For an Enduring Advantage, Accelerate Adoption over Stymieing Theft

Whitney McNamara

While Beijing continues to make headlines for its increasingly aggressive incursions in Taiwan's air space,[1] rapid military buildup of major strategic weapons platforms,[2] and adoption of disruptive technologies like generative artificial intelligence,[3] another consequential yet stubborn threat remains: widespread espionage focused on the theft of critical intellectual property that underpins U.S. economic and military power.

China's "Made in 2025" initiative, released in 2015, was an ambitious 10 year plan to make China more competitive in ten critical high-tech industries including artificial intelligence, automated manufacturing, microelectronics, telecommunications, and aerospace. A crucial part of this strategy involves acquiring technology under a policy that encourages both state and private Chinese entities to adopt, understand, and innovate upon foreign technologies under the IDAR program, which stands for "introduce, digest, absorb, and re-innovate."[4] This approach allows China to capture foreign – largely U.S. – innovations and make enough modifications to claim

Whitney McNamara is senior vice president in the Technology and National Security Practice at Beacon Global Strategies where she leads their disruptive technology portfolio. Ms. McNamara is also a nonresident senior fellow at the Center for Strategic and Budgetary Assessments as well as the Forward Defense program of the Atlantic Council's Scowcroft Center for Strategy and Security. In this role, she supports the Commission on Defense Innovation Adoption and the Commission on Software Defined Warfare.

intellectual property rights over them and leverage their benefits.

Nearly ten years later, coincidentally, China has become the leading commercial and strategic competitor to the United States, and it's hard to argue they got here alone. Beijing leverages every tool in its toolkit to steal IP, from the seemingly innocuous courting and investing in foreign businesses, tech transfer agreements, and leveraging the benefits they incur from participating in international organizations like the World Trade Organization[5] to the more egregious, like espionage and large, sophisticated cyberattacks. Hacking is China's primary lever of espionage with FBI Deputy Director Paul Abbate stating Beijing leverages its extensive and sophisticated cyber theft program to conduct more cyber intrusions than all other nations combined.[6] According to the U.S. Department of Justice, 80% of its economic espionage cases are perpetrated by China.[7]

The PRC's reach for intellectual capital touches all pillars of the U.S. industrial base from academia, commercial industries, and the federal government; all institutions that benefit from the United States' entrepreneurial, risk-taking culture, large talent pools, predictable government policies, and ample flexible capital. An analysis of open source cyber intrusions of Chinese espionage notes that 29% were focused on acquiring military technology.[8] The thefts from academia are no less damaging to national security given over half of the Department of Defense's basic research budget is allocated to universities.[9]

Targeting of the U.S. commercial sector is similarly expansive, with FBI Director Christopher Wray warning Beijing was spying on companies everywhere "from big cities to small towns - from Fortune 100s to start-ups, folks that focus on everything from aviation, to AI, to pharma."[10] In fact, 54% of China's cyber espionage[11] incidents are aimed at obtaining commercial technologies and a survey of Chief Financial Officers estimates 1 in 5 U.S. corporations has had their IP stolen.[12] Even tech giants like Google have not been impenetrable with the Department of Justice charging Linwei Ding, a Chinese national, with stealing sensitive artificial intelligence that underpins advanced supercomputing capability from the company.[13] The challenge is particularly compelling when you consider some of the most advanced firms start out as small businesses, unlikely to invest in state of the art cybersecurity. Compounding the challenge is the voluntary IP transfer by some of the most tech proficient corners of U.S. commercial industrial base, providing the PRC with critical information and communication based technology (ICT) enablers, products, and access through academic partnerships and collaboration.[14]

The IDAR approach has potentially borne more fruit than Beijing could have anticipated when it comes to defense modernization: China's sixth-generation fighter jets, hypersonic weapons, missiles, and even infamous Chinese spy balloons seem to incorporate features of American technology, *Defense One* reported.[15]

While the estimated cost of intellectual property theft is the oft cited range of $225 billion to $600 billion annually[16], it's difficult to quantify or even qualify the impact this has likely had on Beijing's ability to meaningfully augment research programs, accelerate R&D timelines for advanced platforms, and better determine vulnerabilities in U.S. systems to generate countermeasures, to say nothing of the broad economic benefits the PRC has generated from the backs of U.S. innovation.

Efforts to Limit Technology Transfer

In the face of this persistent and consequential threat, the United States has enacted a series of ambitious reforms over

the last several years to stymie the flow of technology to Beijing: The Bureau of Industry and Security has strengthened its export control regulations particularly in areas such as semiconductors, artificial intelligence, and advanced computing[17]; the Committee on Foreign Investment in the United States (CFIUS) continues to expand its resources to assess foreign investments in U.S. companies and their potential impact on national security[18]; and there are new guidelines to restrict partnerships between U.S. research institutions and Chinese entities in critical technology areas.[19]

Although sweeping export control reforms will no doubt help stymie the flow of critical technologies to Beijing, total implementation will remain elusive. Rapid technological advancement means policy to manage it will consistently be behind the curve and plagued with loopholes to exploit, as government struggles to keep up.

