has a cyber strategy better aligned to the challenge and an improved capability to execute it.

Framing the Strategic Significance of China's IP Theft

Common refrains regarding the strategic significance of China's theft of U.S. IP include concerns of immediate economic losses—with estimates ranging from $250-600 billion annually—and a potential longer-term threat of dis-incentivizing innovation investments.[7,8] A focus on these consequences obscures the true strategic intent of China's cyber-enabled IP theft campaign. Around 2010, CCP leadership recognized that, based on historical patterns, China was approaching the limits of its time to transition from a middle to high income economy.[9] The historical consequences of failing—slowing economic growth and socio-political upheavals (the MIT)—could put at risk both the CCPs' legitimacy and China's great power status.[10,11] In response, the CCP adopted a multi-faceted technology transfer policy to counter expected slowing growth by stimulating indigenous innovation. Only one facet of that policy—a centrally-directed, massive cyber-enabled campaign of IP theft—was able to produce results with certainty, immediacy, and at a scale necessary to ensure China avoided the MIT. Unanticipated downward economic pressure emerging in 2018 is, again, pushing China toward the precipice of a MIT,

---

SbGtJVTRJOFh0eGdCNzNiXC8zMHprZW1taklwaURpU1hLUHdNdXNxZkM0cSt0Y1RDQXlQejNqQ2g0aCJ9, and Ken Dilanian, "China's Hackers Are Stealing Secrets from U.S. Firms Again, Experts Say," October 9, 2018, NBC News, https://www.nbcnews.com/news/china/china-s-hackers-are-stealing-secrets-u-s-firms-again-n917836.

[7] See, for example, *Foreign Economic Espionage in Cyberspace*, National Counterintelligence and Security Center, 2018, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf .

[8] For a report estimating annual damage in dollars, see *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974,* Office of the United States Trade Representative: Executive Office of President, March 22, 2018), https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF. For a report on impact on U.S. GDP (between 1 and 3%), see *Annual Intellectual Property Report to Congress,* Executive Office of the President of the United States, February 2019, https://www.whitehouse.gov/wp-content/uploads/2019/02/IPEC-2018-Annual-Intellectual-Property-Report-to-Congress.pdf.

[9] For the current 2020 fiscal year, low-income economies are defined as those with a Gross National Income (GNI) per capita of $1,025 or less in 2018 (as calculated using the World Bank Atlas method); lower middle-income economies are those with a GNI per capita between $1,026 and $3,995; upper middle-income economies are those with a GNI per capita between $3,996 and $12,375; high-income economies are those with a GNI per capita of $12,376 or more. See, https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups.

[10] Indermit S. Gill and Homi Kharas, "The Middle Income Trap Turns 10," World Bank Group, op. cit. and Jan Rudengren, Lars Rylander, and Claudia Rives Casanova, "It's Democracy, Stupid: Reappraising the Middle-Income Trap," Stockholm Paper, Institute for Security and Development Policy, 2014, https://www.files.ethz.ch/isn/184240/2014-rudengren-rylander-casanova-reappraising-the-middle-income-trap.pdf.

[11] Japan, South Korea, and Singapore spent 21, 23, and 29 years, respectively, as middle-income economies before moving up to upper-income level.

and so the CCP is returning to its previously successful strategy of cyber-enabled IP theft to mitigate the risk.

Expressions of Concern and Policy Platforms

In October 2010, Liu He, a key author of China's 12th Five-Year Plan stated that the CCP was aware most countries attempting to transition from a middle to high income economy stagnated, consequently fueling social upheaval. Subsequently, he noted the CCP is "concerned about how to avoid the so-called 'middle-income trap'."[12] In 2013, President Xi similarly "stressed his hope of avoiding the middle-income trap."[13] The CCP's economic research reveals the same concerns. In 2011, the Development Research Center of the State Council published a compendium of MIT research, and in 2013, they coordinated with the World Bank to publish *China 2030: Building a Modern, Harmonious and Creative Society*, including a section on structural reforms repeatedly mentioning concerns of falling victim to the MIT. [14,15]

The 12th Five-Year Plan (2011–2015) was one of several platforms promoted by the CCP in response to these concerns. MIT scholars prescribe shifting to an innovation-based economy to avoid the MIT. Unsurprisingly, China's State Council released the "Decision on Accelerating the Development of Strategic Emerging Industries (SEIs)" in October 2010, which called for intensifying technological innovation in numerous high technology areas.[16,17] The 12th Five-Year Plan reiterated this call through the Chairman of the Chinese People's Political Consultative Conference National Committee linking the plan's success to science and technology (S&T) and indigenous innovation capacity.[18] In December 2011, President Hu emphasized the same: "We must improve our capabilities for original innovation,

---

[12] Hu Shuu, Zhu Changzheng, Yang Zheyu, "Liu He on China's New Transformation Trail," Caixin Online, October 28, 2010, http://english.caing.com/2010-11-08/100196829.html

[13] See, respectively, Indermit Gill, "Future Development Reads: Xi Jingping, China's People's Party, and the Middle-Income Trap," Brookings, October 20, 2017, https://www.brookings.edu/blog/future-development/2017/10/20/future-development-reads-xi-jinping-chinas-peoples-party-and-the-middle-income-trap/; and, "China May Be Running Out of Time To Escape the Middle-Income Trap," Asia Society, October 2017, https://asiasociety.org/new-york/china-may-be-running-out-time-escape-middle-income-trap.

[14] The compendium is entitled *Trap or Wall: Real Challenges and Strategic Choice in China's Economy*, http://en.drc.gov.cn/2014-06/26/content_17617382.htm.

[15] *China 2030: Building a Modern, Harmonious and Creative Society*, The World Bank and Development Research Center of the State Council, the People's Republic of China, 2013, https://www.worldbank.org/en/news/feature/2012/02/27/china-2030-executive-summary.

[16] See, Indermit S. Gill and Homi Kharas, "An East Asian Renaissance: Ideas for Economic Growth," World Bank, January 1, 2007, http://documents.worldbank.org/curated/en/517971468025502862/An-East-Asian-renaissance-ideas-for-economic-growth and Indermit S. Gill and Homi Kharas, "The Middle Income Trap Turns 10," op. cit. For a more nuanced analysis of the phenomenon, see Xuehui Han and Shang-Jin Wei, "Re-examining the Middle-Income Trap Hypothesis (MITH): What to Reject and What to Revive?" National Bureau of Economic Research, February 2017, https://www.nber.org/papers/w23126.pdf.

[17] *State Council Decision on Accelerating the Development of Strategic Emerging Industries* (State Council, Guo Fa [2010], No. 32, issued Oct. 10, 2010), https://chinaenergyportal.org/wp-content/uploads/2017/01/Development-Strategic-Emerging-Industries.pdf.

