Center for
21st Century Security
and Intelligence
at BROOKINGS

JULY 2015

There's no app for that:

Disrupting the military-industrial complex

JASON TAMA
Federal Executive Fellow

The views expressed in this monograph are those of the author and do not reflect the official policy or position of the United States Coast Guard, Department of Homeland Security, or the U.S. Government.

The Brookings Institution is a private, non-profit organization. Its mission is to conduct high-quality, independent research and, based on that research, to provide innovative, practical recommendations for policymakers and the public. The conclusions and recommendations of any Brookings research are solely those of its author(s), and do not reflect the view of the Institution, its management, or its other scholars.

CONTENTS

Page

EXECUTIVE SUMMARY

"Innovation has nothing to do with how many R & D dollars you have. When Apple came up with the Mac, IBM was spending at least 100 times more on R & D. It's not about money. It's about the people you have, how you're led, and how much you get it."

—Steve Jobs

The Digital Revolution is not over. Rapidly emerging technologies continue to disrupt manufacturing and services across global markets. Despite the pace of change, the United States' military-industrial complex (MIC) remains dominated by a highly consolidated base of "traditional" prime contractors and has proven to be nearly impervious to smaller, and in many cases more agile and more diversified, "non-traditional" companies.

Indeed it is difficult to overstate how formidable the barriers to entry are for "non-traditional" companies in the context of evolving 21st century global markets. These barriers significantly limit the government's access to human capital, intellectual property, and potentially disruptive innovation in other more agile segments of the economy.

In order to sustain long-term global technological advantage, the future MIC must leverage the full strength and depth of the rapidly evolving U.S. technology sector, particularly in places like Silicon Valley, which by almost all measures remains the world's leading innovation ecosystem.

Current leadership in both the Pentagon and Congress seem to acknowledge this imperative and have spoken of the need to diversify the MIC with faster-moving, more commercially diversified companies from places like Silicon Valley. Unfortunately, this is easier said than done.

Considering this context, what are the most significant barriers to entry for "non-traditional" companies, and how can they be lowered in order to attract new entrants, increase competition, and help ensure future military technological superiority? How do "non-traditional" companies in Silicon Valley view prospects for doing business with the federal government in defense, and how can this inform efforts inside the beltway to reform defense acquisitions?

While much has been written on the federal government's attempts to increase competition through acquisition reform, little research has been done to assess this issue from the perspective of Silicon Valley executives and venture capitalists. This paper offers a comprehensive overview of barriers to entry from the perspective of Silicon Valley technology executives and venture capitalists.

Findings suggest Silicon Valley executives see exceptionally high barriers to entry in defense, not because of ideological objections, but rather because of an acquisitions system and culture heavily biased in favor of larger, "traditional" defense contractors. The current system neither works in their favor nor is remotely consistent with the speed and agility these companies need to simultaneously compete in broader and in many cases more liquid global technology markets. Sadly, most executives and venture capitalists interviewed do not see a way to "win" in the current system.

This paper concludes with a number of policy recommendations, including more comprehensive and politically difficult initiatives, as well as those that can be executed by better leveraging existing authorities and capabilities.

Foreword

In early 2013, serial entrepreneur Jim Marggraff (StrataCom, LeapFrog, Livescribe) acquired technology and intellectual property assets from Eye-Com, a small Nevada-based optics research company that had developed an advanced pair of prototype glasses to track eye motion and gaze location in 3D space. Funded with nearly $15 million in government research grants, including significant resources from the Department of Defense (DOD), Eye-Com's more than 10-year effort began as pure research, with no focus on commercial applications.

In 2012, with Google's announcement of Glass, and the emergence of the Oculus Rift virtual reality headset, the world embraced "wearables," with head mounted display (HMD) devices offering extraordinary potential for consumer applications.

Seeing an opportunity to leverage Eye-Com's groundbreaking work, Marggraff founded a new company, Eyefluence, opened a local office in Silicon Valley, and immediately set out to develop a user interface for controlling an HMD with nothing but your eyes.

The MIT-educated Marggraff sees a future where eye movements will replace or supplement traditional "touch" controls for both HMDs and other devices, changing the way people interact not just with technology but the broader world around them. "We've broken through barriers that will allow access and control of information like never before. We transform intent into action through your eyes. Anything you can do with your fingers on a cell phone, you can now do with your eyes in a virtual reality or augmented reality headset, but faster," said Marggraff, who is excited by both the industrial and consumer market applications for the technology.

Marggraff is equally excited about potential applications for optically-controlled HMDs in both defense and intelligence, as a means to give personnel rapid, hands-free access to vital information, at a speed approaching thought, through simple eye-movements. Marggraff has no ideological opposition to doing business with the Pentagon or Intelligence Community, pointing out his entire career has been based on "applying high value technology to solve interesting problems with great personal and social impact." Marggraff added, "I do worry about our adversaries using this technology against us."

Sadly for both Marggraff and the federal government, the defense funding and associated ties with government officials dissolved shortly after Marggraff founded Eyefluence. As Marggraff explains it, "I thought the work with defense and intelligence had potential, and I worked to sustain both the funding and the relationships. I even had a contractor who was experienced in navigating this landscape, but there was always one more meeting, and the meetings just never went anywhere." In the meantime, Marggraff and his team were also looking hard at commercial applications. They received a round of Series A venture capital funding at the end of 2013 and never looked back.

Marggraff knew going in that he couldn't rely on defense funding and also knew the "required investment would likely be too high and the risks too great" to make defense sales a viable option for his new company. "My focus goes into what I need to do to make my company survive and flourish," said Marggraff, who saw a higher probability of speed, growth, and success in commercial applications. Marggraff's sense is that his perspective matches that of many entrepreneurs in Silicon Valley who have little interest in "navigating a long, slow, confusing maze which they don't know and may or may not lead to a contract; so the attitude in Silicon Valley is just stay away. The [venture capitalists] aren't interested for the same reasons."

When asked how he squares his company's current trajectory with its deep history of taxpayer and defense funding, Marggraff says in one sense the system is working. "Look, this would not have happened without U.S. government funding, no venture guys would have ever put money behind this research in the early stages. Now we have some tremendous foundational technology that was developed along the way and I hope will ultimately make a massive positive impact on society, and this is a good use of taxpayer dollars." However, Marggraff sees a missed opportunity as well, "the nation and the government suffer by not having better and faster access to new and emerging technologies, technologies that are going forward commercially and could easily be shaped and tailored for great government applications as well." Marggraff says he'd like to do more work in defense, but there first "has to be a vehicle through which an entrepreneur can achieve sales and develop a market."

Sadly, Marggraff's story is not unique, and it reflects both the promise and peril many Silicon Valley entrepreneurs see when it comes to doing business with the Department of Defense, much less any other agency in the Federal government.

Introduction

Defense acquisitions at a crossroads

"In the world of then, defense technology originated in a defense technology base that was embedded in defense companies that resided in the United States, for which defense was their main driver. That was then. Now, defense technology increasingly originates in a commercial technology base that's embedded in commercially driven companies that are not American, rather they are global, for which defense is a niche player. Everything is opposite from the way it used to be."

—Secretary of Defense Ashton Carter

The Digital Revolution is not over. Rapidly emerging technologies continue to disrupt manufacturing and services across global markets. Indeed, the Information Age may only be in its infancy, with innovations such as 3-D printing, artificial intelligence, advanced robotics, and predictive analytics on the cusp of game-changing applications in a number of industries. Despite the pace of change, the United States' military-industrial complex (MIC) remains dominated by a highly consolidated base of "traditional" prime contractors and has proven to be nearly impervious to smaller and in many cases more agile and more diversified "non-traditional" companies.

The Information Age has brought defense acquisitions to a crossroads with three potential paths forward: 1) Maintain the status quo, waiting for a crisis to shock the system; 2) Cultivate the depth, breadth, and speed of innovation that will be needed in the 21st century from the existing MIC; or 3) Attract new entrants to the MIC to fuel innovation.

An example of path number one was the acquisition and delivery of 11,500 Mine-Resistant Ambush Protected (MRAP) vehicles from the MIC to Iraq in 27 months (tremendously fast for a program of this size) and another 8,000 to Afghanistan in 16 months. Even with heavy losses among U.S. troops due to improvised explosive device (IED) attacks, the process was only expedited after then Secretary of Defense Robert Gates dubbed the program the "highest priority Department of Defense acquisition" and ordered the specially created MRAP task force with "taking 'extraordinary steps' to cut through red tape, rally the defense industry, and deliver the vehicles."[1]

While the MRAP deployment undoubtedly saved hundreds if not thousands of lives, as did a number of other rapidly fielded counter-IED technologies like sensors and jamming equipment, it took extraordinary leadership and effort to get them deployed, including overcoming what Secretary of Defense Ashton Carter described as a perception within the Pentagon that "such a vehicle could not be funded and built before the wars ended and thus were unnecessary."[2] Such an extraordinary process is sadly unsustainable across the defense enterprise and suggests future crises will be inevitable without more fundamental change.

As for the second path, the highly consolidated and specialized nature of the existing MIC makes keeping pace with faster-moving commercial markets nearly impossible, at least where there are similar technological applications. In other words, Newport News Shipbuilding does not need to worry about keeping up with the commercial aircraft carrier market because there is none. The U.S. will always need a strong traditional MIC to continue to lead and innovate in the limited market for pure public goods like warships, warplanes, and munitions to name a few.

However, new technologies are rapidly blurring the boundaries between traditional public goods and private goods, like drones and robotics, cyber weapons, and encryption technologies. Additionally, payloads may soon eclipse platforms in terms of their importance to sustaining technological superiority on the battlefield. It is in this context that the third path of attracting new entrants to the MIC becomes most acute.

It is difficult to overstate how formidable barriers to entry are for "non-traditional" companies in the context of evolving 21st century global markets. Many of these barriers are structural in nature but are also significantly influenced by powerful cultural differences and market forces. These barriers are limiting government's access to human capital, intellectual property, and potentially disruptive innovation in other more agile segments of the economy.