It will also be nearly impossible to trace materials through the complex supply chain, particularly when PRC will likely use evasion tactics like intermediaries or shell companies to obscure their activities. For example, despite the 2014 Russia export controls, recovered Russian weapon systems in Ukraine contained U.S. and allied components, including semiconductor electronics manufactured years after the controls were enacted.[20]

In a CSIS report focused on export control enforcement, both Department of Commerce and U.S. Intelligence community officials admitted it can sometimes take the Russian or Chinese military days to set up a shell company to purchase U.S. technology, while the current process for uncovering a shell company's illegal activity may take years, if it is uncovered at all.[21]

We also know Beijing cannot be dissuaded from these activities. The trend in commercial espionage shows a dip after a 2015 agreement between President Obama and President Xi to restrict these activities but the decline was quickly reversed within a year.[22] Lastly, multiple government agencies will struggle to contend with the sheer volume of illicit activities our adversaries carry out. For example, the FBI, one of the lead agencies in countering Chinese espionage, faces resource limitation given the sheer volume of PRC driven espionage activities and the variety of methods they use.[23]

As a result, the United States is in a perpetual state of reactive footing which at worst, leaves them chasing the threat unsuccessfully and at best, puts them only one step ahead of Beijing. In the balance is precious taxpayer dollars across multiple government organizations being spent in the churn of activity.

While it is abundantly clear these measures are necessary to slow the flow of intellectual capital to Beijing, they are not a complete solution. As the United States and the PRC get closer to parity from both a military and technological standpoint, an enduring advantage can come from an organization that has institutionalized innovative practices to be able to rapidly adopt and leverage the benefits that come from technological advancement.

This is the perennial theme and the subject of voluminous efforts in the defense innovation space.[24] The challenges the Department of Defense faces in modernizing its force is how to adopt the advancements in technology into actual results that give the U.S. military an edge.

In a Congressional testimony to the U.S-China Economic and Security Review Commission, CSIS fellow Greg Allen explained that U.S.

adoption of stealth aircraft was done on the back of Soviet breakthroughs on stealth technology.[25] Despite having the foundational technology 9 years ahead of the U.S., the Soviet Union was never able to translate that discovery into stealth aircraft. The United States, conversely, successfully adopted the Soviet's initial breakthrough into a technology that would define the next era of military competition.

Mr. Allen's anecdote underscores that advanced research alone does not translate into true adoption and therefore meaningful innovation. This message is evergreen for those working on this problem set in and out of government: tech adoption for military advantage is never just about the technology.

Adopting Technology as a Solution

Historically, novel capabilities in the Department of Defense stemmed from top down, capital intensive, platform approach which incentivized rigid waterfall processes and silos of explicit responsibilities. This approach may have worked to develop complex platforms but likely left little room for adaptation or creative problem solving.

This is a particular challenge today when military advantage will not stem from one platform or type of technology like stealth or precision, but rather, from the creative combination of advancements in things like digitized command and control, software driven workflows, AI-driven intelligence, and autonomous systems. This puts a premium on the Department to be able to identify, procure, and adopt capabilities on significantly quicker timelines and work across silos to ensure these systems work together to achieve specific Service and Joint missions.

The Department of Defense still allocates a substantial portion of its budget to complex major systems that often rely on proprietary solutions. This reliance hinders interoperability and limits the potential force multiplication that could be achieved by connecting these systems effectively. The complexity of these individual platforms also means U.S. capabilities are less responsive to the evolving nature of threats to the U.S. military, and to the systems Beijing fields specifically to counter them.

Additionally, the Department of Defense's requirements and acquisition processes were established when it was a major funder of global research and development. However, by 2020, the federal government's share of national R&D had dropped below 20%.[26] Furthermore, innovations from noncommercial R&D organizations often lack a clear pathway for commercialization and adoption. Although the DoD invests billions annually in research and prototypes, only a small percentage successfully transition to production contracts that can generate the revenue needed for sustainable operations at scale.

Ultimately, while the Department is making great strides, it still is working towards being an organization that can quickly adapt the innovations in the commercial sector vice creating them indigenously.

A recent CSET report, "Build the Tech Coalition," presents a case study of the successful adoption of a complex AI-based decision support system by the 18th Airborne Corps.[27] When identifying the key pillars that enabled the rapid development of this operationally-relevant system, once dubbed "a holy grail for the Army," the technology's intellectual property is never once mentioned.