[18] "China's Top Political Stresses Indigenous Innovation", *Xinhua English*, April 19, 2011, http://english.sina.com/china/p/2011/0419/369456.html.

integrated innovation and re-innovation through digesting introduced technologies to transform to an innovation-driven economy and society" and "must have a sense of urgency and crisis."[19] Hu's exigency may have reflected frustration with China's lack of innovation progress as, six years prior, the "National Medium- and Long-Term Science and Technology Development Plan (MLP)" called out China's "relatively weak innovation capacity" while calling for building an innovation-oriented country.[20] MIT concerns also influenced the 13th Five-Year Plan (2016–2020), "the Made in China 2025 Notice," and "Guidelines for China's Innovation-Driven Development Model," a document establishing broad goals for China becoming an "innovative nation" by 2020.[21,22,23]

Observers and analysts of China's economy identified the same concerns, recognizing these platforms as efforts to avoid the MIT. Damien Ma argues the "13th Five-Year Plan … aims to prevent the country from falling into the middle-income trap," and James Lewis testified in 2013 that the CCP's stance on IP acquisition acknowledges that rapid economic growth is crucial to their ability to retain power. [24,25] Ominously, Ambassador Charles Freeman argues "… if China fails to carry out the reforms it is currently attempting, its growth rate will fall significantly and its future power will diminish accordingly."[26]

Sustained Growth as a Political Mandate and Regime Legitimacy

Coincident with the 13th Five-Year Plan, Beijing forecasted a 2016 GDP target of 6.5–7%, a figure consistent with President Xi's goal of doubling the size of China's 2010 economy by 2020. Achieving the 2020 goal, which is tantamount to a political mandate, requires a GDP average of at least 6.5% through

---

[19] See "China Celebrates Success of Space Docking Mission", *Space Daily*, December 19, 2011, http://www.spacedaily.com/reports/China_celebrates_success_of_space_docking_mission_999.html.

[20] "Notice on Issuing the National Medium- and Long-Term Science and Technology Development Plan Outline (2006–2020)," State Council, Guo Fa [2005] No. 44, issued Dec. 26, 2005), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/China_2006.pdf. In this Notice, indigenous innovation referred to "enhancing original innovation, integrated innovation, and re-innovation based on assimilation and absorption of imported technology, in order improve our national innovation capability."

[21] See Michel Aglietta and Guo Bai, "China's 13th Five-Year Plan. In Pursuit of a 'Moderately Prosperous Society,'" CEPII Policy Brief, September 2016, http://www.cepii.fr/PDF_PUB/pb/2016/pb2016-12.pdf and Katherine Koleski, "The 13th Five-Year Plan," U.S.-China Economic and Security Review Commission, February 14, 2017, https://www.uscc.gov/sites/default/files/Research/The%2013th%20Five-Year%20Plan_Final_2.14.17_Updated%20(002).pdf

[22] Scott Kennedy, "Made in China 2025," Center for Strategic and International Studies, June 21, 2015, https://www.csis.org/analysis/made-china-2025.

[23] State Council of the People's Republic of China, "Guideline for China's Innovation-Driven Development," May 20, 2016. http://english.gov.cn/policies/latest_releases/2016/05/20/content_281475353682191.htm.

[24] Damien Ma, "Can China Avoid the Middle Income Trap," *Foreign Policy* (March 12, 2016), https://foreignpolicy.com/2016/03/12/can-china-avoid-the-middle-income-trap-five-year-plan-economy-two-sessions/

[25] Kenneth Corbin, "Economic Impact of Cyber Espionage and IP Theft Hits U.S. Businesses Hard," CIO, July 10, 2013, https://www.cio.com/article/2384269/economic-impact-of-cyber-espionage-and-ip-theft-hits-u-s--businesses-hard.html.

[26] Ambassador Chas W. Freeman, Jr. (USFS, Ret.), "China as a Great Power: Remarks to China Renaissance Capital Investors," op. cit.

2020, a target Xi announced on November 3, 2015.[27] In 2015, China could no longer count on additions to the labor force and fixed-asset investment to sustain GDP growth.[28] Analysis suggests that meeting Xi's targets requires that 3% of growth in the 2016–2020 period come from engineering- and science-based innovation, areas in which China is weak by the CCP's own admissions.[29] Moreover, these innovation archetypes generally don't make significant contributions to GDP for 5–10 or 15–20 years after investments.

How was Mr. Xi reconciling his targets with the realities of slowing growth, decreasing contributions from labor force expansion and fixed-asset investment, and negligible contributions from engineering- and science-based innovation?[30] Xi's confidence in 2015 is defensible given evidence that China's commitment (around 2010) to a centrally directed and massive campaign of cyber-enabled IP theft with an engineering- and science-based innovation focus was already bearing fruit, contributing to growth with certainty, at scale, and within a fraction of the time experienced historically by other nations.[31]

China's Technology Transfer Policy

Since publication of the MLP and SEIs, the CCP has introduced numerous directives and incentives to facilitate indigenous innovation through technology transfers of U.S. IP.[32] These represent a multi-faceted technology development strategy comprising licit and illicit methods to achieve innovation objectives. They include the legal and regulatory environment, S&T research and development (R&D) investments, mergers and acquisitions, joint ventures, non-traditional collectors, research partnerships,

---

[27] Damien Ma, "Can China Avoid the Middle Income Trap?" op. cit.; Edward Wong, "China Aims for 6.5% Economic Growth Over Next 5 Years, Xi Says," *The New York Times*, op. cit.

[28] Wayne M. Morrison, "China's Economic Rise: History, Trends, Challenges, and Implications for the United States," *Congressional Research Service*, June 25, 2019, https://crsreports.congress.gov/product/pdf/RL/RL33534.

[29] "The China Effect on Global Innovation," McKinsey Global Institute, October 2015, https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/Gauging%20the%20strength%20of%20Chinese%20innovation/MGI%20China%20Effect_Full%20report_October_2015.ashx.

[30] Similar confidence was expressed by Liu Yuanchun, an economist and vice president of Renmin University of China, after listening to Xi's address to the 19th National Congress. "I think it will be no problem for China to avert the middle-income trap, and we should be confident about this," Liu told media on the sidelines of the congress. "China Focus: How China Can Avoid Middle Income Trap in a New Era", Xinhua, October 23, 2017, http://www.xinhuanet.com/english/2017-10/23/c_136699982.htm.