In order to sustain long-term global technological advantage, the future MIC must be capable of fully leveraging the strength and depth of the rapidly evolving U.S. technology sector,[3] particularly in places like Silicon Valley, which by almost all measures remains the world's leading ecosystem for technological innovation.[4]

Global asymmetric challenges like cybersecurity have further intensified the imperative to diversify the MIC and speed the deployment of innovative technologies. Advanced commercial technologies are now ubiquitous on a global scale. Cyber weapons in particular are a precise and attractive tool for a resource-constrained state, failed state, or non-state actor, and barriers to developing these technologies are extremely low relative to larger conventional weapons systems with similar geographic reach.

To be clear, the United States defense industrial base is the largest and most advanced in the world by almost any metric. It has a history of delivering game-changing innovations, from nuclear weapons, to the internet, to stealth technology, to precision guided weapons, to the Global Positioning System, some of which brought revolutionary change to the whole of humanity. The defense industrial base has served the nation well in this context.

However, the ability to sustain the military's technological superiority has never been a foregone conclusion and may in fact be one of the nation's defining national security imperatives for the 21st century. Since World War II, United States military strategy has been successfully undergirded by the principal of technology overmatch. But in an era of globalization and commercialization, out-innovating the enemy is becoming increasingly difficult. Indeed, the military must figure out how to become what House Armed Services Committee Chairman Mac Thornberry (R-TX) called "the world's fastest incorporator of commercial technology."[5]

Acquisition reform has traditionally focused on how to make the current system work better for the current players. Former deputy secretary defense and current CEO of Finmeccanica North America, William Lynn III, says the bigger and more consequential problem in the long term is "how to make the system work better for non-traditional companies."

Considering this context, what are the most significant barriers to entry for non-traditional companies—a convenient term used within defense acquisition circles to describe "the rest" of the economy—and how can they be lowered in order to attract new entrants, increase competition, and help ensure long-term technological advantage for the U.S. military? How do non-traditional companies in Silicon Valley view prospects for doing business with the federal government in the national security arena, and how can this inform efforts inside the beltway to reform defense acquisitions?

While much has been written on work inside the beltway to increase competition through acquisition reform and other policy initiatives, little research has been done to assess this issue from the perspective of Silicon Valley. Through dozens of interviews with current and former technology executives and venture capitalists, as well as leading government technology and acquisition professionals, a narrative has emerged regarding barriers to entry and opportunities for improvement for Silicon Valley companies in the federally funded national security space.

Despite this research's focus on national security applications, findings can be broadly applied across the federal enterprise where similar and in some cases more significant challenges exist with respect to accessing, deploying, and effectively leveraging new technologies.

Similarly, while Silicon Valley is clearly the largest and most recognizable new technology ecosystem in the United States and perhaps the world, it is certainly not alone. Vibrant technology ecosystems exist throughout the United States in places like New York City, Los Angeles, Seattle, Cambridge, and Boulder, to name a few. While this project included some research in other technology ecosystems, it was not the main focus of the effort. That said, consistent themes emerged from interviews with technology executives with experience in other regions. The key point is that Silicon Valley is by no means the nation's sole engine for developing innovative technologies, and efforts to attract new entrants to the MIC should not be limited in this context.

The good news is that the secretary of defense and chairmen of both congressional armed services committees have all gone on record to state that attracting new entrants to the defense industrial base is a priority. This refrain is now being repeated across senior management levels within the DOD enterprise, the Department of Homeland Security, and other agencies in government where mission success demands effective use of cutting edge technology.

The bad news is most of these discussions are beltway-centric and tend to result in highly technical proposals to reform acquisitions processes without seriously considering the perspective from the non-traditionals themselves.

This is why the focus of this research is *not* acquisition reform itself—an inherently insular, bureaucratic, and Washington-centric concept—but rather an effort to frame the challenge from the "outside looking in." In other words, it assesses the perspective of the potential non-traditionals, in this case primarily early-stage Silicon Valley technology and venture capital firms. Efforts to attract new entrants from places like Silicon Valley will never be successful without a better understanding of their culture, markets, and incentives, and how these contribute to their willingness (or lack thereof) to do business with the federal government's national security apparatus.

Notes

[1] Ashton B. Carter, "Running the Pentagon Right: How to Get the Troops What They Need," *Foreign Affairs* (January/February 2014) http://www.foreignaffairs.com/articles/140346/ashton-b-carter/running-the-pentagon-right, accessed April 2015.

[2] Ibid.

[3] "Adapting and evolving: Global venture capital insights and trends 2014," EY, 2014, http://www.ey.com/Publication/vwLUAssets/Global_venture_capital_insights_and_trends_2014/$FILE/EY_Global_VC_insights_and_trends_report_2014.pdf, accessed April 2015.

[4] Rip Emerson, "Startup Genome Ranks The World's Top Startup Ecosystems: Silicon Valley, Tel Aviv & L.A. Lead The Way," *TechCrunch*, November 20, 2012, http://techcrunch.com/2012/11/20/startup-genome-ranks-the-worlds-top-startup-ecosystems-silicon-valley-tel-aviv-l-a-lead-the-way/, accessed April 2015.

[5] Sean Lyngaas, "Thornberry's defense acquisition bill: 'not enough … but it's a start," *FCW*, March 23, 2015, http://fcw.com/articles/2015/03/23/thornberry-acquisition-bill.aspx, accessed April 2015.

Chapter 1: What are "offsets" and why do they matter?

The importance of sustaining competitive advantage in an era of globalization

Role of technology in post-World War II national security: What's an "offset"?

Advanced technologies have always played a significant role in American post-World War II national security and will continue to do so in the future. Moving forward into the 21st century, it is clear that the sources of advanced technologies will continue to broaden, the pace of innovation will quicken, and the reach of their global adoption will significantly expand. In order to better understand the significance of these trends in the context of modern non-traditional defense companies, it is important to first cover a rudimentary history of the role of military technological innovation in the latter half of the 20th century.

Since World War II, the United States military has generally occupied a position of unequivocal technological superiority relative to almost any adversary. In response to the Soviet Union's vast numerical superiority during the early years of the Cold War, the United States implemented what today is commonly referred to as the first offset strategy, which emphasized the deployment of technologically superior nuclear weapons with global strike capability.[1] The primary objective of an offset strategy is to create a sustained competitive advantage that compensates for a known vulnerability—in other words, if you cannot win the game you are playing, then change the game.

Soviet modernization of its nuclear and conventional forces would ultimately erode the advantages of the first offset, and the United States once again found itself in search of a strategy to counter the Soviet capacity advantage. This time, the second offset focused on establishing a credible conventional deterrent as both another counter to the Soviet's numerical advantage and a mechanism to provide strategic leverage and flexibility below the threshold of nuclear conflict.

The second offset, marked by intense research and development (R&D) investments, is widely credited with ushering in game-changing innovations such as stealth technology, long-range intelligence, surveillance, and reconnaissance (ISR), the Global Positioning System (GPS), precision guided weapons, and a host of networked information technology (IT) systems that enhanced global command and control.[2] The United States military has effectively leveraged these core technologies to sustain global technological superiority for nearly four decades.

The success of the second offset depended largely on the United States' underlying industrial, economic, and academic superiority, and the MIC's ability to effectively leverage it to produce innovative, game-changing technologies. Certainly, the United States still has the world's largest and most innovative economy, finest university system, and technologically advanced military by almost any metric. However, in an era of globalization, wherein societies are networked like never before and advanced commercial technologies are ubiquitous, some of the advantages the United States has enjoyed for decades are beginning to erode.

Nations like China are investing in targeted strategies to counter and perhaps one day achieve parity with U.S. technologies on the battlefield, including stealth fighters, anti-ship and anti-satellite ballistic missiles, and new cyber and electronic warfare technologies.[3] The Chinese are of course a long ways from achieving the capability and capacity to project substantial global military power. However, their clear focus on investing in advanced technologies is unmistakably part of their long term strategy to one day match or attempt to surpass the United States in military capability.

Even smaller nation-states and non-state actors now have access to potentially destabilizing asymmetric technologies such as cyber weapons and drone systems. Here again, the United States' current advantage in both arenas is generally accepted, but the pace of innovation is exceptionally fast and technologies like cyber are particularly attractive for resource-constrained states and non-state actors looking for global reach.

With respect to drones, consider also that the world's largest producer of small, unmanned aerial drones is not a U.S. or European manufacturer but rather the Chinese firm DJI Innovations. Clearly, small consumer drones carrying GoPro cameras do not yet pose an existential threat to U.S. military technological superiority. However, the DJI eample illustrates the potential for rapid, disruptive, commercial innovation in countries like China in sectors that are ripe for defense applications and in which the U.S. military was perhaps the first mover. Chris Anderson, former editor of Wired and now CEO of 3D Robotics, said DJI "is in the first wave of 21st century Chinese companies that we are all going to be dealing with."[4]

In some respects, DJI and its competitors exemplify what agile second movers can do with nascent first generation technology: effectively capitalizing on the difficult and expensive initial R&D work funded by the U.S. government and then rapidly scaling the capability for mass production and consumption. In the future, small drones could be modified and deployed in mass quantities for asymmetric military or terrorist applications, whether surveillance or otherwise. This is not an abstract concept, and in fact is one that is garnering great interest amongst defense and homeland security officials.[5]

What does an "offset" look like in an era of unprecedented globalization and commercialization?

So what might a third offset look like, how long will it last, and where will the technology come from? Perhaps more appropriately, is it even productive to frame the next technological challenge as a singular offset when the pace of innovation might make a dynamic strategic framework more appropriate? What are the appropriate investments and policies to ensure continued U.S. technology superiority? In the absence of a hegemonic Cold War adversary, what are the primary threats we will be trying to offset in the 21st century?