Rather, enablers that allow for a virtuous cycle of iterative learning and adaptation are cited as the key takeaways: experienced, technically literate leaders who understood how to take experimental success and turn them into acquisition outcomes, a process that facilitated quick feedback loops between

operators and engineers to rapidly develop, test, and improve the system; flexible contracting that allowed for experimentation and a diverse vendor pool that not only injected competition into capability development but reduced risk; and individuals from tech companies who knew how to iterate on solutions to solve warfighting problems.

The impact of battlefield innovations is no more germane than on the frontlines of Ukraine. In the Black Sea, the Ukrainians have continued to leverage waves of armed surface drones, combined with ballistic missiles provided from allies, to decimate nearly half of Russia's Black Sea fleet and preventing Russian access to Ukraine's southern coast. The Battle of the Black Sea represents the first time a country with no navy has won a naval battle.[28]

However, procuring and deploying drones is just the first step. Ukrainian operators say that it often takes less than a week for Russian and Ukrainian forces to find ways to trick algorithms and AI models.[29] For instance, placing tires on top of a tank can confuse a computer's vision and neutralize the system. In a potential war, DoD would need to ensure its operators had drones with reprogrammable software, leveraging advanced algorithms that are not only trained on real world data but have preexisting data pipelines in place to ensure the model is continuously getting retrained against intentional obfuscation.

To enable this, DoD would need buyers that are incentivized to buy cheap, software-defined drones with contracts that enable real time updates. The Department would also need to factor in time and resources for operators and technologies to experiment alongside one another, iterate on solutions, and create novel tactics, techniques, and procedures (TTPs) to creatively leverage these systems; a dedicated data collection and refinement effort for model training; robust, inherently well-governed pipelines for model training; and an iterative test and evaluation process to ensure systems don't attrit once deployed into the real world. Institutionalizing these pillars of innovation adoption would constitute the most important step in establishing an enduring advantage over the PRC.

Beijing's theft and appropriation of the U.S. industrial base's intellectual property is a severe challenge that deserves the attention of senior U.S. leaders. However, when the Department of Defense is at its best, it enables a cycle of eyewatering advancements that—by virtue of its sheer velocity and speed of delivery—can give it an enduring edge over the PRC. The Department must continue to accelerate its efforts to foster culture and processes that leverage these critical technologies, that takes them out of a move-countermove cycle, and provides a more enduring military advantage.

Endnotes

1. Guillermo. “Breaking the Barrier: Four Years of PRC Military Activity around Taiwan.” Foreign Policy Research Institute, 10 Oct. 2024, www.fpri.org/article/2024/10/breaking-the-barrier-four-years-of-prc-military-activity-around-taiwan.

2. Department of Defense’s Annual Report to Congress: Military and Security Developments of the People’s Republic of China, Department of Defense, 2023, media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

3. Bresnick, Sam. 2024, China’s Military AI Roadblocks, https://cset.georgetown.edu/publication/chinas-military-ai-roadblocks/#:~:text=China%20has%20made%20significant%20investments,developing%20and%20deploying%20these%20technologies.

4. Office of the United States Trade Representative. Findings of the Investigation into China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation. March 22, 2018. Pg 109. https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

5. Copan, W. G. (2024, October 15). China’s Ally in Stealing Western IP: The United States. Center for Strategic and International Studies. https://www.csis.org/analysis/chinas-ally-stealing-western-ip-united-states;

6. Lyngaas, Sean. “Chinese Hackers Cast Wide Net for Trade Secrets in US, Europe and Asia, Researchers Say.” CNN, 4 May 2022, www.cnn.com/2022/05/04/politics/china-hackers-economic-espionage-manufacturing/index.html.

7. United States. Justice Department. “Information about the Department of Justice’s China Initiative and Compilation of China Related Prosecutions since 2018. 2021. https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related.

8. Survey of Chinese Espionage in the United States Since 2000 | CSIS. (n.d.). https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000.

9. Congressional Research Services. (June 2022). Federal Research and Development (R&D) Funding: FY2024. (CRS Report: R47161).

10. Yong, B. N. (2023, January 16). Industrial espionage: How China sneaks out America’s technology secrets. https://www.bbc.com/news/world-asia-china-64206950.

11. Survey of Chinese Espionage in the United States Since 2000.

12. Jensen, Bejamin. Testimony of Dr. Benjamin Jensen, before the House Judiciary Subcommittee on Courts, Intellectual Property, and the Internet on “How the Chinese

Community Party Uses Cyber Espionage to Undermine the American Economy." 19 October 2013. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-10/ts231019_Ben_Jensen_Statement.pdf?VersionId=X6O2RFy0FkUeJS5Yxe3sKevSCWtnVogG.

13. Chinese national charged with stealing hundreds of secret AI files from Google. (2024, April 10). NBC News. https://www.nbcnews.com/tech/innovation/linwei-ding-google-software-engineer-alleged-thief-trade-secrets-rcna146623.