[31] A similar argument within a longer Chinese historical context is made by Julian Baird Gewirtz, "China's Long March to Technological Supremacy: The Roots of Xi Jinping's Ambition to 'Catch Up and Surpass,'" *Foreign Affairs*, August 27, 2019, https://www.foreignaffairs.com/articles/china/2019-08-27/chinas-long-march-technological-supremacy

[32] See *Section 301 Investigation and Hearing: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation,* Office of the United States Trade Representative: Executive Office of President, October 10, 2017, https://ustr.gov/sites/default/files/enforcement/301Investigations/China%20Technology%20Transfer%20Hearing%20Transcript.pdf, and Sean O'Connor, "How Chinese Companies Facilitate Technology Transfer from the United States," U.S.–China Economic and Security Review Commission, May 6, 2019, https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf.

talent recruitment programs, academic collaborations, and Ministry of State Security (MSS) and military intelligence services (human intelligence (HUMINT) and cyber-enabled IP theft).[33]

Although all could have conceivably contributed to engineering- and science-based innovation growth post-2015, regulatory and economic analyses, the nature of intelligence tradecraft, cyber campaign forensic analyses, and cleared DoD contractor reporting suggest that cyber-enabled IP theft between 2010 and 2013 likely contributed significantly to growth to-date. It is the only method that simultaneously addressed the requirements for certainty, immediacy, and scale to avoid the MIT. It is no surprise, then, that this method began playing a central role in economic policy at the time CCP leadership began expressing MIT concerns.

To support this argument, in light of the aforementioned analyses, each facet of China's technology transfer policy is considered between 2010 and 2013 against the requirements of certainty, immediacy, and scale. Certainty is captured by two aspects—a method's effectiveness at facilitating IP acquisition and/or China's effectiveness at absorbing and actualizing it. Immediacy addresses a method's effectiveness at acquiring IP hastily and/or China's effectiveness at absorbing and actualizing it against growth soon after acquisition. "At scale" represents a method's effectiveness at acquiring IP at a volume that would make a noticeable contribution to growth were China able to effectively absorb and actualize it.[34]

Legal and Regulatory Environment and S&T R&D Investment

The most potentially relevant change in China's IP legal and regulatory environment occurred in March 2019, when China's State Council enacted the Foreign Investment Law of the People's Republic of China, part of which addresses U.S. concerns regarding "forced technology transfer."[35] Xi could reasonably conclude the law would facilitate additional opportunities for innovation through Foreign Direct Investment (FDI). However, given its recency, this method can be ruled out as a basis for his confidence in 2015. Similarly, S&T R&D investments, while a critical foundation for long-term engineering- and science-based innovation growth, would not address immediacy because it typically takes 15–20 years (or more) for R&D efforts to make growth contributions. Moreover, R&D would also not address certainty, as it is uncertain by its very nature.

Mergers and Acquisitions and Joint Ventures

Acquisitions could address both aspects of certainty and immediacy. Between 2010 and 2013, some Chinese FDI targeted industries were deemed to be strategic by the Chinese government including

---

[33] *Foreign Economic Espionage in Cyberspace*, National Counterintelligence and Security Center, 2018, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

[34] A similar framework, but serving a different purpose, is proposed by Lindsay and Cheung. See Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application", in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, Eds., *China and Cybersecurity: Espionage, Strategy, and the Politics of the Digital Domain*, (Oxford University Press: Oxford UK, 2015), https://global.oup.com/academic/product/china-and-cybersecurity-9780190201265?cc=us&lang=en&.

[35] See, http://www.fdi.gov.cn/1800000121_39_4872_0_7.html.

information technology and biotechnology. At the time, however, there was no clear link between FDI decisions and CCP policies or incentive programs.[36] Still, such acquisitions could lead to the transfer of U.S. IP and technology to China.[37] Analysis of these acquisitions, however, does not suggest investors were acquiring assets and moving capacities to China or that the primary value proposition was a quick grab of patents.[38] Additionally, these acquisitions numbered only in the tens. It is possible, then, that Xi's confidence was not based on knowledge or belief that acquisitions were, or would be, making notable engineering- or science-based innovation contributions to post-2015 growth.

Joint ventures would address both aspects of certainty. Studies conclude that international joint ventures, especially with a technology transfer element, have significant, positive impacts over time on China's growth.[39] If, from 2010–2013, joint ventures in SEIs (which are required by law) numbered in the hundreds or perhaps thousands, they might also address scale.[40] Joint ventures can be formed rather quickly, addressing one aspect of immediacy; however, product life cycles in engineering-based industries tend to be 5–10 years or longer.[41] Consequently, joint ventures might not address immediacy's aspect of prompt actualization against growth. Additionally, international investor sentiment at the time was not favorable. According to AmCham China's 2013 survey, 42% of respondents in SEI sectors expressed concerns over "de facto technology transfer requirements as a requirement for market access," and sentiment that there was "growing pressure for technology transfer" increased by 10% over 2012.[42] Perhaps as a consequence of this environment, FDI and, by association, joint ventures declined as a percentage of GDP in 2010 and 2015 from 4% to 2.2%, thereby contributing far less to growth in 2015.[43] This suggests that joint venture activity was not the basis of Xi's 2015 confidence.

---

[36] Sean O'Connor, "How Chinese Companies Facilitate Technology Transfer from the United States," U.S.-China Economic and Security Review Commission, op. cit.

[37] *2017 Report to Congress of the U.S.-China Economic and Security Review Commission*, November 2017, https://www.uscc.gov/sites/default/files/2019-09/2017_Annual_Report_to_Congress.pdf.

[38] Thilo Hanemann and Daniel H. Rosen, "High Tech: The Next Wave of Chinese Investment in America: Special Report," *Asia Society*, April 2014, https://asiasociety.org/high-tech-next-wave-chinese-investment-america. Example investments in this period include the acquisition of Enstrom Helicopter Corporation by Chongqing Helicopter Investment and the acquisition of ZONARE Medical Systems by Mindray Medical International.

[39] See John Van Reenen and Linda Yueh, "Why Has China Grown So Fast? The Role of International Technology Transfer," January 27, 2012, https://www.economics.ox.ac.uk/materials/papers/5634/paper592.pdf ; Kun Jiang, Wolfgang Keller, Larry D. Qiu, William Ridley, "International Joint Ventures and Internal vs. External Technology Transfer: Evidence from China," The National Bureau of Economic Research, October 2019, https://www.nber.org/papers/w24455.pdf; and Thomas J. Holmes, Ellen R. McGrattan, and Edward C. Prescott, "Quid Pro Quo: Technology Capital Transfers for Market Access in China," The National Bureau of Economic Research, July 2013, http://www.nber.org/papers/w19249.

[40] *Catalogue for the Guidance of Foreign Investment Industries* (Amended in 2011), Ministry of Commerce Peoples Republic of China, http://english.mofcom.gov.cn/article/policyrelease/aaa/201203/20120308027837.shtml.

[41] *The China Effect on Global Innovation*, McKinsey Global Institute, October 2015, op. cit.

[42] AmCham China, *2013 China Business Climate Survey Report*, https://media.npr.org/documents/2013/may/AmChamSurvey.pdf.

[43] The World Bank, *Foreign Direct Investment, Net Inflows (% GDP)*, https://data.worldbank.org/indicator/BX.KLT.DINV.WD.GD.ZS?locations=CN.

