Protecting America's Defense Industrial Advantages in Cyberspace

By Travis D. Howard, CISSP

The opinions expressed herein are the author's own and in no way reflect the official position of the United States Government, Department of Defense, or the Navy.

The greatest cyber hazard facing America's national security is not a new zero-day exploit or fancy-coded malware. The biggest, long-term threat to national security is the rampant exfiltration of America's technological advantages from the defense industrial base. The U.S. government is working to better manage information risk, but these efforts require private sector buy-in and stronger partnerships with industry in a holistic, one-team-one-fight approach. Failure to do so will incur additional risk that could erode America's military supremacy and put future strategies, plans, and even service-members in danger.

> "The biggest, long-term threat to national security is the rampant exfiltration of America's technological advantages from the defense industrial base."
>
> - Travis D. Howard, CISSP

It was the ancient Chinese military theorist, Sun-Tzu, who said, "subjugating the enemy's army without fighting is the true pinnacle of excellence." The United States never really internalized the Taoist military strategies of the east, despite studying it for years. With a fondness for strategies developed by European thinkers such as Carl von Clausewitz and Alfred Thayer Mahan, America and her allies have always sought to end confrontations with decisive and overwhelming power. Cyber conflicts have become no exception.

Since the creation of U.S. Cyber Command, resources for cybersecurity have been pouring into America's impressive military and signals intelligence engines, but the greatest threat to U.S. military supremacy in the 21st century goes largely unchecked. For years, the industrial base the military depends on has been bleeding information critical to U.S. defense technology, future programs, and decisive infrastructure. Efforts are underway to empower government agencies to partner with the industrial base against this threat. Now, they must move with all possible speed or face unacceptable risk in a future conflict with a near-peer competitor. It is a complex problem, and while not entirely military in nature, Sun-Tsu said it best in his seventh book: "In military combat what is most difficult is turning the circuitous into the straight, turning adversity into advantage." With so much at risk and many actions already late-to-need,

both the federal government and the industrial base must now move at best possible speed to arrest this alarming trend by closing vulnerabilities and finding ways to impose heavier costs on adversaries.

The Erosion of America's Industrial and Military Supremacy

A 2018 report by cybersecurity firm BitSight noted that, "a security performance gap exists between the U.S. federal government and its contractor base," and that many contractors were failing to meet the prescribed cybersecurity controls as outlined in their contracts. From the government's perspective, a focus on affordability and fostering fair competition within the industrial base has translated to accepting information risk in technology programs that many consider critical to U.S. national security. This failure is not solely located within the defense industrial base, but several of the sixteen critical-infrastructure sectors outlined within Presidential Policy Directive 21 (PPD-21). The effect is an erosion of America's advancements in emerging defense technology, both domestic and military, which could ultimately result in adversarial capabilities equaling or even out-performing allied forces in the next military conflict.

> "The highest realization of warfare is to attack the enemy's plans; next is to attack their alliances."
>
> - Sun-Tzu

According to Sun-Tzu, "the highest realization of warfare is to attack the enemy's plans; next is to attack their alliances." Theft of critical infrastructure and defense information from the industrial base attacks America's plans, forcing costly changes to major programs and research projects. Beyond the impact on America, China's penchant for stealing information to use in their own programs and China and Russia's influence campaigns could also disrupt the competitiveness of the international industrial base. Perhaps they have already done so, as we seem to discover incidents far after they have happened. It is clear that America's adversaries have a very different definition of information warfare than we do, one that embraces the strategies of Sun-Tzu, and perhaps Mao Zedong, over von Clausewitz or Mahan.

Turning the Circuitous into the Straight

2014 was a landmark year for federal lawmakers looking to improve America's cybersecurity posture in critical-infrastructure sectors. According to a recent report from the Congressional Research Service, five bills aimed at strengthening federal and industrial cybersecurity were signed by President Obama that year: the first bills on the subject since 2002. At the same time, the 113th Congress codified the National Institute for Standards and Technology's (NIST) responsibility to develop standards to reduce risk, strengthened the Department of Homeland Security's mandate to coordinate with the private sector, improved the federal cyber workforce, and updated the Federal Information Security Management Act.

While defensive efforts within the energy and financial sectors have been underway, actions to protect the defense sector have lagged. Congress began addressing the challenge through the 2018 and 2019 National Defense Authorization Acts which directed the Department of Defense (DoD) to develop a framework for increasing cybersecurity standards within the defense industrial base. This work was already underway when the bill was signed by President Trump. These standards, dubbed the Cybersecurity Maturity Model Certification (CMMC), have been developed in full cooperation and transparency with the industrial base, receiving significant attention, and even praise, in 2019. The standard is set to go into effect in 2020 for a limited number of new contracts; DoD has stated that full implementation for all contracts can be expected by 2026.

The CMMC seeks to enhance the protection of sensitive data using a certification process to measure a company's ability to protect controlled unclassified information that, if stolen and aggregated, could pose a grave risk to national security. DoD contracting officers would seek a higher certification level for a list of critical programs and technology as developed by Pentagon officials. In partnership with this effort, NIST is working to release an update to its publication, 800-171, intended for use by federal contractors. It will include the 31 new cybersecurity controls that CMMC will leverage in its certification levels, including hardened identity management and access controls, separating government and contractor data through network segmentation, and, for the highest levels, employing threat-hunting teams and a continuously monitored security operations center.