The answers to these and other difficult questions will be defining for the U.S. military and the future balance of global power. These questions also provide context for considering the future MIC and the potential role of non-traditional contributors. Despite the uncertainty regarding what exactly a third offset might entail, there are a few fundamental core principles that will likely define it.

First, should future historians one day decide a third offset actually occurred in the early decades of the 21st century, then it will likely have been much shorter than the previous two; the ubiquitous nature of advanced technology in a globalized economy all but guarantees this. Identifying the "correct" technology investments up front is less important than creating an acquisitions system that is agile enough to adapt to emerging threats, attract new entrants, and quickly incorporate new technologies.

Second, private R&D investment is poised to play a much larger role in determining the pace and direction of technological development for several reasons. Absent a major budget deal, the portion of federal spending allocated to discretionary programs will continue to decline, as will associated R&D investments across all sectors of government. DOD is already following a similar trend, with R&D spending either declining or generally remaining flat since the 2008 financial crisis.[6] Even the once vaunted defense industry itself has pulled back substantially on the R&D front, with major prime contractors investing a paltry 2 percent of their revenue in pursuit of new innovations and companies like Lockheed Martin deploying their cash for stock buybacks to support their share price.[7] This dynamic is not a positive reflection of investor's confidence in the longer term prospects for the defense industry.

In contrast, other advanced sectors within the global economy are spending more on R&D than ever before. Consider the world's 10 largest corporate R&D spenders worldwide, which includes companies like Volkswagen, Samsung, Microsoft, Intel, and Google. On average, these companies spend over 12 percent of annual revenues on R&D investments.[8] In absolute dollars, Microsoft, Google, and Apple combined spent more than five times the $4.1 billion spent by five of the top 10 U.S. defense contractors in 2013: Boeing, L-3 Communications, Lockheed Martin, Northrop Grumman, and Raytheon.[9]

These are not apples to apples comparisons, however, as companies producing consumer products sell to a much broader market than do the typical 21st century defense contractors that, for the most part, produce public goods. But the significant gap between the defense industry and other advanced industries in terms of R&D investments illustrates the powerful role of the private sector in shaping future technological innovation. That said, it is important to acknowledge that DOD's annual $65 billion R&D budget dwarfs that of any private company,[10] with funding supporting a broad range of public, private, and academic research activities, including basic and applied research, prototyping, and operational testing.[11]

Third, we are entering an era in which payloads may matter more than platforms, not just in terms of capability but also in cost and efficiency. While capital ships, aircraft, submarines, and satellites will be needed for decades to come, the performance of the individual platform may ultimately be less impactful than the payload it is carrying, e.g. a precision munition, surveillance sensors, or an electronic warfare pod. This concept lends itself to smaller, more agile, and adaptive acquisition programs that support regular payload refresh with the best available technology, as opposed to the wholesale recapitalization of a platform and/or its integrated weapons system. Chief of Naval Operations Admiral Jonathan Greenert brought widespread attention to this concept in 2012 when he advocated a "payloads over platforms" acquisitions strategy for the Navy, arguing that "shifting to modular payloads as the primary source of capability enables the U.S. to more rapidly and affordably incorporate new technology."[12]

All this underscores the point that we do not know what the future will require in terms of specific technologies, much less what future technologies will emerge. Needless to say, the United States must be prepared to face a range of adversaries, from near-peer rivals like Russia or China, to smaller regionally-focused states like Iran, to dangerous non-state actors, and everything in between. Given the absence of a unifying national security imperative, like containing the Soviet Union, future offset strategies will require the MIC to be more diversified, agile, and innovative to rapidly respond to emerging global challenges and technologies.

The danger here is obvious. Words like "agile" and "responsive" are not typically associated with either the Pentagon workforce or today's defense industry. Despite a storied history of game-changing innovations in the post-World War II era, weapons system cost overruns, schedule delays, and embarrassing failures to deliver promised capabilities plague the Pentagon. Just as troubling, the Information Age has ushered in another dangerous defense acquisitions phenomenon: the fielding of promised capabilities already eclipsed by faster-moving commercial technologies. This cycle must be broken lest we end up offsetting tomorrow's threat with yesterday's technology.

Notes

[1] James Hasik and Alex Ward, "Third Offset Strategy, Second Adversary," Atlantic Council, November 18, 2014, http://www.atlanticcouncil.org/blogs/defense-industrialist/third-offset-strategy-second-adversary, accessed April 2015.

[2] Ben FitzGerald, "Can America Maintain Its Military-Technology Edge?" *The National Interest*, August 13, 2014, http://nationalinterest.org/feature/can-america-maintain-its-military-technology-edge-11071, accessed April 2015.

[3] "Russia, China aim to close military technology gap with U.S.: Hagel," *Reuters*, September 3, 2014, http://www.reuters.com/article/2014/09/03/us-usa-military-spending-idUSKBN0GY2CC20140903, accessed April 2015.

[4] Brad Stone, "DJI's Drone Is Simple Enough for Anyone to Use," *Bloomberg*, May 15, 2014, http://www.bloomberg.com/bw/articles/2014-05-15/dji-innovations-drone-is-simple-enough-for-anyone-to-use, accessed April 2015.

[5] Kevin Poulsen, "The US government is terrified of hobbyist drones," *Wired*, February 5, 2015, http://www.wired.com/2015/02/white-house-drone/, accessed April 2015.

[6] Zachary Fryer-Biggs, "DoD Reshapes R&D, Betting on Future Technology," *Defense News*, April 20, 2014, http://archive.defensenews.com/article/20140420/DEFREG02/304200006/DoD-Reshapes-R-D-Betting-Future-Technology, accessed April 2015.

[7] Doug Cameron, "Lockheed Martin to Boost Buybacks, Keep Spending Flat," *The Wall Street Journal*, October 21, 2014, http://www.wsj.com/articles/lockheed-martin-forecasts-sales-and-margins-drop-in-2015-1413890941, accessed April 2015.

[8] Michael Casey and Robert Hackett, "The 10 biggest R&D spenders worldwide," *Fortune*, November 17, 2014, http://fortune.com/2014/11/17/top-10-research-development/, accessed April 2015.

[9] Marcus Weisgerber, "Tech Giants Spend Billions More Than Defense Firms on R&D," *Defense News*, May 26, 2014, http://archive.defensenews.com/article/20140526/DEFREG02/305260015/Tech-Giants-Spend-Billions-More-Than-Defense-Firms-R-D, accessed April 2015.

[10] Mark Boroush, "Federal R&D Funding, by Budget Function: Fiscal Years 2013-15," National Science Foundation, National Center for Science and Engineering Statistics, November 2014, http://www.nsf.gov/statistics/2015/nsf15306/pdf/nsf15306.pdf, accessed June 2015.

[11] Fryer-Biggs.

[12] Jonathan W. Greenert, "Payloads over Platforms: Charting a New Course," *Proceedings* 138/7/1,313 (July 2012), http://www.usni.org/magazines/proceedings/2012-07/payloads-over-platforms-charting-new-course, accessed April 2015.

Chapter 2: The military-industrial complex, Silicon Valley, and defense acquisitions

Comparing today's military-industrial complex to the world's most innovative ecosystem

Is today's military-industrial complex well positioned to innovate?

Today's military-industrial complex is arguably more consolidated and less commercially diversified than at any point during the post-World War II era. Major prime defense contractors deal almost exclusively in defense with few overlapping business lines into other advanced commercial markets. There are some exceptions to this, Boeing being the most notable example with its robust commercial aircraft business. This stands in contrast to the military-industrial complex that dominated the second half of the 20th century, one that included more diversified conglomerates that saw defense as complementary to their commercial sales.

Over the past 40 years the industry has undergone multiple waves of consolidation driven by a variety of factors. The dramatic force and spending drawdown in the post-Vietnam War era led many companies in the MIC to look beyond the defense industry to sustain cash flows and some to exit the business entirely. During the second Reagan Administration, slowing defense spending and increased controls from the Department of Defense limiting profits further eroded the industry's attractiveness to investors, particularly relative to growing advanced commercial sectors. This ultimately resulted in 10 of DOD's top 60 contractors acquiring or being acquired by others in the industry from 1985 to 1988.[1] The most recent major consolidation occurred in the mid-1990s after the breakup of the Soviet Union, when over $55 billion in mergers occurred, further skewing top players to a pure defense market play.[2]

Large portions of the defense industry will always be heavily consolidated. Competition for public goods like warships and warplanes will always be limited as the market for these products is narrow and barriers to entry are extremely high. A 2014 study by the Center for Strategic and International Studies (CSIS) found that the overall effective competition rate for DOD contracting from 2000 to 2013 was approximately 50 percent, with "effective competition" defined as a contract that receives two or more bids.[3]

Lack of effective competition has always been a challenge in the defense industry, particularly for large weapons systems. For example, Assistant Secretary of the Navy Sean Stackley recently told Congress that of the eight shipyards currently building U.S. Navy ships, "about half of them are about a single contract away from being what I would like to call 'not viable.' In other words, the workload drops below the point at which the shipyard can sustain the investment that it needs to be competitive [and the skilled labor force it needs to function], so they would quickly find themselves outside of the market."[4] While shipbuilding is perhaps a uniquely difficult case as a result of its exceptionally long development and production cycles, as well as a limited number of large contracts, it illustrates the fragility of certain segments of the defense industrial base that have come to rely almost exclusively on government contracts to remain viable.