HUMINT

While an oversimplification, several methods—non-traditional collectors, research partnerships, talent recruitment programs, and academic collaborations—could be considered HUMINT operations when CCP directed. Chinese intelligence agencies focus recruitment efforts on Chinese nationals traveling and living abroad and on university students studying abroad.[44] Every Chinese student studying abroad has been approved by the government, with the vast majority in the U.S. majoring in science and other high-technology subjects. While some return after graduation, others are encouraged to find employment in U.S. companies and may subsequently be approached by intelligence operatives to steal IP. Still others return to China, are trained as intelligence operatives, and attempt to return to the U.S. and obtain jobs in strategic companies.[45] The H1-B visa program is the U.S. government program supporting the employment of Chinese nationals.[46]

By 2009 there were approximately 120,000 Chinese H1-B visa holders in the United States.[47] The U.S. Department of Justice filed only 20 indictments against Chinese nationals for economic espionage in 2010–2013, but this highlights only the HUMINT IP theft that was discovered.[48] H1-B visa holders tend to occupy high technology positions, and it is reasonable to conclude agents would be matched with companies whose technologies aligned with the SEIs. Assuming agents are productive addresses one aspect of certainty—effectiveness in acquiring IP. However, it is questionable that this method would acquire IP hastily, an aspect of immediacy, as a HUMINT tradecraft approach to IP theft is resource-intensive and time-consuming.[49] The second aspects of certainty and immediacy—that China could absorb and actualize acquired IP against growth soon after acquisition—are not addressed, nor precluded, by this method. Regarding scale, given HUMINT's clandestine nature, it is challenging to approximate how much it might contribute to innovation-based growth. Assuming its contribution is relatively constant over time, an assessment can be made of the potential for increases/decreases to annual growth as a function of increases/decreases in annual Chinese H1-B petitions over time.[50] In

---

[44] For an overview of Chinese HUMINT capabilities, see "U.S.-China Economic and Security Review Commission, 'Hearing on Chinese Intelligence Services and Espionage Operations, written testimony of Peter Mattis,'" June 9, 2016, https://www.uscc.gov/sites/default/files/Peter%20Mattis_Written%20Testimony060916.pdf

[45] Gary Sibeck. "Chinese Corporate Espionage," *American Intelligence Journal* (28, no. 2, 2010), 66–71, https://jstor.org/stable/44327161 .

[46] See https://www.uscis.gov/working-united-states/temporary-workers/h-1b-specialty-occupations-and-fashion-models/h-1b-fiscal-year-fy-2020-cap-season.

[47] This figure is based on an approximation of 20,000 Chinese petitioners per year and an accumulation of the same over a six-year period. The H-1B visa and status is initially valid for three years and can then be extended for another three years.

[48] For summaries of the cases, see *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, Executive Office of the President of the United States, February 2013, https://www.justice.gov/criminal-ccips/file/938321/download.

[49] For summaries of 20 cases in the January 2010–January 2013 timeframe, see *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, Executive Office of the President of the United States, February 2013, https://www.justice.gov/criminal-ccips/file/938321/download.

[50] For a brief commentary on H1-B visas and espionage, see Grant Goss, "Six China Residents Charged With Stealing US Mobile Phone Technology," CIO, May 19, 2015, https://www.cio.com/article/2924273/six-china-residents-charged-with-stealing-us-mobile-phone-technology.html in conjunction with "H1-B Visas: Industrial Espionage Case, May 20, 2015 Matloff," http://ftp.cwalocal4250.org/article?id=a_1432134073-1537&t=h1b&p=3.

2009–2013, petitions averaged 22,641 annually with fluctuations around that average of -1% to 5%.[51] This relatively stable trend suggests Xi's confidence was not likely founded on expectations of increased HUMINT contributions to growth. Moreover, as an aside, when discussing cyber-enabled IP theft, a former Inspector General of the NSA commented, "If you can steal information or disrupt an organization by attacking its networks remotely, why go to the trouble of running a spy?"[52] This leads to a consideration of the remaining method—cyber-enabled IP theft.

Cyber-enabled IP Theft

Cyber-enabled IP theft could address scale and one aspect each of certainty and immediacy without precluding the other aspects of both. China's cyber operations pre-date 2010, but those before 2010 centered on government and military targets.[53] After intrusions into Google and other Silicon Valley companies in 2009–2010, U.S. officials became concerned that China had begun focusing on the commercial sector.[54] Mandiant's 2013 report on China's Advanced Persistent Group 1 (APT1) validated those concerns by making a compelling case that APT1 (PLA Unit 61398) is responsible for massive theft of U.S. IP from 2010 to 2013.[55] Moreover, as the PLA reports directly to the CCP's Central Military Commission, Mandiant argues that PLA enterprise cyber-enabled IP theft is centrally directed by CCP senior members, a view supported by U.S. intelligence experts.[56] Indeed, the U.S. government has evidence the CCP provides competitive intelligence from cyber intrusions to state-owned enterprises (SOEs) through a formal request and feedback loop and a classified communication system for information exchange.[57]

Mandiant estimated that APT1 is staffed by hundreds or perhaps thousands and that it has stolen hundreds of terabytes of data from at least 115 U.S. organizations (up through 2012).[58] Additionally, the

---

[51] See "Number of H-1B Petition Filings Applications and Approvals, Country, Age, Occupation, Industry, Annual Compensation ($), and Education FY2007 - FY2017," U.S. Citizenship and Immigration Services, https://www.uscis.gov/sites/default/files/USCIS/Resources/Reports%20and%20Studies/Immigration%20Forms%20Data/BAHA/h-1b-2007-2017-trend-tables.pdf. This analysis starts in 2009 assuming there will be at least a 5-year lag between a petition being approved and a potential agent acquiring and passing back IP that could be absorbed and actualized to contribute to growth.

[52] Joel Brenner quoted in Shane Harris, "China's Cyber Militia," May 31, 2008, http://triprosec.net/pdf/china_cyber_militia.pdf.

[53] See, for example, Dmitri Alperovitch, "Revealed: Operation Shady RAT," McAfee, http://www.csri.info/wp-content/uploads/2012/08/wp-operation-shady-rat1.pdf and Information Warfare Monitor, "Tracking GhostNet: Investigating a Cyber Espionage Network," Toronto: SecDev and Citizen Lab, March 29, 2009, https://issuu.com/citizenlab/docs/iwm-ghostnet.

[54] William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation* (Routledge: May 2013), 217, https://www.crcpress.com/Chinese-Industrial-Espionage-Technology-Acquisition-and-Military-Modernisation/Hannas-Mulvenon-Puglisi/p/book/9780415821421#googlePreviewContainer.

[55] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," http://it-report-lb-1-312482071.us-east-1.elb.amazonaws.com/.

[56] "U.S.-China Economic and Security Review Commission, 'Hearing on Chinese Intelligence Services and Espionage Operations,'" written testimony of Peter Mattis, op. cit.

[57] *Findings of the Investigation in China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974*, op. cit.