Despite a slow response to the theft of defense technology from the industrial base, America is not without an impressive array of defensive options. Chief amongst them is the still-growing U.S. Cyber Command and its partnership with the intelligence community, specifically the National Security Agency. Efforts are well underway to develop the Cyber Mission Force's (CMF) Unified Platform, which is a network of networks that will give military cyber operators a joint environment for developing and employing offensive and defensive tools. Additionally, Cyber Command is pressing forward with a new defend forward strategy that has elements of the CMF working with partner nations to seek and defeat cyber threats before they reach America's network boundaries. The coupling of the intelligence community with cyber operators has resulted in several success stories, including protecting the U.S. elections in 2018.

Turning Adversity into Advantage

Solutions are in motion, but America has yet to create a bulwark to defend the industrial base. The CMMC is untested, the NIST revisions are, as of this writing, still drafts and not yet prescriptive. As both are fully implemented, 2020 will be a pivotal year. Yet, an industrial base that dislikes over-regulation and a changing competitive landscape has already started to push back. Congress has already weathered pressure from lobbyists and constituent defense corporations who question measures that appear, to them, to be mainly reactionary while harming contractor competitiveness by incurring additional costs.

Self-regulation would do much to shore up defenses in the industrial base, as the biggest defense contractors in America employ hundreds of subcontractors to carry out a plethora of massive defense projects, including Boeing, Lockheed Martin, Northrop Grumman, Raytheon, and General Dynamics. If these five demand greater visibility into their subcontractors' supply chain management and cybersecurity controls and offer help in the form of technical assistance or contractual incentives, it would go a long way to stopping cyber intrusions that, so far, have gone undetected. An often-used example of successful self-regulation comes from safety and quality assurance in automotive industry, yet history has repeatedly shown that same industry avoiding emissions regulations. It is evident that some government regulation and resources must be contributed to protect critical military information from cyberattacks as self-regulation will only go so far.

Federal executive agencies and departments must be prepared to leverage their resources as part of the solution. DoD's new $10B Joint Enterprise Defense Infrastructure contract with Microsoft has the potential to offer fit-for-purpose cloud services for defense contractors looking to store government information in a secure location within a militarily protected perimeter. While there will most certainly be cost and contractual issues to work out, such an offering can ease the burden of smaller defense contractors with limited data storage needs, such as small parts manufacturers. A solution might be for the prime defense contractors to offer cloud services to their subcontractors, which the government could incentivize through their agreements with the primary defense contractors.

Finally, law enforcement and the intelligence community play a big part in shedding light on the adversarial actions against the industrial base. Much of this advantage comes from addressing the advanced persistent threats (APTs) that smaller, private firms are unlikely to detect, much less deter. Passing classified cyber intelligence reports to key defense contractors with cleared analysts must increase, including tactical and technical information such as known malware hashes and attack vectors for APT groups. Cyber Command's CMF has garnered praise for already doing this.

Conclusion

America's industrial base is under siege from adversaries who would undermine our military superiority while advancing their own with our technology. Perhaps more alarming is that this cyber threat is not exclusive to critical infrastructure; according to a 2019 article in Fortune, a CNBC poll found that one in five American corporations were the victim of intellectual property theft by China. This represents an existential threat to America's economic prosperity from another major world power, yet there are no military forces engaged in physical combat. Military strategists such as Sun-Tzu explain how this deceptive warfare is being used against the United States: "display profits to entice them; create disorder and take them."

Within the defense industrial base, efforts like the CMMC, NIST updates to standards, and renewed pressure from lawmakers have thankfully created a surge of effort to close security

gaps and better manage information risk. The CMMC is a great tool in DoD's tool belt to manage this risk, but it must be coupled with the intelligence community's support of cyber defense efforts, industry self-regulation, and law enforcement activity. Only a unified effort will keep America's sensitive defense information where it belongs: in the hands of industrial partners who will turn it into a decisive advantage for America's warfighters and allies in the next great power conflict.

About the Author

Travis D. Howard is an information technology and cybersecurity practitioner with over 20 years of experience. He has been an ICIT member since 2019 and served a full career in the U.S. Navy as an information warfare officer. He holds graduate degrees in business administration and cybersecurity policy, and is a certified information systems security professional. Connect with him on LinkedIn or find him on Twitter @travishoward191.

About ICIT

The Institute for Critical Infrastructure Technology (ICIT) is a 501c(3) cybersecurity Think Tank with a mission to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders.

References

1. Ralph D. Sawyer (ed.). *Sun-Tzu: Art of War*. 1994, Westview Press Inc: Boulder, CO

2. Derek B. Johnson. "With defense contractors in the crosshairs, NIST rolls out new cyber guidelines." FCW.com, Nov 27, 2019. Retrieved from https://fcw.com/articles/2019/06/21/nist-dib-cyber-contractor-threat.aspx

3. U.S. Department of Defense. *Cybersecurity Maturity Model Certification (CMMC), Draft version 0.6.* Nov 7, 2019.

4. Erik Sherman. "One in Five U.S. Companies Say China Has Stolen Their Intellectual Property." Fortune.com, Mar 1, 2019. Retrieved from https://fortune.com/2019/03/01/china-ip-theft/

5. National Institute for Standards and Technology (NIST). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Draft Special Publication 800-171.* June 2019.

6. Rita Tehan. *Cybersecurity: Legislation, Hearings, and Executive Branch Documents.* Congressional Research Service, Nov 8, 2018. Retrieved from https://fas.org/sgp/crs/misc/R43317.pdf

7. BitSight. "Beyond Uncle Sam: Analyzing the Security Posture of the U.S. Government Contractors and Subcontractors." 2019. Retrieved from https://info.bitsight.com/analyzing-security-posture-us-government-contractors-social