In 2013, the top five defense contractors—Lockheed Martin, Boeing, Raytheon, General Dynamics, and Northrop Grumman—accounted for approximately 30 percent of DOD contract obligations and a disproportionate share of contracts exceeding $500 million or more in annual obligations. This is not surprising given the "Big 5's" role as systems integrators and their near-exclusive focus on defense business. Since 2003 the share of awarded DOD contracts obligating at least $500 million has more than doubled and has come at the expense of smaller contracts, which generally have lower barriers to entry and a greater likelihood of attracting new, non-traditional contractors to the industrial base. This phenomenon was exacerbated under sequestration, which caused DOD to focus its resources on sustaining its largest acquisitions.[5]

When the net is cast even wider, the data shows that 16 of the top 20 defense vendors from 2003 remained on the list in 2013. Furthermore, the top 20 account for nearly 50 percent of contract awards, roughly the same percentage as in 2003. Finally, the only turnover in the top 20 over the past decade can generally be attributed to unique Iraq war spending or merger and acquisition activity.[6]

In general, sequestration, continued shutdown threats and continuing resolutions had a number of cumulative adverse impacts, including stifling R&D investment, introducing additional financial risk for contractors, increasing the costs of settled, multi-year acquisitions that could have otherwise been funded on schedule, and ultimately discouraging new entrants from competing. The prevalence of these dynamics during the past several budget cycles has only increased the pressures on industry to consolidate.

Sean O'Keefe, former secretary of the Navy, NASA administrator, and CEO of Airbus North America, drew a parallel between the current defense industrial base and the era of government-owned and operated arsenals that predated the rise of the modern military-industrial complex. When asked about this in an interview, O'Keefe stated that the lack of diversification within the industry has effectively recreated the "arsenal system, the only difference being we've outsourced the arsenals."

Even after many waves of consolidation, the major players in the defense industrial base are on a difficult path moving forward. They are making minimal R&D investments at levels well below those in other advanced industries and are instead deploying their cash to buy their own stock. The near-term business case for this approach may be sound: capture income investors and support share prices while awaiting greater fiscal and programmatic clarity from the Pentagon. However, these conditions reflect a lack of market confidence in the longer term health of the MIC, with the slowdown in R&D spending particularly troubling due to its adverse impact on innovation.

What is the state of the emerging technology sector in Silicon Valley, and how is it different from the military-industrial complex?

Much of the United States' defense industrial base depends almost exclusively on government contracts and at present is not significantly investing in its future through R&D. For a variety of reasons, the industry generally moves at a much slower pace than other advanced segments of the economy and serves a market with limited competition and limited incentive to innovate relative to other markets.

In contrast, consider the emerging U.S. technology sector, particularly its epicenter in Silicon Valley. In terms of technological innovation, Silicon Valley has remained the envy of the world for several decades, leads the world in venture capital investment,[7] leads the nation in patent generation per capita,[8] and has had a tremendous record of disruptive innovation since 1961, when Fairchild Semiconductor patented the integrated circuit. Multiple states and nations have attempted to emulate its success through establishment of regional technology hubs, but these attempts have had varying levels of success over the years and no serious rival has yet to emerge.[9]

The combination of innovation and investment has led to tremendous economic growth and the creation of a number of hugely successful companies like Intel, Google, Hewlett-Packard, Apple, Oracle, and Cisco to name a few, companies that continue to fuel the cycle of innovation through their R&D and merger and acquisition investments. These firms are serving vast global markets and padding their balance sheets with, in some cases, unprecedented amounts of cash, positioning themselves to invest in future growth as well as keep their shareholders happy with dividend payments.

Companies like Apple and Google have nearly $180 billion and $60 billion in cash respectively, dwarfing any company within the defense sector. In fact, Google has sufficient cash to buy out any of the major defense contractors, which illustrates the size and power of both the firm and the growing global technology sector.[10] Some of the fundamental drivers of innovation in Silicon Valley are the depth, speed, and liquidity of global technology markets.

Despite these impressive attributes, it is important to remember that what truly sets Silicon Valley apart as the world's most vibrant innovation ecosystem are its people and culture; some have described Silicon Valley as not just a place but a "state of mind." While definitively capturing cultural attributes was not the focus of this research, a number of defining characteristics emerged during interviews with current and former Silicon Valley technology executives and venture capitalists. Below is a brief synopsis of four cultural attributes particularly relevant to understanding the potential (or lack thereof) for greater engagement between the emerging tech industry and the federal government on matters of security.

<u>1. Solving tough problems through disruptive innovation; that is, innovation that helps create a new market and may eventually "disrupt" or entirely displace a previously existing market and/or technology (e.g. cellular phones disrupted the traditional telecom industry).</u> Focus on solving tough and impactful problems by deploying the best available technology. In some cases, the more disruptive the technological solution is to the status quo the better for your product and the larger your potential market.

This runs counter to the nature of a federal bureaucracy—particularly one as massive as that governing defense acquisitions—which is inherently predisposed to sustaining the status quo.

<u>2. Fail fast, fail often.</u> Embrace risk and failure as part of the learning and development process. Determining the "best" technological solution requires testing and prototyping many alternatives. Under this construct, the majority of prototype solutions much like the majority of Silicon Valley startup companies, will fail. In other words, test, fail fast, test some more, fail some more, and keep pivoting to the next idea until you find what works. A culture of failing "fast" allows testing of multiple solutions, and generally prevents excessive investment in bad ideas or promising technologies that perhaps lack the maturity to move forward toward practical deployment.

In the world of federal government acquisitions, failing with taxpayer dollars at stake is a much more difficult proposition. In general, defense acquisition professionals operate in a highly risk averse, rules-based system. There is little incentive to deviate from the status quo, as failures tend to have negative consequences for people and organizations. Secretary of Defense Ashton

Carter put this bluntly, “the officials responsible for acquisitions are loath to take risks, since they can be held personally accountable if something goes wrong.”[11]

RECENT ACQUISITIONS FAILURES

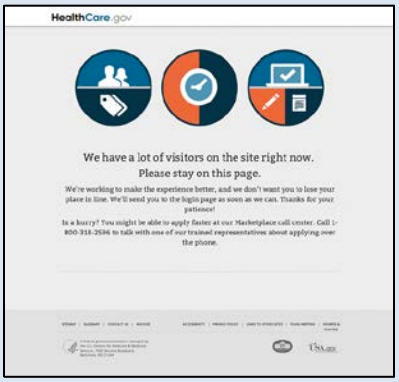
VX71 Presidential Helicopter Replacement. Cancelled in 2009 after investing four years and nearly $4 billion in taxpayer dollars due to ballooning costs and requirements creep.[12]

Army Crusader Artillery System. Cancelled in 2002 after investing four years and $2 billion in taxpayer dollars after the secretary of defense determined the program was no longer needed.[13]

Army Future Combat System (FCS).[14] Cancelled in 2009 after over $18 billion of investment in vehicles and communications infrastructure.[15] In explaining his decision to end the program, then Secretary of Defense Robert Gates concluded, “there are significant unanswered questions concerning the FCS vehicle design strategy” and expressed concern that the lightly armored vehicles did not “adequately reflect the lessons of counterinsurgency and close-quarters combat in Iraq and Afghanistan.”[16]

Air Force Expeditionary Combat Support System (an Enterprise Resource Planning IT system). Cancelled in 2012 after investing seven years and $1 billion after it was determined “it would require an additional $1.1B for about a quarter of the original scope to continue and fielding would not be until 2020,” according to an Air Force spokesman.[17]

Healthcare.gov.[18] While healthcare.gov was not a defense acquisition, it is one of many examples of failed IT system deployments across the federal government, with an estimated total cost of $840 million for both initial deployment and post-deployment system remedies.[19] One study suggested over 40 percent of federal IT projects were either abandoned entirely or restarted from scratch between 2002 and 2012.[20]



We have a lot of visitors on the site right now.
Please stay on this page.

We're working to make the experience better, and we don't want you to lose your place in line. We'll send you to the login page as soon as we can. Thanks for your patience!

In a hurry? You might be able to apply faster at our Marketplace call center. Call 1-800-318-2596 to talk with one of our trained representatives about applying over the phone.

Managing risk to the taxpayer is a good thing, but a culture of excessive risk aversion and fear of failure can have disastrous consequences, particularly when programs with rising costs and constantly evolving requirements (i.e. “requirements creep”) are culturally difficult to terminate.

There are some noteworthy exceptions to this risk posture, but most exist within the Science and Technology (i.e. research and development) enterprise of the Department of Defense, where a higher level of risk tolerance is present given the nature of basic research and early state prototyping. For example, the Defense Advance Research Project Agency (DARPA) has been universally recognized both inside and outside government as a highly innovative organization, not afraid to take calculated risks and fail with taxpayer dollars. The tolerance for failure is balanced both by DARPA's strong legacy of "successful" projects and the relatively small investments it makes in comparison to much larger acquisition programs of record.

3. Speed and growth. Business decisions are driven by speed and growth, particularly in the startup community, in which survival of the company is ultimately at stake.

In the federal government, mission critical capabilities are subject to the same acquisition process as commodities. This involves an exceptionally long sales cycle relative to the private sector and tends to bias the system toward larger, established companies that have the cash flow and resources to wait.

4. Recruit the best people. Strong meritocracy composed of a young, highly educated, and technically proficient workforce.

The 21st century civil service is governed by an archaic personnel management system developed during the post-World War II industrial era. The current General Schedule pay and classification system for federal employees dates back to 1949. This system of compensation and associated rigid recruiting, hiring, promotion, and discipline systems have left the U.S. with an aging civil service that lacks the diversity and expertise needed to meet 21st century challenges. [21]

Across the federal government the average civil servant is 47 years old.[22] People under the age of 30 represented 7 percent of the federal workforce in 2013 compared to 25 percent for the broader U.S. economy; in 1975 more than 25 percent of the workforce was under the age of 30.[23]

The 150,000-person Defense Acquisitions Workforce is 90 percent civilian and over 70 percent male.[24] While the gender split may seem alarming, some data suggests DOD's male-female split within the Defense Acquisitions Workforce is consistent with and may even be better than Science, Technology, Engineering, and Math (STEM) gender demography across the broader U.S. economy.[25] Some data also suggests DOD may have even better gender demography than technology workers in Silicon Valley.[26]

Like the over 700,000 civilian employees across the Department of Defense, the Defense Acquisitions Workforce is disproportionately dominated by those between the ages of 40 and 60, representing 63 percent of the workforce for mission critical positions across the entire Department. Within DOD's IT community, the percentage of employees between the ages of 40 and 60 rises to 65 percent. Approximately 44 percent of DOD's mission critical civilian employees have a record of prior military service,[27] a likely indicator of the powerful influence of veterans hiring preferences on shaping the age, experience, and professional background of the federal workforce.

