AMERICAN ENTERPRISE INSTITUTE

Statement before the House Committee on Armed Services
Subcommittee on Cyber, Innovative Technologies, and information Systems
On Innovation Opportunities and Vision for the Science and Technology Enterprise

Creating a More Agile and Secure Defense Innovation Base

Mr. Klon Kitchen
Resident Fellow

February 23, 2021

The American Enterprise Institute (AEI) is a nonpartisan, nonprofit, 501(c)(3) educational organization and does not take institutional positions on any issues. The views expressed in this testimony are those of the author.

Introduction

Good afternoon Chairman Langevin, Ranking Member Stefanik, and members of the subcommittee. Thank you for this opportunity to testify.

There is good reason for the United States and its citizens to be optimistic about our future. Our technology and innovation industries remain the envy of the world – pioneering technological discoveries and applications that are the foundation of our national prosperity and security.

These advantages, however, are not inevitable and deliberate action is required for the United States to maintain its leadership and to protect its people and interests. I would like to briefly describe two features that should define our policies going forward.

The Strategic Context

First, we must understand how and why the technology sector of our economy is growing in influence and importance within military and national defense decision making.

National security is a team sport – and not just among America's myriad government departments and agencies. While the United States Constitution makes the federal government responsible for ensuring the "common defense" of the nation, individual citizens, civil society groups and private companies have always helped shoulder this burden. This remains unchanged.

What is changing is the distribution of this burden among these stakeholders – particularly private companies.

The technologies that will determine the United States' ability to secure its people and interests are overwhelmingly being developed for commercial purposes in the private sector. It is highly unlikely the government will create its own, distinct capacity to create and distribute these technologies in the near- to mid-term.

This leaves the national defense more dependent on the private sector than ever before, precisely as China is emerging as a true-peer competitor and rival economically, technologically, and militarily.

China also recognizes this migration of the national security burden into the private sector and is responding with what its leaders call "military-civil fusion." This is a form of governance where the Chinese Communist Party (CCP) co-opts Chinese companies and employs them as an extension of the state's political, economic, military, and intelligence enterprises.

This, for example, is the root of Western concerns with Huawei: the potential for a Chinese telecommunications behemoth that has used government subsidies to dramatically undercut Western competitors to build a monopoly over infrastructure that – under Chinese law – could be used as a global surveillance network for Beijing.

All of this adds up to an unavoidable truth: the ability of the United States to invent, design, build, deploy and secure advanced technologies – and their key components – is as important to national security as the nation's capacity to field traditional military capabilities. With this in mind, it follows that new partnerships between the government and industry are essential.

That's not to say the United States should try to "out China" China. America's model of non-coercive private-public cooperation is agile, productive, and fair. But this model only works when partnerships between the government and the free market are voluntary. Naturally, this requires technology firms to act from a shared sense of responsibility – a shared sense that was understandably undermined by a number of events, most notably the illegal disclosures of NSA contractor Edward Snowden. That was seven years ago. We have to move on and we have to do better.

It's not all bad news. Despite these challenges, the world's largest, most profitable and most innovative technology companies are still American companies. While Chinese tech firms are catching up (and fast), the U.S. still holds the advantage. But it is time to use it or lose it.
This requires two adjustments.

The government, for its part, must accept the reality that it is *a* national security stakeholder and not *the* stakeholder. Many of the world's leading technology companies have global interests and influence on par with many nations – they have a legitimate place at the geopolitical table. This isn't hyperbole. Apple's annual revenue exceeds the GDP of Portugal.

This shift in perspective will be as important as our efforts to devise new applications and tactics for employing new capabilities. As my colleague Kenneth Pollack observes:[i]

> The world is shifting from the industrial age to the information age. That transformation has profound implications for warfighting. In the most obvious fashion, new technologies will have a direct impact on combat operations, transforming what is possible and how best to accomplish military ends. However, major technological shifts also exert an indirect impact on military affairs by transforming other aspects of society that will in turn dictate the organization, resources, goals, abilities, and constraints that nations and other groups bring to warfare. As it always does, technology is reshaping economies, political systems, cultures, and organizations of every kind. Although these indirect effects are often less obvious, they are typically no less important.

More concretely, Washington can best demonstrate its intent to be a true partner with the tech industry in the way it shares information and acquires new capabilities.