[58] "APT1: Exposing One of China's Cyber Espionage Units," op. cit.

report concludes these numbers directly observed represent a small fraction of APT1 intrusions and, therefore, should be considered the lower bounds of activity and capacity from 2006–2012.[59] The conservatism regarding *activity* is warranted, given many companies hesitate to reveal that they have been exploited. From investigating APT1 cyber intrusions, a former U.S. Attorney for the Western District of Pennsylvania (2010–2016) claims to have identified thousands of U.S companies targeted by APT1.[60] The conservatism regarding APT1's *capacity* is supported by a 2010 report from the FBI's former deputy director for counterintelligence noting that China sustains 250,000–300,000 soldiers in the 3PLA dedicated to cyber espionage and that much of this capability can be deployed to support China's methods for stealing IP.[61] Unsurprisingly, Mandiant acknowledges that APT1 is but one of more than 20 APT groups with origins in China.[62]

Mandiant's analysis covers 2006–2012, but 76% of activity occurred against U.S. firms from 2010–2012, suggesting that a more concerted effort began in 2010. The industries targeted match China's strategic industries, including four of seven SEIs in the 12th Five-Year Plan, suggesting a centrally directed effort.[63] A subsequent Mandiant analysis (up to 2015) concludes that all seven of China's SEIs were being served by numerous APTs.[64] Data exfiltrated from firms includes a laundry list of IP: product development and use including information on test results, system designs, product manuals, parts lists, and simulation technologies; manufacturing procedures, such as descriptions of proprietary processes, standards, and waste management processes; and more.[65]

In addition, correlating evidence supports the argument that, relative to other Chinese technology transfer methods, cyber-enabled IP theft was the central effort from 2010–2013. Most Chinese cyber operations against U.S. private industry that have been detected were directed against "cleared defense contractors" or information technology and communications (IT&C) firms whose products and services support government and private sector networks worldwide.[66] Retaining cleared contractor status requires firms to report "suspicious contacts," described as "efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared

---

[59] Ibid.

[60] Laura Sullivan, "As China Hacked, U.S. Businesses Turned a Blind Eye", *National Public Radio*, April 12, 2019, https://www.npr.org/2019/04/12/711779130/as-china-hacked-u-s-businesses-turned-a-blind-eye.

[61] Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation," Defense Innovation Unit Experimental (DIUx), January 2018, https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf.

[62] "APT1: Exposing One of China's Cyber Espionage Units," op. cit.

[63] Ibid.

[64] "Hearing before the U.S.-China Economic and Security Review Commission, Commercial Cyber Espionage and Barriers to Digital Trade in China, June 15, 2015, Written Testimony of Jen Weedon, Manager, Threat Intelligence and Strategic Analysis, FireEye and Mandiant, Inc.," https://www.uscc.gov/sites/default/files/Weedon%20Testimony.pdf.

[65] "APT1: Exposing One of China's Cyber Espionage Units," op. cit.

[66] "Foreign Economic Espionage in Cyberspace," National Counterintelligence and Security Center, 2018, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf. A "cleared defense contractor" is a private entity granted clearance by the DoD to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of the DoD.

employee."[67] DoD's Defense Counterintelligence and Security Agency (DCSA), formerly known as the Defense Security Service (DSS), analyzes these data, providing annual, year-over-year statistical and trend analysis on the foreign-entity threat posed to the cleared contractor community.[68]

While not identical, DCCA uses Method of Operations (MO) categories aligning well with many of China's technology transfer methods, including HUMINT, joint ventures, and suspicious network activity (SNA).[69] Similarly, DCSA industry categories match well with technologies specified in China's MLP and 12th Five-Year Plan, and as SEIs.[70] Finally, while DCSA reports provide regional data, by almost any resource measure, China overwhelms other members in the region of which it is a member (East Asian and Pacific). When coupled with China's expressed economic ambitions, it is reasonable to conclude activity reporting for this group primarily represents Chinese behavior.

Consistent with Mandiant's reporting of increasing cyber-enabled IP theft around 2010, DCSA data discloses an increasing relative MO focus on the same during the same period. In 2009 and 2010, SNA reporting increased from third to second-largest percentage of all reported activity, accounting for 28% in 2010.[71] SNA assumed the top MO position in 2011, and it peaked at 42% of overall reported activity in 2012. This jump in percentage further reflects a 245% increase of SNA reports year-over-year and a 1,443% increase in East Asia and the Pacific-attributed SNA reports from 2009–2012. Additionally, in the same period, the number of confirmed (not merely "reported") intrusions into cleared industries' unclassified networks grew by 1,138%.[72] In 2013, SNA was still the top MO at 30% of all reported activity.[73]

Over the 2010–2013 period, targeted U.S. industries are in technology areas consistently aligning with China's SEIs. For example, 2010 and 2011 reports align against all eight SEIs, comprising 58% and 43% of total reporting, respectively.[74] In 2012, SEI-aligned reports populate the top four targeted technology

---

[67] See Chapter I, Section 3 of *Reporting Requirements of the National Industrial Security Program Operating Manual*, 5220.22-M, February 28, 2006, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf.

[68] The DSS was renamed the Defense Counterintelligence and Security Agency in October 2019.

[69] "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry," Defense Security Service, 2011, https://premium.globalsecurity.org/intell/library/reports/2011/2011-dss-targeting-us-tech.pdf.

[70] From 2010–2012 DSS analyzed foreign interest in U.S. defense technology in terms of the 20 categories in the Militarily Critical Technologies List (MCTL) and switched over to the 29 sectors of the Industrial Base Technology List (IBTL) in 2013. For a review of the MCTL, see https://www.wrc.noaa.gov/wrso/security_guide/mctl.htm.

[71] "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry," Defense Security Service, 2012, https://www.dcsa.mil/Portals/69/documents/about/err/2012_Trend_Analysis_Report.pdf.

[72] "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry," Defense Security Service, 2013, https://www.hsdl.org/?abstract&did=757213

[73] "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry," Defense Security Service, 2014, https://www.dcsa.mil/Portals/69/documents/about/err/2014_Trend_Analysis_Report.pdf. Interestingly, this report notes that "The prominence of the SNA MO endured despite significant press coverage during FY13 detailing the results of Western research on and analysis of recent East Asia and the Pacific cyber activities. Reporting cataloged much of the infrastructure; command and control protocols; and tactics, techniques, and procedures (TTPs) East Asia and the Pacific cyber actors used. Industry submissions during the period immediately after the revelations decreased precipitately compared to the same period in 2012." They DSS authors are referring, of course, to the release of the Mandiant Report.