This data shows that the federal workforce is out of step with the broader U.S. economy in terms of age demographics and drastically out of step with the emerging technology sector. For example, in 2013 the following median ages were identified at notable technology companies: Oracle (38), InfoSys (30), Google (29) and Facebook (28).[28] A Harvard Business Review study concluded the average age of founders of some of the most successful startups in Silicon Valley (i.e. venture backed companies valued at over $1 billion) was approximately 31 at the time of founding.[29]

Finally, it is important to also note that the uniformed military services also suffer from an archaic compensation and personnel management system that hasn't substantively changed since World War II. While the services generally have more predictable age demographics than the civil service due to the inherent force structure and "up or out" promotion system, the armed forces are similarly challenged to attract critical talent in a number of key areas related to new and emerging technologies.

The overarching point is that there are fundamental differences in the background, experience, and make-up of the defense acquisition workforce relative to emerging technology companies in Silicon Valley. This point will be revisited later to provide better context regarding barriers to entering the defense industrial base for new tech companies.

The defense acquisition process is not particularly well suited to foster innovation

The defense acquisition system must be capable of delivering the best possible capability to warfighters while balancing affordability and appropriate stewardship of taxpayer dollars.

Defense acquisition legislation, regulations, and policy have evolved over decades shaped by both failures on the battlefield as well as failures of financial stewardship. The former tend not to deliver lasting or sustainable reform as the cases are unique and the acquisition system flexes temporarily in the face of overwhelming political pressure. Sadly, it seems the latter generates greater political momentum for more lasting reform, particularly in the wake of high profile acquisitions failures. In a system designed to progressively reduce cost, schedule, and performance risk before proceeding to the next phase of an acquisition, it is all too easy for Congress to pile on additional studies, reports, requirements, and oversight layers in an effort to "reform" the system.

Congress also plays a significant role supporting and reinforcing the traditional MIC through the appropriations process, with many members having great interest in seeing particular projects move forward to support equities in their districts.

In defense of Congress, multiple attempts have also been made over the years to streamline acquisition requirements, but the end result often turns out the same. That is, with each new administration or congress, a new imperative for reform seems to surface. Reforming the system is hard given the size, complexity, and culture of the acquisitions workforce as well as the political forces in play. Ironically, the current chairman of the House Armed Services Committee summed it up best when outlining his own recent proposal for reform, stating, "no one has all of the answers or understands all of the consequences of a particular change."[30]

Indeed, despite decades of attempts at reform, the defense acquisitions process remains perhaps the most prominent symbol of government bureaucracy run amok. Large defense procurements continue to be associated with exceptionally long development and production cycles, constantly shifting requirements, and an unfortunate history of cost overruns, schedule delays, and failures to deliver capability. With respect to processes and requirements, the system is at best opaque and at worst impossible to manage for new companies looking to break into the defense industrial base.

In many cases, those that successfully establish themselves within the defense contractor ecosystem tend to stay there, as the ecosystem requires unique specialization and business processes that may not be readily transferable to other commercial markets. John DiLuna, CEO of startup firm Technical Assent, a consulting company founded primarily to improve federal government services, sees this dynamic reinforcing an environment where the bureaucracy has little incentive to improve processes and attract new entrants. He described a culture in which some contracting officials mistakenly "think the meal is so good for companies that get a seat at the table that vendors should be lining up to get in the door." If this is the operating assumption, market research becomes a passive activity vice a proactive search for novel ideas.

Furthermore, the startup methodology contrasts drastically with qualification requirements of a typical government contract. For example, a typical government contract requires vendors to submit a performance history of where they have successfully delivered solutions of the same size, scope, and complexity. Contrast this with the prevalent startup teaching that encourages entrepreneurs to develop a prototype that can be improved in partnership with its customers. One system favors the tried and true while the other favors market validation. These dynamics reinforce the idea of an insular system with formidable barriers to entry for new participants.

Broad recognition that new defense acquisition reforms are needed

There is recognition by both administration and congressional leadership that acquisition reforms will be needed to sustain the U.S. military's technological superiority in the globalized economy. But making meaningful change to such a massive bureaucracy is not only incredibly difficult, it is fraught with risk. Given the size and complexity of the system, there is a very real chance that efforts to reform could do more harm than good, particularly if they fail to adequately consider second and third order effects of any policy or legislative change.

As illustration, consider the most recent proposal to improve defense acquisitions. In March 2015, House Armed Services Committee Chairman Mac Thornberry (R-TX) rolled out his much anticipated first wave of proposals to reform defense acquisitions. Thornberry framed the "Agile Acquisition to Retain Technological Edge Act" as a discussion draft intended to elicit feedback, acknowledging that meaningful reform would take years and multiple pieces of legislation. Thornberry was wise to manage expectations. Multiple congresses and administrations have waded into these waters with little to show for their efforts.

The good news is that the bill has strong bipartisan support. Thornberry's bill is cosponsored by Ranking Member Adam Smith (D-WA), and both Pentagon and Senate Armed Services Committee leadership have made reform a priority. There is some political momentum, and the National Defense Authorization Act—the target legislative vehicle—is likely one of few bills in Congress with wheels to move.

The bill also appropriately frames what is at stake. The concept of "acquisition reform" neither resonates with the public nor sufficiently captures the associated national security implications. Yes, traditional tenets of reform like cost, schedule, and performance still matter. However, the fundamental imperative for reform is sustaining our ability to win the fight by out-innovating the enemy.

One proposal on the innovation front is to make "other transaction" (OT) authority permanent and better leverage it to attract more agile companies to defense work. This authority allows for streamlined business transactions not burdened by federal acquisition regulations and has been used by innovative organizations like DARPA for decades. By making the authority permanent, Thornberry is betting it might be used more broadly across other programs to foster innovation.

Thornberry appropriately forecasts more difficult personnel reforms ahead, fully recognizing their intrinsic linkage to acquisitions. Cultural barriers to reform cannot be overstated and are fundamentally rooted in human capital. Developing and sustaining a lean, agile and innovative acquisition process will require a workforce with the same traits, and Thornberry seems to grasp this imperative.

When it comes to reform, more reporting requirements and oversight layers can have undesirable effects such as stifling innovation, diffusing accountability, increasing cost and schedule, and discouraging companies from competing for contracts. Congress generally fails to recognize this risk or overlooks it to make political hay after an embarrassing acquisitions failure. Thornberry acknowledges these cumulative adverse effects and is proposing to eliminate a host of congressional reporting requirements that do not add value.

So what's the bad news? In attempting to remove barriers, Thornberry added another. The bill generally limits the use of OT authority to small business or non-traditional defense contractors. This seemingly innocuous provision will limit innovative cost sharing, partnering, and consortium building between small businesses and established system integrators. While the Pentagon needs to attract new entrants to the defense industry, placing unnecessary restrictions on one of the Pentagon's most flexible transaction authorities is not a good way to do this.

Unfortunately, barriers to reform are more difficult and deeply rooted than even Thornberry realizes. Current acquisition processes and workforce policies came of age largely within a post-World War II industrial framework, and this cultural legacy remains entrenched today. Managing naval ship acquisitions is very different than managing agile software development, and the system is heavily biased toward the former.

Finally, no matter how effective the reforms, defense acquisitions will never be successful without stable and predictable funding. Sequestration, shutdown threats, and continuing resolutions stifle R&D spending, introduce unnecessary contractor financial risks that taxpayers ultimately cover, discourage competition, and increase the costs of settled, multi-year acquisitions that might have otherwise been funded on schedule. Put simply, the nation cannot achieve its national security and defense acquisition goals without more responsible budgeting, and this must be the mantra of any reform effort.

While a good start, Representative Thornberry's proposal illustrates the decades-old challenge of executing meaningful acquisitions reform.

Notes

[1] Barry Watts, "The US Defense Industrial Base: Past, Present and Future," Center for Strategic and Budgetary Assessments, October 15, 2008.

[2] William J. Lynn III, "The End of the Military-Industrial Complex," *Foreign Affairs* (November/December 2014), http://www.foreignaffairs.com/articles/142199/william-j-lynn-iii/the-end-of-the-military-industrial-complex, accessed April 2015.

[3] Gregory Sanders, David J. Berteau, Jesse Ellman, et al, "U.S. Department of Defense Contract Spending and the Industrial Base, 2000-2013," Center for Strategic and International Studies, October 15, 2014.

[4] Sydney J. Freedberg Jr., "Half Of Shipbuilders '1 Contract Away' From Bust: Stackley," *Breaking Defense*, March 18, 2015, http://breakingdefense.com/2015/03/half-of-shipbuilders-1-contract-away-from-bust-stackley/, accessed April 2015.

[5] Sanders, Berteau, Ellman, et al.

[6] Ibid.

[7] Antonio Regalado, "In Innovation Quest, Regions Seek Critical Mass," *MIT Technology Review*, July 1, 2013, http://www.technologyreview.com/news/516501/in-innovation-quest-regions-seek-critical-mass/, accessed April 2015.

[8] Jonathan Rothwell, José Lobo, Deborah Strumsky, et al, "Patenting Prosperity: Invention and Economic Performance in the United States and Its Metropolitan Areas," The Brookings Institution, February, 2013.

[9] Vivek Wadhwa, "Silicon Valley Can't Be Copied," *MIT Technology Review*, July 3, 2013, http://www.technologyreview.com/news/516506/silicon-valley-cant-be-copied/, accessed April 2015.

[10] Lynn.

[11] Ashton B. Carter, "Running the Pentagon Right: How to Get the Troops What They Need," *Foreign Affairs* (January/February 2015), http://www.foreignaffairs.com/articles/140346/ashton-b-carter/running-the-pentagon-right, accessed April 2015.