For too long, the U.S. government has treated information exchange with industry as a one-way street – demanding "real-time" information sharing from private companies on cybersecurity and other threats while being painfully slow in sharing with industry its own insights about malicious actors, their intentions and their capabilities.

This posture increasingly means that it is the government, not industry, who is being left behind. It was the private sector, after all, who discovered and alerted officials to the massive "Holiday Bear" supply chain attack (aka, the SolarWinds attack) that compromised hundreds of public and private networks – the impact of which we still no not fully understand.

There are early signs this might be changing. The NSA's release of its Ghidra tool is a good example of the government proactively treating industry as a partner. This software reverse engineering framework was developed by Fort Meade for the NSA's national security mission, but its release to the public allows private sector security personnel to better defend themselves as well.

Likewise, when Cyber Command publishes fresh malware samples used by U.S. adversaries in public repositories, it democratizes access to information all network defenders need to protect themselves.

Less progress is being made in government purchasing and procurement, where a rigid and outdated acquisition bureaucracy makes it difficult for new technology companies to help Washington. Tech companies thrive when they spend precious resources on engineers and coders, not on hordes of contract specialists and lawyers.

Organizations like the Pentagon's Defense Innovation Unit and the CIA's In-Q-Tel are good at technology scouting and at strategic investment. But we still struggle to transition these technologies from niche experimental programs into stable, long-term solutions.

None of these very real frustrations with the government excuse tech companies from the responsibilities that come with their growing global influence.

It is precisely because they are amassing this power and influence, and because they are enabled to do so only under the military, legal, and economic protections of the U.S. government, that these companies must also change.

Specifically, American technology companies must acknowledge their growing national security responsibilities. They must also accept the fact that Great Power competition is returning and that this return requires them to choose sides.

While the Chinese market may be lucrative, it is also a moral minefield and ultimately a dead end for Western companies. American companies' submission to Beijing's predatory demands on intellectual property, proprietary information, trade secrets, data, and other assets weakens American economic competitiveness, individual and national cybersecurity, and broader national security to the degree that this capitulation enables China's technological ascendance over the U.S. This participation also gives cover to Beijing's rampant political oppression and human rights violations.

The business risk is extreme, too. China has a proven record of allowing U.S. companies to take part in their market for only as long as is required to pilfer their intellectual property and secrets. Once these are sufficiently harvested, Beijing caps the companies' market presence and prioritizes domestic competitors that have been built with the information stolen from American firms.

Consider the experience of Microsoft: back in 2018, some 90 percent of Chinese firms used the company's operating system, but only 1 percent actually paid for it. This, according to former Microsoft CEO Steve Ballmer, cost the company more than $10 billion in profits.[ii] But, thus far, such losses have been accepted as the cost of doing business in what, until recently, was the world's fastest growing market.

Companies that chase short-term profits in the Chinese market over long-term stability are in for a rude shock.

Ultimately, western technology companies and the U.S. government must recognize that the long-term interests of both are better served through national security partnerships. They should do this out of patriotism, out of economic interest, and because these partnerships enable the expansion of truly free markets and human thriving around the world.

The time for rhetoric has passed. We don't need another study or another commission. Instead, the United States – its government, industry, and civil society – must establish a consensus on, and shared commitment to, our national security. This requires new levels of cooperation and mutual support.

Nowhere is this cooperation needed more than in the arena of defense innovation and acquisition.

Agile and Secure Acquisition

The second defining feature of any successful defense innovation policy, will be a more agile and secure technology acquisition system.

American military superiority is essential, but it is not inevitable. It is the result of strategic planning, deliberate investment, and an industrial base that is able to anticipate and deliver the capabilities needed to fight and win wars. We've made significant progress but a recent report shows that our defense industrial base is falling behind.

The National Defense Industrial Association (NDIA) gives the U.S. defense industrial base a "C" grade and says it is getting worse. "The defense industrial base is increasingly struggling to meet the 'unprecedented' challenges it faces," the NDIA concludes.

In the new report mentioned above, *Vital Signs 2020: The Health and Readiness of the Defense Industrial Base*, nearly 20 experts reviewed eight different dimensions shaping the capabilities of defense contractors and came away with the following judgments[iii]:

- The overall composite score for the industrial base was 77 points, just over the passing grade of 70 points and a decline of two points from 2018;
- Scores for three dimensions – production inputs, industrial security, and supply chain – fell below 70 points;
- Composite scores for four of the eight dimensions declined from 2018 to 2019; and,
- The lowest scoring dimension was industrial security, with a score of 63.