[74] "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry," Defense Security Service, 2012, op. cit.

categories—electronics; information systems; lasers, optics and sensors; and aeronautics—comprising nearly 35% of all reporting.[75] The top four are the same in 2013, and they comprise 20% of total reporting.[76]

Together, the DCSA and Mandiant reports support an argument that, around 2010, cyber-enabled IP theft from U.S. companies became China's primary method for facilitating engineering- and science-based innovation growth necessary for avoiding the MIT. Considered in light of analyses of the other technology transfer methods, it becomes clear why this is the case—cyber-enabled IP theft was the only method able to address simultaneously concerns regarding scale (thousands of IP targets), certainty (effective at acquiring IP), and immediacy (effective at acquiring IP hastily). This method does not address or preclude certainty regarding China's effectiveness in absorbing and actualizing acquired IP or immediacy in actualizing it against growth soon after acquisition. It has been argued that the absence of these aspects explains why, after acquiring U.S. fifth-generation jet fighter IP through cyber exploitation, China has, to-date, been unable to "re-innovate" it into a comparable fighter.[77] Thus, were Xi's 2015 confidence based on contributions from cyber-enabled IP theft, he would have needed evidence that re-innovation was, in fact, occurring. Such evidence existed.[78]

Successes in Re-innovation

In May 2014, U.S. federal prosecutors charged five PLA members with cyber intrusions into the computers of four U.S. companies from 2010 to 2012 with the objective to "steal information from those entities that would be useful to their competitors in China."[79] The five charged are allegedly members of Unit 61398. The companies targeted include SolarWorld, U.S. Steel, and Westinghouse. Additionally, in October 2018, prosecutors charged 10 Chinese MSS-affiliated persons with conspiring to steal sensitive, commercial technological, aviation, and aerospace data from numerous companies from 2010 to 2015 to support a Chinese SOE-led effort to build a turbofan engine of the same or similar design as developed by the targeted companies.[80] There is evidence that Chinese companies promptly re-innovated stolen IP from each of these companies to develop comparable, competitive, domestically produced products.[81]

---

[75] "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry," Defense Security Service, 2013, op. cit.

[76] "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry," Defense Security Service, 2014, op. cit.

[77] Andrea Gilli and Mauro Gilli, "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage," *International Security* (43:3, Winter 2018/19), 141-189, https://www.mitpressjournals.org/doi/full/10.1162/isec_a_00337. Lindsay and Cheung make a broader statement that skepticism is warranted

[78] Ibid. This evidence does not discredit Gilli and Gilli's arguments—rather, it suggests conclusions from their important, but highly specific, analysis of state-of-the-art weapons systems should not be generalized uncritically to other technologies and technological processes.

[79] United States District Court, Western District of Pennsylvania, *United States of America v. Wang Dong*, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui, Criminal No. 14-118, https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf.

[80] United States District Court, Southern District of California, *United States of America v. Zhang Zhang-Gui, Zha Rong, Chai Meng, Liu Chunliang, Gao Hong Kun, Zhuang Xiaowei, Ma Zhiqi, Li Xiao, Gu Gen, Tian Xi*, Case No. 13CR3132-H, https://www.justice.gov/opa/press-release/file/1106491/download.

[81] It generally takes a few years, from intrusion to indictment, before cases of cyber-enabled IP theft become public knowledge through published indictments. Thus, given recent FBI comments regarding the number of IP

SolarWorld, U.S. Steel, Westinghouse, and Capstone Turbine/CFM International

In 2012, when SolarWorld was bringing to mass production Passivated Emitter Rear Contact (PERC) solar cells, PLA operatives allegedly conducted at least 12 intrusions into SolarWorld's computers, acquiring detailed PERC manufacturing metrics, technological innovations, and production line information.[82] By early 2014, a Chinese-based solar rival, JA Solar, announced it was converting to PERC technology and began mass production of PERC in May of that year. In early 2015, Chinese-based Trina announced its own PERC conversion and, later that year, brought to the market a comparable PERC technology.[83] In 2017, testimony before a special committee of the U.S. Trade Representative, SolarWorld's AG CEO argued there was a clear connection between the IP theft and his Chinese rivals' rapid adoption of PERC technology, a technology that took SolarWorld eight years to develop.[84] Only 2–3 years after the IP theft, two Chinese SOEs were mass-producing the same technology.

Also in 2012, U.S. Steel filed an International Trade Commission complaint that a company researcher's computer was breached in 2011 and that plans were stolen for developing new steel technology that took a decade to develop.[85] The plans included the chemistry for the alloy and its coating, the necessary temperature for heating and cooling the metal, and the layout of production lines—the product was known as Dual-Phase 980, one of U.S. Steel's best performers. Two years after the alleged intrusion, Chinese SOE and steel giant Baosteel Group Corp. had a new line of products on the market. Among them: Dual-Phase 980.[86]

In 2008–2009, Westinghouse signed a technology transfer agreement with the State Nuclear Power Technology Corp to build four AP1000, third generation reactors. This progressed in 2013 to a joint venture for building four Chinese nuclear power plants and getting Chinese nuclear scientists and technology up to speed.[87] From 2010 to 2013, PLA operatives allegedly exfiltrated from Westinghouse's computers proprietary and confidential technical and design specifications for pipes, pipe supports, and

---

theft cases currently under investigation, we should expect to see more indictments from this same period. See Mark Hosenball and David Brunnstrom, "To Counter Huawei, U.S. Could Take 'Controlling Stake' in Ericsson, Nokia: Attorney General", Reuters, February 6, 2020, https://www.reuters.com/article/us-usa-china-espionage/top-u-s-officials-to-spotlight-chinese-spy-operations-pursuit-of-american-secrets-idUSKBN2001DL?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202.

[82] United States District Court, Western District of Pennsylvania, op. cit.

[83] United States of America Office of the United States Trade Representative, *Section 301 Investigation and Hearing: China's Act, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation*, October 10, 2017, https://ustr.gov/sites/default/files/enforcement/301Investigations/China%20Technology%20Transfer%20Hearing%20Transcript.pdf.

[84] Ibid.

[85] See John W. Miller, "Steelmaker Alleges Chinese Government Hackers Stole Plans for Developing New Steel Technology," *Wall Street Journal*, April 28, 2016, https://www.wsj.com/amp/articles/u-s-steel-accuses-china-of-hacking-1461859201 and David Lawder and Ruby Lian, "U.S. Panel Launches Trade Secret Theft Probe into China Steel", *Business News*, May 26, 2016, https://www.reuters.com/article/us-usa-china-steel-idUSKCN0YH2KX.

[86] Ibid.

[87] Kenneth Rapoza, "Westinghouse Electric's Chinese 'Trojan Horse,'" May 17, 2016, *Forbes*, https://www.forbes.com/sites/kenrapoza/2016/05/17/westinghouse-electrics-chinese-trojan-horse/amp/.

pipe routing associated with power plants Westinghouse contracted to build.[88] In December 2014, China's National Energy Administration approved a two-unit (HPR1000) construction plan for Fangchenggang Nuclear Power Plant (NPP) Project.[89] According to China Nuclear Power Group, the HPR1000, China's first third-generation reactor, "assimilates domestic and overseas experience on nuclear design, construction and operation."[90] One year later, Unit 3 of Fangchenggang NPP started construction, which was within four years of cyber-enabled theft of third-generation technical and design IP from Westinghouse.

