Technology Protection: Securing Modernization Efforts

Illustration by Emma Morris, MIPB

by the Directorate of Intelligence and Security, U.S. Army Futures Command

Introduction

The U.S. Army established Army Futures Command (AFC) to realign elements of the modernization efforts and bring unity of effort to the development process of the future force. The Army is modernizing **how we fight, what we fight with,** and **who we are as an Army.** Ensuring the Army is able to "fight tonight" while also actively seeking next-generation solutions to stay ahead of potential adversaries is fundamental to the modernization strategy. Equally fundamental, is safeguarding those solutions throughout the development and fielding processes. The AFC initiatives to safeguard technology innovations highlighted in this article are threat awareness, the protection of critical technology in order to deliver uncompromised technology to the force, and the development of more stringent disclosure programs.

Threat Awareness

Education on threats to innovation and intellectual property is the first step to protecting the technologies used in our future systems. The education program is a continual requirement that should focus on the current methodologies of near-peer adversaries to acquire U.S. intellectual property and the status of their game-changing technologies. The overall theft of U.S. intellectual property and technology has occurred on a scale that affects our national security. The financial loss from the theft of U.S. trade secrets is estimated to be as much as $540 billion annually, resulting in years of wasted research and development and lost jobs.[1] It also places the United States at risk for losing our leadership in advanced technologies. The AFC/Army's challenge is to introduce applicable security practices at the moment of ideation for a new technology that could potentially overmatch an adversary. Timing is important because ideation occurs early in a project, during the generation and development of a new idea.

China is a prime example of a current adversarial challenge the Army faces. Over the past several decades, China and our other adversaries developed new and improved methods for acquiring United States technology. These new approaches are significant, as Director of the Federal Bureau of Investigation Christopher Wray stated in 2018: "I think China, from a counterintelligence perspective, in many ways represents the broadest, most challenging, most significant threat we face as a country. And I say that because for them it is a whole of state effort. It is economic espionage as well as traditional espionage; it is nontraditional collectors as well as traditional intelligence operatives; it's human sources as well as cyber means."[2]

Director Wray also sheds light on new methods of theft of intellectual property, from American academia and businesses to the traditional espionage of government secrets and legal but targeted business acquisitions. However, near-peer adversaries have increased their efforts to collect our ideas, thoughts, and research; their sources are American

university campuses, corporate boardrooms, government-sponsored research sites, and military offices. Through the Chinese Communist Party, China is able to fund these ventures, lending them money via their industrial policy, which gives Chinese companies an economic advantage and enables them to grow significantly. In 2010, for the first time, a Chinese organization was among the world's top 10 largest public companies on the Forbes Global 2000 list. In 2020, 5 of the 10 largest companies on that list were Chinese. Of the remaining five, four were U.S. companies.[3]

China's strategic goal is to obtain comprehensive national power through economic development by dominating its domestic markets and then by becoming a global leader, particularly in advanced technological disciplines. To achieve its strategic goals, China relies on a top-down, state-directed approach. As many as 100 different plans guide China's foreign acquisition in science and technology, making the effort broad in scale and influence. Among the most prominent are the Five-Year Plans and the Made in China Plan, also known as MIC 2025.

What is Made in China 2025?

The Chinese government has launched "Made in China 2025," a state-led industrial policy that seeks to make China dominant in global high-tech manufacturing. The program aims to use government subsidies, mobilize state-owned enterprises, and pursue intellectual property acquisition to catch up with—and then surpass—Western technological prowess in advanced industries. [It] is the government's ten-year plan to update China's manufacturing base by rapidly developing ten high-tech industries. Chief among these are electric cars and other new energy vehicles, next-generation information technology (IT) and telecommunications, and advanced robotics and artificial intelligence.[4]

To enact those plans, China uses multiple techniques, including legal business means, science and technology investments, mergers and acquisitions of United States companies, and legal means in academia. The People's Republic of China recruits individuals in those environments to acquire United States technology. While these individuals may not be trained intelligence officers, they are working for an intelligence officer and are considered co-opted by a Chinese intelligence service. When China recruits individuals who are in the private sector and academia to acquire United States technology, we refer to them as "nontraditional collectors" because they are not employees of the Chinese government and are not employed as intelligence officers.

Assistant Attorney General John C. Demers clearly captured China's efforts in a testimony before the Senate Judiciary Committee in 2018, stating, "In all of these cases, China's strategy is the same: rob, replicate, and replace. Rob the American company of its intellectual property, replicate the technology, and replace the American company in the Chinese market and, one day, the global market."[5] In order to stop the assault on the American economy and our status in the world, intelligence and security must work hand in hand with other government agencies to reach out to academia and businesses to educate them on the threat to their intellectual property and, by extension, national security, and we must do it early.