It is clear that national security leaders recognize the new era of great power competition requires significant and sustained investment in military capabilities, but the nation's defense industrial base is not ready to meet these challenges.

A decline in innovation is of particular concern. According to the NDIA report, innovation received a score of 74 for 2019, down two points from the previous year.
In a time where emerging technologies will define the battlefield, the U.S. cannot settle for a "passing grade" in developing, acquiring, and deploying these innovations. We have to dominate.

Such domination requires alternative partners, reduced bureaucracy and regulations, and industrial security.

Our current defense contractors are essential for key capabilities, especially marque platforms like aircraft carriers, fifth-generation jets, and modern fighting vehicles. But they are not typically the source of bleeding-edge developments in artificial intelligence, advanced robotics, or quantum computing. These advancements are overwhelmingly developed by companies who do not regularly work with the department of defense and who are not currently trying to solve defense challenges.

These companies' lack of involvement is not due to a lack of patriotism. It is the result of poor incentives and massive bureaucratic hurdles. It is time to clear the way for these alternative partners so that our national security can profit from their agility, creativity, and expertise.
We can make dramatic improvements by making three key changes.

First, we need to recognize and employ new incentives. The current system does not prioritize the best available technology. Instead, it favors cost accounting, regulatory compliance, and administrative ease. Budgets are programmed years in advance with little ability for companies to realize profits in current fiscal years. And, perhaps most significantly, research and development are often spread across many small contracts instead of investing deeply in key or promising capabilities.

Encouraging a diverse ecosystem of innovation is wise only if it regularly produces the capabilities you need when you need them. Ours is not.

Generally speaking, innovative companies in the technology sector do not need government "investment," they need government contracts. There is plenty of venture capital in the United States; but those dollars only follow markets where there is a real opportunity for profits. These companies need real contracts, not one-off awards, and they need to know that these contracts can be scaled into real programs of record. Do this, and the defense innovation market place will boom. While some progress is being made using "other transactional authorities," these efforts need to be greatly expanded.

The second critical action is to get rid of the innovation killing regulatory burdens that block the partners we need.

The Federal Acquisition Regulation (FAR) — which governs all federal acquisitions, including those of the Department of Defense — is more than 2,000 pages long and even includes a definition on what constitutes a "copier." Certainly, rules need to be in place to ensure the U.S. government gets its money's worth and that taxpayers are treated fairly. But this bloated framework is a massive hurdle for companies who want to have more programmers and engineers than they have lawyers and contract officers.

There is ongoing effort to update FAR, but it is progressing too slowly, and it must take the nation's innovation needs as a central concern.

Finally, the U.S. should prioritize the security of our domestic technological and manufacturing capabilities. Do not forget, it was industrial security that was the lowest scoring dimension in the NDIA report.

This is not a call for economic protectionism – U.S. companies are very competitive – it is a call for commonsense security.

In a world where securing nations means securing networks and supply chains, it is unavoidably true that the loyalties and security practices of those creating and building our defense innovations matters.

This is part and parcel of developing and maintaining the American defense base in general. As the ongoing European capitulation to China's Huawei telecommunications company demonstrates, the lack of a robust and secure domestic technology industry leaves governments in desperate straits with few good options.

The United States should never accept such outcomes.

In the final analysis, American policymakers and citizens should be encouraged, but also feel a sense of urgency. Our industrial base is still the envy of the world, and U.S. emerging technology innovators are second to none. But, if the United States is going to secure its people and its interests going forward, we must do better in leveraging and securing these engines of innovation.

[i] Pollack, K. (2019, November). Society, Technology, and Future Warfare. Retrieved February 18, 2021, from https://www.aei.org/wp-content/uploads/2019/11/Society-technology-and-future-warfare.pdf?x91208

[ii] Limitone, J. (2018, November 01). China is ripping off Microsoft to the tune of $10B. Retrieved February 18, 2021, from https://www.foxbusiness.com/business-leaders/china-is-ripping-off-microsoft-to-the-tune-of-10b

[iii] National Defense Industrial Association, (2020, February 10). Vital Signs 2020: The Health and Readiness of the Defense Industrial Base. Retrieved February 18, 2021, from https://www.ndia.org/-/media/vital-signs/vital-signs_screen_v3.ashx?la=en