Finally, in 2009, the state-owned Commercial Aircraft Corporation of China (COMAC) struck a deal with CFM International—a joint venture between U.S.-based General Electric's aviation business and French aerospace company Safran developing a new commercial aircraft engine called LEAP-X. The deal called for CFM to develop LEAP-X1C for China's C919 aircraft, a variant of CFM's LEAP-1C engine.[91] Around the same time, China's state-owned Assets Supervision and Administration Commission tasked both COMAC and the state-owned Aviation Industry Corporation of China (AVIC) with developing an "indigenously created" turbofan engine.[92] In June 2011, CFM International and COMAC signed a Memorandum of Understanding to study joint assembly—CFM and AVIC—of the LEAP-X1C engine in Shanghai, however, two years later, Chaker Chahrour, CFM's executive vice president, ruled out the joint assembly effort.[93]

Soon after COMAC signed the 2010 development deal, MSS cyber operators allegedly targeted Los Angeles-based Capstone Turbine, a manufacturer whose technology was key to the aircraft engine development.[94] Further, just over a year after Chahrour ruled out the assembly joint venture, MSS cyber operators allegedly intruded into networks in Safran's office in Suzhou, Jiangsu, China, exfiltrating proprietary information on LEAP-X.[95] In August 2016, the state-owned Aero Engine Corporation of China (AECC) was established, with COMAC and AVIC as main shareholders, to domestically manufacture an "indigenously created" turbofan engine for the C919. Just over a year later, they completed an assembly process for the first CJ-1000AX demonstrator engine, an engine closely resembling both the LEAP-X and

---

[88] United States District Court, Western District of Pennsylvania, op. cit.
[89] "China General Nuclear Power Group's Fangchenggang-3 Begins Construction with First Concrete Pour," China General Nuclear Power Group, January 8, 2016, https://electricenergyonline.com/article/organization/29681/559216/China-General-Nuclear-Power-Group-s-Fangchenggang-3-begins-construction-with-first-concrete-pour.htm.
[90] Ibid.
[91] Gopal Ratnam, "Underground Hackers and Spies Helped China Steal Jet Secrets Crowdstrike Researchers Reveal Beijing's Efforts to Boost Its Own Domestic Aircraft Industry," *Rollcall*, October 15, 2019, https://www.rollcall.com/news/policy/hackers-spies-helped-china-steal-jet-secrets-report-says. Note that from 2010 to 2015, MSS cyber operators allegedly targeted several other aerospace firms, including Ametek and Honeywell, who manufacture aircraft parts.
[92] Frank Fang, "Cybersecurity Firm Details How China Hacked Western Firms to Steal Aviation Tech," *The Epoch Times*, October 16, 2019, https://www.theepochtimes.com/cybersecurity-firm-details-how-china-hacked-western-firms-to-steal-aviation-tech_3118899.html.
[93] Keith Crane, Jill E. Luoto, Scott Warren Harold, David Yang, Samuel K. Berkowitz, and Xiao Wang, "The Effectiveness of China's Industrial Policies in Commercial Aviation Manufacturing," The Rand Corporation (2014), https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR245/RAND_RR245.pdf.
[94] United States District Court, Southern District of California, op. cit.
[95] Ibid.

LEAP-1C engines.[96,97] A CrowdStrike analysis concludes it is highly likely that AECC benefitted significantly from the cyber efforts of the MSS, knocking several years off CJ-1000AX's development time.[98]

A Qualified Success

Reported GDP figures support an argument that cyber-enabled IP theft and China's capacity to re-innovate that IP has kept China, so far, from falling victim to the MIT—the GDP reportedly averaged between 6.5 and 6.6% from 2015 to 2019.[99] When these data are coupled with a trend analysis of Global Innovation Index measurements for China, arguments for success find additional support—from 2013 to 2019, China's innovation measure rose, relative to all other states, from 35th to 14th, thus establishing itself in the group of leading innovative nations.[100] This climb arguably reflects progress in engineering- and science-based innovation previously argued as necessary for China to average 6.5% growth from 2015 to 2020. All of that said, qualifications are prudent. An upward adjustment to China's 2018 GDP, announced in November 2019 by China's National Bureau of Statistics (NBS), feeds skepticism regarding the accuracy of recent NBS figures, as the adjustment aligns with Xi's declared 2020 growth target.[101,102] Importantly, this adjustment may serve as evidence that U.S. tariffs, first imposed in January 2018, are exerting downward pressure on growth—pressure Xi did not anticipate when declaring growth targets in 2015. Indeed, Ding Zhijie, vice-president of the Beijing-based University of International Business and Economics who was recently appointed to head a think-tank under China's foreign exchange administration, argues that "China-US trade friction" is impeding China's ability to avoid the middle-income trap.[103] It may also be the case, as some argue, that China has *consistently* over-reported its growth for many years.[104] If this is the case, CCP concerns after the tariffs were levied were likely even

---

[96] Frank Fang, "Cybersecurity Firm Details How China Hacked Western Firms to Steal Aviation Tech", op. cit.
[97] Stephen Trimble, "China Completes Assembly of First High-Bypass Turbofan Engine," December 29, 2017, Flight Global, https://www.flightglobal.com/systems-and-interiors/china-completes-assembly-of-first-high-bypass-turbofan-engine/126587.article.
[98]Frank Fang, "Cybersecurity Firm Details How China Hacked Western Firms to Steal Aviation Tech," op. cit.
[99] International Monetary Fund, "Word Economic Outlook Database," https://www.imf.org/en/Countries/CHN#data. This same average is found in data provided by "Trading Economics: National Bureau of Statistics of China," https://tradingeconomics.com/china/gdp-growth-annual. World Bank data for 2017 to 2019 shows an average of 6.5% growth. The World Bank, https://data.worldbank.org/country/china.
[100] Cornell University, INSEAD, and WIPO, "Global Innovation Index 2019" (Ithaca, Fontainebleau, and Geneva, 2019), https://www.globalinnovationindex.org/userfiles/file/reportpdf/GII2019-keyfinding-E-Web3.pdf.
[101] "GDP Revisions Put China on Target to Double Economy, but Data Doubts Remain," *Reuters*, November 21, 2019, https://www.reuters.com/article/us-china-economy-gdp/gdp-revisions-put-china-on-target-to-double-economy-but-data-doubts-remain-idUSKBN1XW04C.
[102] A far more aggressive claim that China "falsifies economic statistics" has been made by the U.S.-China Economic and Security Review Commission. See "2019 Report to Congress of the U.S.-China Economic and Security Review Commission," November 2019, https://www.uscc.gov/sites/default/files/2019-11/2019%20Annual%20Report%20to%20Congress.pdf.
[103] Frank Tang, "China Set to Break Key Economic Barrier Despite Trade War, but Can It Avoid the Middle Income Trap?" *South China Morning Post*, January 1, 2020, https://www.scmp.com/economy/china-economy/article/3044124/china-set-break-key-economic-barrier-despite-trade-war-can-it.
[104] The emphasis on *consistently* is important. That China uses a consistent methodology year-over-year does not challenge the argument that growth was sustained post-2015. Rather, it argues for a caveat that growth was sustained but at a rate lower than NBS announced while being *consistent* with lower, unpublished rates from prior years. For a discussion of NBS' methodology, see Wi Chen, Xilu Chen, Chang-Tai Hsieh, and Zheng (Michael) Song,