[12] David Pugliese, "$400M Choppers May Be Sold For Parts," *Defense News*, November 8, 2010, http://archive.defensenews.com/print/article/20101108/DEFFEAT04/11080313/-400M-Choppers-May-Sold-Parts, accessed April 2015.

[13] "Rumsfeld kills Crusader artillery program," *USA Today*, May 8, 2002, http://usatoday30.usatoday.com/news/washington/2002/05/08/rumsfeld.htm, accessed April 2015.

[14] Photo courtesy of The U.S. Army Flickr, C. Todd Lopez, "NLOS-C Unveiled on Capitol Hill," June 12, 2008, https://creativecommons.org/licenses/by/2.0/legalcode.

[15] Rowan Scarborough, "Pentagon has spent billions on doomed programs; cash looms large with budget cuts," *The Washington Times*, March 17, 2013, http://www.washingtontimes.com/news/2013/mar/17/pentagon-has-spent-billions-on-doomed-programs/?page=all#!, accessed June 2015.

[16] Noah Shachtman, "Pentagon chief rips heart out of Army's 'future'," *Wired*, April 6, 2009, http://www.wired.com/2009/04/gates-rips-hear/, accessed June 2015.

[17] Chris Kanaracus, "Air Force scraps massive ERP project after racking up $1 billion in costs," CIO, November 14, 2012, http://www.cio.com/article/2390341/cio-role/air-force-scraps-massive-erp-project-after-racking-up--1-billion-in-costs.html, accessed April 2015.

[18] Photo courtesy of Chris Messina Flickr, "Health Insurance Marketplace: Please Wait," October 7, 2013, https://creativecommons.org/licenses/by-nc-sa/2.0/legalcode.

[19] Kate Pickert, "Report: Cost of Healthcare.Gov Approaching $1 Billion," *TIME*, July 30, 2014, http://time.com/3060276/obamacare-affordable-care-act-cost/, accessed April 2015.

[20] Niam Yaraghi, "Healthcare.gov and the History of Failed IT Projects: A New Solution to an Old Problem," *TechTank*, blog, The Brookings Institution, April 2, 2014, http://www.brookings.edu/blogs/techtank/posts/2014/04/03-healthcare-dot-gov-failed-it-project-yaraghi, accessed April 2015.

[21] "Building the Enterprise: A New Civil Service Framework," Partnership for Public Service and Booz Allen Hamilton, April 2014, http://ourpublicservice.org/publications/viewcontentdetails.php?id=18, accessed April 2015.

[22] "Data, Analysis & Documentation: Federal Employment Reports," Office of Personnel Management, September 20, 2013, https://www.opm.gov/policy-data-oversight/data-analysis-documentation/federal-employment-reports/reports-publications/profile-of-federal-civilian-non-postal-employees/, accessed April 2015.

[23] Rachel Feintzeig, "U.S. Struggles to Draw Young, Savvy Staff," *The Wall Street Journal*, June 10, 2014, http://www.wsj.com/articles/u-s-government-struggles-to-attract-young-savvy-staff-members-1402445198, accessed April 2015.

[24] "Defense Acquisition Workforce Key Information," PDF presentation, United States Department of Defense, September 30, 2014.

[25] David Beede, Tiffany Julian, David Langdon, et al, "Women in Stem: A Gender Gap to Innovation," United States Department of Commerce, ESA Issue Brief #04-11, August 2011.

[26] Elizabeth Weise, "Tech: Where the women and minorities aren't," *USA Today*, August 15, 2014, http://www.usatoday.com/story/tech/2014/05/29/silicon-valley-tech-diversity-hiring-women-minorities/9735713/, accessed April 2015.

[27] "Fiscal Years 2013-2018 Strategic Workforce Plan Report," United States Department of Defense, July 25, 2013, http://dcips.dtic.mil/documents/SWPWholeReportCDv2.pdf, accessed April 2015.

[28] Quentin Hardy, "Technology Workers Are Young (Really Young)," *The New York Times*, July 5, 2013, http://bits.blogs.nytimes.com/2013/07/05/technology-workers-are-young-really-young/?_r=0, accessed April 2015.

[29] Walter Frick, "How Old Are Silicon Valley's Top Founders? Here's the Data," *Harvard Business Review*, April 3, 2014, https://hbr.org/2014/04/how-old-are-silicon-valleys-top-founders-heres-the-data/, accessed April 2015.

[30] William M. "Mac" Thornberry, "Input Requested on Initial Acquisition Reform Legislation," United States House of Representatives, Committee on Armed Services, March 25, 2015.

CHAPTER 3: THE CASE FOR CHANGE

WHY MAINTAINING THE STATUS QUO IS A BAD IDEA

The preceding chapters made the case that sustaining the U.S. military's global technological superiority may be its foundational national security imperative for the 21st century. I also suggested that doing so will not be easy in an era of globalization and advanced technological commercialization. Finally, I made the case that the current acquisitions process and MIC are not well suited to develop and deliver the latest technology to warfighters in a timely and affordable fashion, and that perhaps the solution lies outside the current defense industrial base with more agile and innovative companies like those in Silicon Valley.

Before going further with this argument, let us pause and ask whether the stark contrast between the state of the MIC and the emerging technology sector really matters. Markets and incentives within the commercial technology sector are inherently different than those associated with producing public goods for national defense. Perhaps the two are fundamentally incongruent?

The United States has maintained the world's leading defense industrial base for decades, with a history of either developing its own game-changing technology, or assimilating it through mergers and acquisitions or technology transfer, and then optimizing it for use on defense platforms. Why can't we just continue with the status quo?

Payloads matter more than platforms, and the rest of the world is working hard to "catch up"

The United States still deploys the world's finest ships, aircraft, submarines, and space systems in the world and generally has since the end of World War II. While smaller nation-states and non-state actors have always been able to inflict harm on U.S. forces via asymmetric means, particularly in ground combat, the United States has unquestionable dominance in the global commons, and this is unlikely to erode in the near-term.

However, as many scholars have suggested, the proliferation of advanced technologies through globalization offers greater opportunity for the rest of the world to catch up. Catching up may not require matching the capital assets of the United States, but rather extending asymmetric capabilities to the global commons through, for example, the innovative use of technology such as precision anti-ship missiles and stealth counter-detection methods fueled by rapid increases in computing power.

Scholars continue to debate how, when, and whether the rest of the world will catch up. Defining "catching up" also remains an open question, as peer-to-peer competition is unlikely in the near-term, but the ability to deny U.S. forces access or inflict harm asymmetrically could be sufficient to catch up in certain national security scenarios.

Recognition of these risks is helping usher in an era in which the performance of payloads may soon eclipse that of the platform, particularly in terms of providing a differentiating technological capability against the enemy. Payload refresh is faster and cheaper than platform refresh and may offer the best vehicle to rapidly deploy the newest technologies to the field. In 2012, Admiral Jonathan Greenert wrote, "Just as Apple's fleet of platforms has provided incentives for the development of new 'apps' and peripheral devices that easily plug into its operating system, the Navy can spur the development of new capabilities and payloads to plug into the Fleet. This model will help us to maintain our warfighting edge, build the Fleet capacity that keeps us forward, and improve our readiness for today's missions."[1]

Greenert's writing tacitly acknowledges the evolving technology inversion between cutting edge technologies in the private sector and those eventually deployed through the defense acquisitions process via traditional supply chains. In other words, the ability for defense platforms to remain on the frontier of leading edge technologies is slowly being eroded by globalization, the rapidly increasing complexity of technology, and the inability to deliver it quickly through the traditional MIC. Emphasizing more agile payload acquisitions as a means to help speed the process is a logical step in the right direction but one that will also be deployed by our adversaries to cheaply field the most current technology. So the payload strategy only works if our technology is better and our process is faster than theirs!

The "tail" matters too, and most of these IT systems are lagging way behind

Beyond frontline military operations, the logistics infrastructure, or "tail," matters too. Underlying information technology systems for communications, command and control, maintenance, finance, and personnel management are critical to the day-to-day functioning of the Armed Services. Sadly, like many systems supporting operations in the federal government writ large, many of these systems have a reputation for being antiquated, difficult to use, lacking interoperability with other critical systems, and in some cases ineffective.

A 2015 report of 40 IT systems by Michael Gilmore, director of operational test and evaluation, found DOD has "a poor track record of meeting system reliability requirements" and had a number of cybersecurity vulnerabilities stemming from unnecessary network services or system functions and misconfigured or outdated software.[2]

More glaring is perhaps DOD's seemingly perpetual inability to pass a financial audit, which erodes readiness and redirects precious resources and political attention from critical frontline operations and future investments. Critics often cite the Department's reliance on a dizzying array of 2,200 information technology systems operating at a cost of $17 billion annually to manage finance, human resources, property, and weapons acquisition, many of which are antiquated, duplicative, and lack interoperability.[3,4]

Antiquated and ineffective information technology systems are at best an efficiency drag on the enterprise and at worse a cybersecurity vulnerability that could be exploited by an adversary. Just as supply lines in the physical domains are critical to propagating power, so are the underlying systems in the cyber domain. One mid-grade military officer stated, "For every 'healthcare.gov' the public sees, I can show you 10 such systems inside DOD that nobody has ever heard of."

These are real systems that impact readiness and efficiency across the enterprise, and in many cases were developed using antiquated technology and system architecture. Sadly, DOD is not unique in this respect, and similarly problematic systems can be found across the federal government.

The state of government IT systems reflects both its much slower rate of technology adoption relative to the private sector and an antiquated system design and procurement process biased toward more traditional physical systems. For example, the settling of rigid requirements up front may not be possible for a complex enterprise-wide IT system, as new requirements often evolve during system development that simply were unknown previously.