Protection of Critical Technology

Under the 2019 National Defense Authorization Act, Congress required the Secretary of Defense to establish cross-functional teams to tackle specific high-priority initiatives and complex problems that crosscut the Department of Defense (DoD) enterprise. In 2018, the Secretary of Defense chartered one such group, aptly named the Protecting Critical Technology Task Force (PCTTF). Its goal is to secure the defense industrial base and the research and development enterprise by **preventing loss of classified and controlled unclassified information, as well as inhibit the data exfiltration** of trade secrets by foreign adversaries. The PCTTF immediately began working on new standards to integrate security and intelligence into the requirements development and acquisition process, as well as developing strategies to counter foreign threats to secure national security and America's military superiority.

At the same time the DoD created the PCTTF, the Secretary of the Army established AFC to address several challenges to modernization, including a dispersion of effort and inability to modernize at speed or scale. This lack of unity of command and accountability, combined with the loss of information and intellectual property that Congress had identified, have begun to erode the lethality and survivability of Army forces. Thus, AFC's mission was not only to focus on modernization strategies but also to deliver the investments uncompromised.

AFC immediately began assessing technology protection gaps in the Army acquisition, security, and intelligence enterprises. Drawing from best practices of sister organizations and the expertise of PCTTF members, a multi-disciplined team created a plan to improve the protection of early technology development. This new strategy focuses on weaving security, intelligence, and counterintelligence into the acquisition process during the ideation process. AFC's science and technology investments now focus on key modernization efforts approved through a single command structure instead of disparate offices that lacked a cohesive vision.

This process allows our researchers and technologists to understand the existing and future battlefield gaps identified by intelligence and threat analysts, not just the collaborative research world, which can lack connection to the Army mission. Further integrating intelligence into science and technology planning allows the assessment and mitigation of threats before the initiation of new programs and iteratively throughout a project. Security experts are involved in the early research planning to validate appropriate acquisition strategies and funding mechanisms, develop protection measures, and ensure the appropriate application of multi-disciplined security constraints throughout each phase of work. Each of these efforts is designed to ensure future fielded systems can truly be delivered uncompromised.

Development of More Stringent Disclosure Programs

Weaving security, intelligence, and counterintelligence into the acquisition process during the ideation phase includes the introduction of security policies and tools such as disclosure guidance. AFC's disclosure program initiative created an analytic template for new and current technology development efforts. The template is a four-step process, described in detail below:

- Analysis and data identification.
- Audience category identification.
- Risk analysis and disclosure development.
- Dissemination.

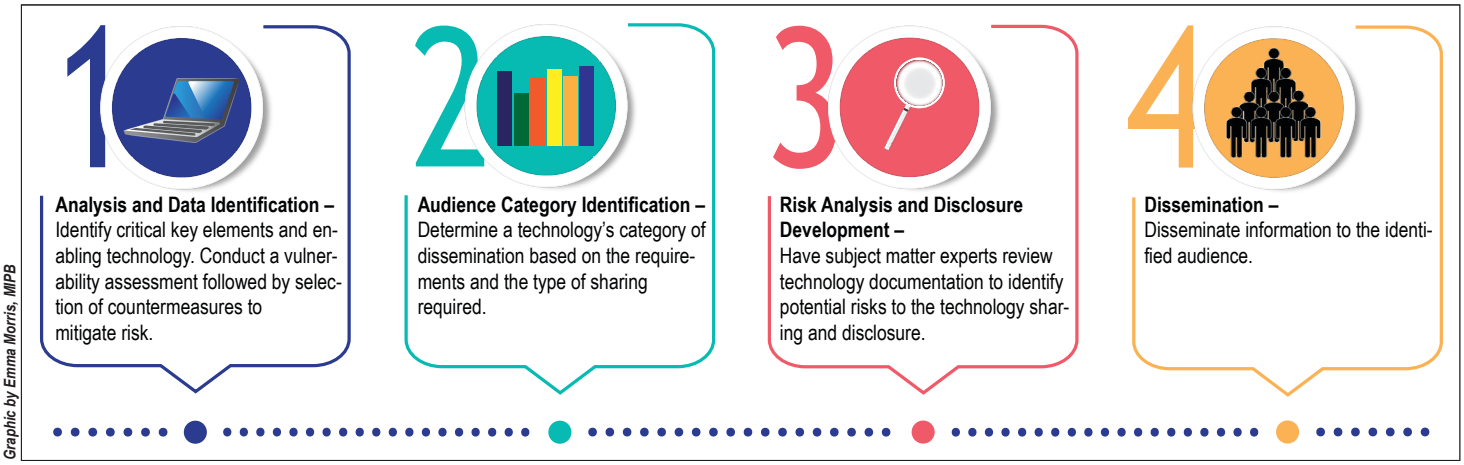
Analysis and Data Identification. This step begins with the completion of a science and technology protection plan, which requires identification and a vulnerability assessment of critical enabling technologies, followed by a selection of countermeasures to mitigate the identified risks. Following this is the use or creation of a program protection plan. The creation of this plan requires the identification of critical program information, controlled technical information, critical supply chain elements, and any horizontal protection considerations. When complete, the analysis and data identification process will have identified and documented key elements of technology that may be deemed—