14. American Security Project. "CODE WAR: How China's AI Ambitions Threaten U.S. National Security." American Security Project, 2023. http://www.jstor.org/stable/resrep53845.

15. Corbett, T., & Singer, P. W. (2023, February 16). How the West May Have Helped Build China's Spy Balloons. Defense One. https://www.defenseone.com/ideas/2023/02/how-west-may-have-helped-build-chinas-spy-balloons/383029.

16. United States. Federal Bureau of Investigation. Executive Summary: China: The Risk to Corporate America. 2019. https://curtis.house.gov/uploadedfiles/china-executive-summary-risk-to-corporate-america-2019.pdf.

17. Fischer, N. A. (2024, September 12). BIS Imposes New Export Controls on Quantum, Semiconductor and Additive Manufacturing Technologies. Global Trade & Sanctions Law. https://www.globaltradeandsanctionslaw.com/bis-imposes-new-export-controls-on-quantum-semiconductor-and-additive-manufacturing-technologies.

18. Akin Gump Strauss Hauer & Feld LLP. (n.d.). CFIUS Continues to Expand Its Authority and Increase Enforcement Activity. Akin Gump Strauss Hauer & Feld LLP - CFIUS Continues to Expand Its Authority and Increase Enforcement Activity. https://www.akingump.com/en/insights/alerts/cfius-continues-to-expand-its-authority-and-increase-enforcement-activity#:~:text=CFIUS%20recently%20proposed%20to%20expand,of%20a%20real%20estate%20transaction.

19. Cimino-Isaacs, Cathleen, Sutter, Karen, M. (12 August 2024). Regulation of U.S. Outbound Investment to China. (CRS Report: IF12629). https://crsreports.congress.gov/product/pdf/IF/IF12629.

20. Mackinnon, A. (2024, February 27). Russia Is Evading Ukraine War Sanctions to Import Western Weapon Parts. Foreign Policy. https://foreignpolicy.com/2024/02/22/russia-sanctions-weapons-ukraine-war-military-semiconductors.

21. Allen, G. C., Benson, E., & Reinsch, W. A. (2024). Improved export controls enforcement technology needed for U.S. national security. https://www.csis.org/analysis/improved-export-controls-enforcement-technology-needed-us-national-security.

22. Survey of Chinese Espionage in the United States Since 2000.

23. Xue, X. (2023, March 17). US Experts Urge More Efforts to Thwart China's Acquisition of

US Military Technology. Voice of America. https://www.voanews.com/a/us-experts-urge-more-efforts-to-thwart-china-s-acquisition-of-us-military-technology-/7010346.html

24. See: McNamara, Whitney, Modigliani, Peter, MacGregor, Matthew, Lofgren, Eric. (2024, January) Atlantic Council Commission on Defense Innovation Adoption: Final Report. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/atlantic-council-commission-on-defense-innovation-adoption/; Work, Lord, Brown(2024, April 3). Innovation Adoption for All: Scaling Across the Department of Defense - War on the Rocks. War on the Rocks. https://warontherocks.com/2024/04/innovation-adoption-for-all-scaling-across-department-of-defense/; Department of Defense (2024 June). Aligning Incentives to Drive Faster Tech Adoption. Defense Innovation Board. https://innovation.defense.gov/Portals/63/20240701%20DIB%20Report_Aligning%20Incentives%20PUBLISHED%20STUDY_1.pdf.

25. Allen, G. C. (2024, April 29). China's Pursuit of Defense Technologies: Implications for U.S. and Multilateral Export Control and Investment Screening Regimes. Center for Strategic and International Studies. https://www.csis.org/analysis/chinas-pursuit-defense-technologies-implications-us-and-multilateral-export-control-and.

26. McNamara, Modigliani, MacGregor, Lofgren. (2024, January) Atlantic Council Commission on Defense Innovation Adoption: Final Report. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/atlantic-council-commission-on-defense-innovation-adoption/

27. Probasco, Emily. (2024, August). "Building the Tech Coalition." Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/building-the-tech-coalition.

28. Williams, B. G. (2024, July 19). How the Ukrainians – With No Navy – Defeated Russia's Black Sea Fleet. Military.com. https://www.military.com/daily-news/2024/07/19/how-ukrainians-no-navy-defeated-russias-black-sea-fleet.html

29. Bondar, K. (2024, October 15). Closing the Loop: Enhancing U.S. Drone Capabilities through Real-World Testing. Center for Strategic and International Studies. https://www.csis.org/analysis/closing-loop-enhancing-us-drone-capabilities-through-real-world-testing#:~:text=In%20conversations%20with%20CSIS%2C%20Ukrainian,vision%20and%20confuse%20the%20system.

SALVE
THE PELL CENTER

About the Pell Center

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

www.pellcenter.org