Google's robotics play and what it means for defense

Consider the realm of advanced robotics, where Google has purchased seven different robotics companies since 2013, including Boston Dynamics, a DARPA funded company, as well at Tokyo-based Schaft, which in 2013 had a winning trial run for DARPA's upcoming robotics competition in Pomona, California. Prior to the Google acquisition, both companies were widely regarded as world leaders in advanced robotics technology, and DARPA saw an opportunity to draw these new advanced commercial entrants toward the defense industrial base.[5]

Google has different ideas. It is no secret that Google is making some of the biggest robotics bets of any player in the private or public sector, including their well-known effort to produce self-driving cars. According to one former employee familiar with company policy, despite Google's investments and the military's clear interest in robotics technology, Google has little interest in doing business with the Pentagon. DARPA experienced this posture first hand after Google withdrew Schaft from the robotics competition promptly after completing the acquisition.[6]

It is unclear whether Google's posture is strictly ideological, market-based, or some combination of both—the company would not comment for this report. From a business perspective, commercial applications obviously offer a much broader, deeper, and more liquid market for robotics than defense. From an ideological perspective, Google has shown great concern over how its technology is being used, particularly in the wake of Edward Snowden's disclosures suggesting that the National Security Agency was accessing Google cloud data without their knowledge or consent.[7] Google even established what some characterized as a mysterious ethics board in the wake of its purchase of DeepMind, a United Kingdom-based artificial intelligence lab.[8]

Whether Google's concerns are driven by an ideological opposition to military applications or perhaps a more commercial desire to distance itself from government applications to reassure customers in the wake of the Snowden revelations is unknown. Regardless, two diverging views have emerged regarding the long-term implications of Google's robotics acquisitions on defense technology.

The first is that Google's acquisition and associated posture represents a lost opportunity for defense, as the initial DARPA investment will not be recouped and the technology will be lost to the private sector. Furthermore, this view reinforces the inability of the traditional defense industrial base to have the cash and foresight to acquire these technologies in the first place, much less invest in continued development of the nascent technology absent a Pentagon-funded program. The difficulty is further compounded in an era of federal budget dysfunction in which sequestration, threats of government shutdown, and perpetual continuing resolutions erode any semblance of fiscal certainty for companies focused on defense contracts.

The second view is that Google's acquisition is representative of the natural and healthy evolution of advanced technologies in the 21st century. Yes, the DARPA investment is initially lost to the private sector, but it may ultimately deliver substantial return on investment to the taxpayer with commercialization and widespread adoption of the technology in society, just as the taxpayer funded ARPANET of the late 1960s evolved into the Internet of today. This bet is the fundamental justification for the billions of dollars in research funded by the federal government annually.

But what's the benefit for defense? One argument is that military funding alone would never be sufficient to produce the kinds of robots it needs in a manner that is reasonably cost effective as the economies of scale are just not there. Those in this camp argue it is better for Google to throw their market power at robotics and commercialize and scale the technology so it's ready to be assimilated back into the defense enterprise, assuming the technology could at that point be acquired from Google or another supplier. At this stage the defense industrial base could apply their unique skills to harden and/or weaponize the robot chassis. In this scenario the military achieves the dual benefit of fielding a platform developed with billions of dollars in private sector investment while also leveraging the full benefit of the unique and highly specialized skills within the existing defense industrial base.

Certainly this approach carries risk, such as the transfer of the underlying technology to foreign competitors via global commercial sales, as well as the ability of the defense industrial base to assimilate and produce a militarized version of the technology in a timely manner without it being made obsolete by the faster moving commercial segment of the market. Additionally, it is reasonable to question whether large system integrators are best equipped to assimilate, militarize, and deploy some of these advanced technologies, particularly if they do not involve the production of large capital assets.

Despite the divergent views on Google and robotics, there are three salient takeaways for the issue at hand—how advanced technologies may evolve in the globalized economy.

<u>The defense industrial base cannot deliver advanced technologies on its own.</u> Beyond pure defense plays, the defense industrial base lacks the market power and cash to compete with global commercial firms for the acquisition of new technologies that cross both the public and private domains. As discussed in chapter one, the defense industrial base also lacks the resources to compete with the broader base of advanced technology companies in terms of R&D.

<u>Assimilation may work, but it will be slow.</u> The eventual assimilation of advanced technologies into the defense industrial base will occur, but it will be slow and inefficient within the current system of exceptionally long development cycles and "requirements creep." The parallel development path on the commercial side will undoubtedly be much faster, increasing the risk of obsolescence of the underlying technologies. Additionally, foreign competitors or non-state actors may have access to the same underlying technology, considerably leveling the playing

field with respect to militarization or deployment of a crudely modified commercial technology as an asymmetric threat (e.g. IEDs strapped to a robot or drone aircraft).

Even Google can't predict the future. Despite Google's huge investment in robotics, there is no guarantee it will pay off. Agencies like DARPA help leverage relatively small taxpayer investments to explore potentially big technological bets, and in some cases they result in the additional deployment of private capital to take the bet even further, as is the case with Google. Bringing the power of commercial markets to bear to explore these new technologies is one of the underlying innovative strengths of the U.S. economy, and it ultimately ensures the taxpayer does not bear all of the risk. Indeed, the future of many advanced technologies is uncertain in the near-term, and a diversified defense industrial base can help mitigate these risks, with many players researching and investing in new technologies that may have both a public and private nexus.

Given these points, it is clear that technological superiority will be unsustainable in an era of globalization and commercialization without fully leveraging the strength and depth of the U.S. economy, particularly in the emerging tech sector, and also reforming acquisition processes to speed the deployment of new technologies.

"It's tough to make predictions, especially about the future."—Yogi Berra

We know what the last "revolution" in defense technology looked like and approximately how long it lasted; however, we cannot predict the next one. The diffusion of current advanced technologies via globalization and commercialization is increasing the potential threat to U.S. forces, as is the specter of additional global instability in the post-Cold War era.

All this is to say we must be more flexible and agile than ever before, as there is a higher probability we won't get our 21st century security investments right the first time. To this end, our defense industrial base must be as diverse as possible, and this means attracting new entrants, and making our acquisitions system flexible and agile enough to accommodate them. Increasing diversity of the base will also increase competition, a positive market force for the health of the system.

This does not necessarily mean pushing traditional players out but rather developing a system in which new entrants can add value, extract value, and play a complementary role. As it stands, the system is in every respect biased toward traditional actors, resulting in tremendous barriers to entry for new entrants and little incentive to change.

As a result, two key questions remain.

1. Do emerging technology companies in places like Silicon Valley even want to play?

2. If some do want to play, how can barriers be lowered to get them in the door?

Notes

[1] Jonathan W. Greenert, "Payloads over Platforms: Charting a New Course," *Proceedings* 138/7/1,313 (July 2012), http://www.usni.org/magazines/proceedings/2012-07/payloads-over-platforms-charting-new-course, accessed April 2015.

[2] Amber Corrin, "Audit finds gaps in cybersecurity of critical DoD systems," *C4ISR & Networks*, January 22, 2015, http://www.c4isrnet.com/story/military-tech/cyber/2015/01/22/cybersecurity-reliability-gaps-dod/22167231/, accessed April 2015.

[3] Scot J. Paltrow and Kelly Carr, "How the Pentagon's payroll quagmire traps America's soldiers," *Reuters*, July 2, 2013, http://www.reuters.com/investigates/pentagon/#article/part1, accessed April 2015.

[4] David Francis, Why the D.O.D. Can't Balance Its Books," *The Financial Times*, February 11, 2013, http://www.thefiscaltimes.com/Articles/2013/02/11/Why-the-Defense-Department-Cant-Balance-Its-Books, accessed April 2015.

[5] Doug Cameron and Alistair Barr, "Google Snubs Robotics Rivals, Pentagon," *The Wall Street Journal*, March 5, 2015, http://www.wsj.com/articles/google-snubs-robotics-rivals-pentagon-1425580734, accessed April 2015.

[6] Ibid.

[7] Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *The Washington Post*, October 30, 2013, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html, accessed April 2015.

[8] Patrick Lin and Evan Selinger, "Inside Google's Mysterious Ethics Board," *Forbes*, February 3, 2014, http://www.forbes.com/sites/privacynotice/2014/02/03/inside-googles-mysterious-ethics-board/, accessed April 2015.

CHAPTER 4: RESEARCH RESULTS

DO NON-TRADITIONAL COMPANIES IN SILICON VALLEY EVEN WANT TO DO BUSINESS WITH THE PENTAGON?

Chapters one through three have set the stage by looking broadly at the environmental, historical, and market factors that have shaped the evolution of today's MIC. The following research is based on interviews with 47 people including Silicon Valley executives and venture capitalists, senior government officials, and corporate leaders within the traditional defense industrial base. The majority of interviews offered perspectives from far outside the beltway and were formative in shaping the complexity described in the previous chapters, the analysis provided in chapter five, and the series of policy recommendations presented in chapter six.

Research sources and methodology

With limited resources and sample size, it is of course impossible to speak for a business community as large and diverse as Silicon Valley's. In fact, the functional and geographic scope of the term itself can be reasonably debated.

The Silicon Valley perspective reflects the results of 22 interviews with current or former technology executives, managers, and venture capitalists (some of whom are not physically located in Silicon Valley). Interviewees were identified and selected through a variety of mechanisms, including announcements on social media forums, as well as leveraging the author's various professional networks. Interviewees were not limited to any particular sector within technology, with the goal being a diverse cross-section of companies, including software, hardware, big data, and cybersecurity. With the exception of three large, established players, the majority of companies were early stage, with an average size of 70 employees.

The response to interview requests was generally favorable, but many respondents indicated a reluctance to engage on the topic given their generally unfavorable view regarding the state of leadership and management in the federal government with respect to effectively leveraging technology. Some more seasoned entrepreneurs noted the stark contrast in this perception today relative to the more highly regarded era of productive government research investments in the post-World War II era that ultimately fueled the Digital Revolution.

A total of 19 interviews were conducted with current or former senior government officials engaged in acquisitions, research and development, human capital management, or technology policy in the Department of Defense, Department of Homeland Security, National Security Agency, White House Office of Management and Budget, White House Office of Science and Technology Policy, and the U.S. Digital Service. The focus of these interviews was to assess barriers to entry for non-traditional companies from the perspective of government stakeholders, as well as barriers to reform.