- Revolutionary.
- Critical to system performance.
- Perishable (easily countered).
- Enabling to other systems.
- Sensitive to supply disruptions.
- Sharable with industry or foreign partners.
- Enabling for another DoD system.

Audience Category Identification. Audience category identification is a deliberate process to differentiate between categories based on requirements and the type of sharing required. Coordination with subject matter experts (SMEs) is essential to the successful execution of audience categorization. The following dissemination categories should be considered at the inception of every development effort:

- **Public dissemination:** Unlimited dissemination—known to be a source for adversary and partners alike.
- **Controlled dissemination:** Dissemination under controlled unclassified information specific to technology developments and used to protect information within audiences that have a need-to-know.
- **Limited dissemination:** Dissemination limited to specific audiences such as partner nations, briefings/symposiums, contractors, and academia.

Identifying the audience of a technology development effort from inception and maintaining that information throughout the life cycle of a technology development fosters effective communication while protecting information key to the sustainment of a U.S. technological advantage.



Graphic by Emma Morris, MIPB

A stringent disclosure program is a fundamental safeguarding solution to the U.S. Army Future Command's modernization strategy.

Risk Analysis and Disclosure Development. Risk analysis occurs once a technology is mature and after identification of data sharing requirements. The risk analysis includes gathering the appropriate documentation on the technology and having SMEs review the information to identify potential risks to technology sharing and disclosure. The SMEs include—

- Technology owner representatives.
- Program managers.
- Technology SMEs.
- Research and technology protection officers.
- Foreign disclosure officers.
- Operations security officers.
- Information security officers.
- Legal staff.

The SMEs determine risk based upon the state of technology, type of application, audience required for continued development and integration, plan for transfers to foreign partners, and anticipated disclosure. With the appropriate documentation in place, the SMEs conduct a comprehensive analysis to determine the risk to adversary exploitation. The following are some the documents that should be available for the analysis:

- Science and technology protection plan.
- Security classification guides (draft or approved).
- Program protection plan.
- Critical information lists.
- Critical programs and technologies list.
- Horizontal protection list.

Dissemination. The final step is disseminating information to the required audiences and using the classification guide or other controls that were established based on the risk analysis.

Conclusion

Securing the modernization efforts that will transform our force to compete in the future operational environments is not an easy task. Understanding how the threat to our modernization efforts has changed, understanding the ability of potential adversaries to inform our science and technology efforts, and protecting our intellectual property from inception to fielding and sustainment are all key factors for success. AFC and its partners are leading the way to change the existing paradigm and build a flexible process that adjusts to the ever-changing threat environment.

Endnotes

1. Sherisse Pham, "How much has the US lost from China's IP theft?" CNN Business website, March 23, 2018, https://money.cnn.com/2018/03/23/technology/china-us-trump-tariffs-ip-theft/index.html.

2. Tara Francis Chan, "FBI director calls China 'the broadest, most significant' threat to the US and says its espionage is active in all 50 states," Business Insider, July 18, 2018, https://www.businessinsider.com/fbi-director-says-china-is-the-broadest-most-significant-threat-to-the-us-2018-7.

3. Andrea Murphy, Hank Tucker, Marley Coyne, and Halah Touryalai, "Global 2000, The World's Largest Public Companies," Forbes, May 13, 2020, https://www.forbes.com/global2000/#612237ff335d.

4. James McBride and Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?" Council on Foreign Relations website, May 13, 2019, https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.

5. *China's Non-Traditional Espionage against the United States: The Threat and Potential Policy Responses: Hearings before the Committee on the Judiciary United States Senate* (2018) (statement of John C. Demers, Assistant Attorney General, National Security Division, U.S. Department of Justice), 5, https://www.judiciary.senate.gov/imo/media/doc/12-12-18%20Demers%20Testimony.pdf.

The Directorate of Intelligence and Security, U.S. Army Futures Command, orchestrates the evaluation and assessment of current, emerging, and future threats and the development of the operational environment; synchronizes multi-disciplined technology protection activities; and conducts intelligence and requirements integration for the Future Force Modernization Enterprise to build a multi-domain operations (MDO)-capable force by 2028 and an MDO-ready force by 2035.