more pronounced. Given its previous success, unsurprisingly, the CCP in 2018 ramped up another campaign of cyber-enabled IP theft to mitigate this unanticipated pressure, which could challenge its legitimacy and China's great power status. A second endogenous shock—novel coronavirus—is further straining growth. At a minimum, China may still escape the MIT by taking longer than anticipated to do so and while walking a knife's edge or, alternatively, may backslide to such a degree as to fall victim to the consequences of the MIT. The United States may be in a strong position to influence which outcome comes to pass.

Policy Implications

Although some argue the rise of China's economy is inevitable, CCP leadership's publicly expressed concerns suggest that the outcome is not pre-ordained. Nor should there be resigned acceptance that the CCP's economic trajectory targets cannot be influenced. President Xi's recent comment that a "lack of strength in innovation ability" is "the 'Achilles heel' of this lug of an economy of ours," a reprise of concerns expressed in 2010, invites a strategic response.[105] China's economy is, again, in a vulnerable state and the CCP is, again, seeking to secure its internal legitimacy and China's external status by jump-starting China's innovation engine through cyber-enabled IP theft. Today, however, the United States is far better postured in cyberspace than in 2010 to respond to this challenge (and opportunity).

Recognizing that previous cyber strategies were ineffective in curbing strategic gains adversaries were reaping through cyber campaigns short of armed conflict (including IP theft), DoD's *2018 DoD Cyber Strategy* argues that, in addition to deterring significant cyber events, it is necessary to "persistently contest malicious cyber activity in day-to-day competition" short of armed conflict.[106] This mission primarily falls to USCYBERCOM, which has operationalized it through a new strategic approach: persistent engagement, comprising operational concepts of anticipatory resilience, defend forward, and contest.[107] This active strategic approach, in turn, finds support in National Security Presidential Memorandum 13, in new/clarified authorities for cyber operations associated with the 2019 National Defense Authorization Act (which appear in 10 U.S.C. § 394), and, most recently, in the DoD General

---

"A Forensic Examination of China's National Accounts," *Brookings Papers on Economic Activity*, https://www.brookings.edu/wp-content/uploads/2019/03/bpea-2019-forensic-analysis-china.pdf.

[105] Ben Blanchard, "Lack of Innovation Is 'Achilles Heel' for China's Economy, Xi Says," *Reuters*, May 15, 2019, https://www.reuters.com/article/us-china-politics-xi/lack-of-innovation-is-achilles-heel-for-chinas-economy-xi-says-idUSKCN1SM08G.

[106] *Department of Defense Cyber Strategy* (Department of Defense, 2018), 4, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[107] *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (U.S. Cyber Command, February 2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

Counsel's framework for evaluating the legal sufficiency of proposed military cyber operations.[108,109] The most visible manifestation of persistent engagement is USCYBERCOM's efforts, through the Russia Small Group, to secure the U.S. 2018 mid-term elections by conducting operations allowing the United States to identify and counter threats as they emerged.[110] Given that most known Chinese cyber-enabled IP theft operations target cleared defense contractors or IT&C firms whose products and services support government and private sector networks, helping secure this group seems an appropriate USCYBERCOM mission. To be sure, this would be an operational challenge for USCYBERCOM and the interagency, but as noted by General Nakasone, it's the *use* of cyber capabilities that is strategically consequential, not their mere possession.[111] Importantly, this is not to argue a counter-IP theft cyber campaign is the only way of potentially shaping the rise of China's economy. Rather, it is to argue that at this particular strategic moment in time, given Mr. Xi's predilections, it would likely be the most effective.

---

[108] *United States Code Title 10-Armed Forces, Subtitle A-General Military Law, Part I-Organization and General Military Powers, Chapter 19-Cyber Matters, Section 394-Authorities Concerning Military Cyber Operations*, https://casetext.com/statute/united-states-code/title-10-armed-forces/subtitle-a-general-military-law/part-i-organization-and-general-military-powers/chapter-19-cyber-matters/section-394-authorities-concerning-military-cyber-operations.

[109] Honorable Paul C. Ney, Jr., "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," March 2, 2020, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

[110] United States Senate Committee on Armed Services Hearing, "Review Testimony On United States Special Operations Command and United States Cyber Command in Review on the Defense Authorization Request for Fiscal Year 2020 and the Future Years Defense Program," February 14, 2019, https://www.armed-services.senate.gov/imo/media/doc/19-13_02-14-19.pdf.

[111] "An Interview with Paul. M. Nakasone," *Joint Force Quarterly* (92, 1st quarter 2019), pp. 4-9, 4, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-04-20	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Opportunity Seldom Knocks Twice: Influencing China's Trajectory via Defend Forward / Persistent Engagement in Cyberspace	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Michael P. Fischerkeller	C5107
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	NS D-13135

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Institute for Defense Analyses 4850 Mark Center Dr., Alexandria, VA 22311	IDA
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Michael P. Fischerkeller

14. ABSTRACT

In 2010, after years of meteoric economic growth, the Chinese Communist Party (CCP) leadership was publicly expressing concerns about economic stagnation and social unrest—conditions CCP leadership associated with the middle-income trap (MIT). As part of a multi-faceted strategy to mitigate the MIT and stave off impending calamity, China launched a massive campaign of cyber-enabled theft of U.S. intellectual property (IP). Evidence of successfully re-innovating illicitly acquired IP was arguably behind President Xi's confident exclamation in 2015 that growth would average 6.5% from 2015 to 2020, a target necessary for keeping the MIT at bay. The United States' inability to abate China's campaign of IP theft, or willful choice to disregard it, was a lost opportunity to shape China's rise when its economy was in a vulnerable state. Opportunity is knocking again, however, as China's economy faces unexpected downward pressure from the Trump administration's tariff policy and novel coronavirus. To mitigate these pressures, the CCP has returned, again, to cyber-enabled IP theft. This time around, however, the United States has a new arrow in its quiver to act on this opportunity: a mature U.S. Cyber Command and a Department of Defense cyber strategy aligned to the challenge.

15. SUBJECT TERMS

China, persistent engagement, defend forward, intellectual property

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Institute for Defense Analyses
Unclassified	Unclassified	Unclassified	Unlimited	16	19b. TELEPHONE NUMBER (Include Area Code)