Finally, six interviews were conducted with current or former executives within the traditional defense industrial base. While not the primary focus of this research, these interviews provided perspective on how traditional prime contractors view the innovation challenge.

Silicon Valley interview results

Interviews were in-depth sessions that generally lasted 45 minutes to an hour, covering a range of questions regarding barriers to doing business with the federal government in the national security space. A summary of the questions and answers most relevant to this report follows.

With respect to your company's strategy and values, how would you characterize its desire/willingness to do business with the federal government's national security apparatus (e.g., DOD, DHS, FBI, CIA, NSA, etc.)?

Seventy-five percent of executives indicated a general willingness and in some cases a strong desire to do business with the federal government on matters of national security, provided it makes sense for their business.

But the vast majority of these executives could not envision a viable scenario in which doing business with the federal government made sense commercially. In general, they cited a host of significant barriers to doing business with the government, including an exceptionally slow and cumbersome process that would quickly erode any potential commercial benefits, particularly for smaller companies focused on speed, cash flow, and growth.

Of the 25 percent not willing to do business with the federal government in the national security space, the majority cited fundamental risks or incongruities with their business model.

For example, data and marketing analytics companies like Klout, whose business model involves mining social media data from millions of users and selling it to other companies for targeted marketing efforts, saw any engagement with the federal government as a risk to the integrity of their business model. Former CEO Joe Fernandez clearly recognized that a government security agency might be interested in knowing what "700 million people talk about around the world on social media and how likely these people are to be incited or inspired by what others say." Fernandez also recognized how damaging any engagement with the government could be to his business as it had the potential to erode the trust of its users, particularly in the wake of the Snowden revelations. "We had people come poke around to look at our data, political campaigns, banks, and security people, and we always stayed away as much as possible as we didn't want consumers freaking out about what we were doing with their data."

Taking a different tact on fundamental incongruities, Quick Left Software co-founder Ingrid Alongi cited the difficulty of deploying "agile" software development techniques within the constraints of typical government contracting vehicles. Quick Left, one of the only companies interviewed for this project outside of Silicon Valley, specializes in agile techniques and sees the government's process as too antiquated to support the best software products.

Alongi explained that government procurement systems are generally biased toward the more traditional "waterfall" methodology of software development, in which an extensive list of requirements and schedule of deliverables are settled and priced up front. In some cases there is technical justification for this approach, but in the case of government procurement it is often predominantly reflective of the need to accommodate rigid requirements.

Alongi generally steers well clear of government contracts, as her firm is committed to agile development projects. Alongi views the requirements articulated through the government's request for proposals (RFPs) process as increasing the risk of failure in complex software development. As Alongi explained from her office in Boulder, Colorado, "No matter how clear the deliverables are [with a software project], they change as soon as we start the project," and the resulting iterative process is very difficult to execute within the confines of a government contract.

According to Alongi, changes along the way are driven by a number of factors, including client feedback, integration challenges between services and technologies, unanticipated market changes driven by competitors, or evolving customer feedback. "Of course, not showing anyone progress is a way to avoid some of these, but then you risk the 'grand unveiling,' and in that way you most certainly will get it wrong, and by then you've spent far too much time and money to correct things," said Alongi.

As a technology executive, how would you characterize your personal desire/willingness to do business with the federal government's national security apparatus?

Ninety percent of executives had no personal or ideological objections to doing business with the federal government on matters of national security. In fact, many executives were quick to point out they do not pick and choose customers based on ideological positions but rather that commercial interests strictly carry the day.

Oren Michels, former CEO of Mashery, an application program interface (API) platform company, said the primary moral issue is, “Can you serve the government in a way that is consistent with running your business and being successful when there are a lot of hurdles to cross to get there?” Tom Lounibos, CEO of Soasta, stated, “For me it’s about finding a problem and solving it, there are no borders that are defined by a government agency.”

While not specifically asked, many executives responded to this question by affirming their patriotism and general willingness to work with the government should an opportunity arise that would not compromise the viability of their business.

The 10 percent of executives ideologically opposed to working with the government on matters of national security expressed general concern that their technology might be weaponized.

What was the impact of the Snowden affair? Did it substantially change your or your company's perspective on doing business with the national security apparatus?

Eighty percent of executives interviewed indicated that the Snowden disclosures had no impact on their companies’ perspectives on doing business with the national security apparatus. However, the remaining 20 percent had very strong feelings regarding the adverse impacts the Snowden affair had on their willingness to consider business with the national security apparatus.

Regarding the Snowden affair, John Balen, general partner at Canaan Partners, said, “It's a nice thing to talk about over wine, but it does not show up in the boardroom because most small companies are solely focused on getting customer traction in order to build revenues and become self-sustaining."

The remaining 20 percent were generally limited to specific technology sectors like cybersecurity and “business to consumer,” wherein any engagement with the federal government’s national security enterprise might risk alienating customers concerned about privacy. This dynamic was particularly pronounced in businesses that had a significant overseas portfolio and may have lost customers in the wake of the Snowden revelations. Reinforcing this point, Yusuf Bashir, head of global venture capital for Infosys, said, “Look, if you are a business-to-consumer company, your biggest concerns are what's going to stop people from using your solution, and what's going to strike fear in your users?"

Have you ever met (in person or via phone) with someone from the federal government's national security apparatus to discuss a potential project?

Sixty-five percent of executives had met with someone within the federal government's national security apparatus (e.g. DOD, DHS, FBI, NSA, CIA) at some point in their career to discuss a particular project or service.

While this could be interpreted as a positive statistic in terms of the government's ability to reach the Silicon Valley startup community, the downside is that despite this level of reach and personal engagement, the majority of these executives were not interested in pursuing future business with the government.

Have you or your company ever bid on a project funded by the federal government's national security apparatus?

Approximately 50 percent of executives interviewed had formally "bid"—a difficult term to define due to the wide array of government contracting vehicles—on at least one government contract in the national security space at some point in their career. The majority of this subset was also successful in securing government business at some point in their career. In most cases success stories involved either larger, established companies or companies in the cybersecurity sector.

This could be interpreted as good news in terms of reach and level of success. However, this number is particularly disconcerting because, here again, the majority of executives were not interested in pursuing future business with the government.

What are the biggest barriers to increasing Silicon Valley's desire/willingness to work with the federal government's national security apparatus?

Approximately 70 percent of executives cited the exceptionally difficult nature of the government procurement process as the most significant barrier to entry; specifically, that it was too hard, too slow, and not transparent.

Serial entrepreneur Jim Marggraff, CEO of Eyefluence, developers of an optically controlled user interface for head-mounted displays (HMDs), gave up on defense funding for his startup because, "There was always one more meeting, but it never went anywhere."

One executive at an innovative financial technology company who asked not to be identified, described the company as mission driven, motivated to solve important problems, and eager to attract a military clientele. In her view, business with any element of the federal government would be too risky because "sadly, they just don't move fast enough … I just don't see a world where there is a partnership with government that makes any sense for us because of the all drawbacks."

Balen, from Canaan Ventures, told of an earlier attempt by one of his companies to sell to the government. "It took one person working full-time in Washington to get one company on the GSA schedule and we ultimately got some deals out of it after three years; you can't build a company on this kind of business."

Clint Chao, managing director at Moment Ventures, sees tremendous potential and win-win opportunities for both the companies he invests in and the government on a number of fronts. "However, a startup company can't go broke trying to sell to the federal government, so they can't afford to spend the resources on a long drawn out bureaucratic sales process." Chao sees business with government as a very tough space to incentivize for the startup community. "Given the long sales cycles, we've found it to be a hard sell to fund a startup specifically targeting a federal application, so in most circumstances, I'm not likely to fund a company if that was their initial target," said Chao.

One CEO of an early stage cybersecurity firm who asked not to be identified due to the sensitive nature of his company's work with the government, saw defense procurement processes as more than just difficult for small businesses but also as having an adverse impact on cybersecurity. "Rules and regulations slow things down so much that it is pointless to try to fight the bad guys because they are just moving so much faster," said the CEO, adding that acquisitions professionals often "view speed as something that they don't have to be concerned with, and this makes it almost impossible to secure and protect government networks."

Twenty-five percent of executives cited the specialized nature of the market as a significant barrier to entry. For example, the investment required to engineer a specialized "government version" of a particular piece of hardware or software may not be justifiable relative to doing business with a much larger commercial market.

Roger Hine, co-founder and chief technology officer of Liquid Robotics, a company that successfully secured some small defense contracts early in its history for their autonomous Wave Glider ocean robots, sees both challenges and opportunities in the defense space. Hine explained the commercial "benefits snowball from having a larger application base and multiple adopters of the platform." According to Hine, Liquid Robotics is working hard not to divert its engineering resources to work on perhaps unnecessary government specialization that may not transition to higher volume commercial applications and is optimistic they are making headway on this front.

Multiple executives cited a lack of transparency regarding both processes and potential project opportunities as a significant barrier to entry. Milan Minsky, vice president of product development at Rayvio, a Silicon Valley-based ultraviolet lighting startup commented on her recent experience signing up for the DOD's Small Business Technology Transfer (STTR) program. "The whole process was incredibly painful. All we wanted was some transparency and easier access to the people involved. Instead the websites we had to use seemed overly complex and were very difficult to navigate; you had to do handstands and cartwheels just to get limited information and sign up for the program."

What are the strongest incentives to do business with the federal government's national security apparatus?

Approximately 60 percent of executives cited the potential for new revenue sources as the primary incentive, acknowledging that once you get your foot in the door it has the potential to be a steady stream of good revenue.

Fifty percent of executives cited either being mission driven or helping to solve important and interesting problems as an incentive.

Kenneth Carter, legal counsel at the Internet performance and security firm CloudFlare, said fixing tough problems provides tremendous motivation and is part of the ethic of Silicon Valley companies. Carter acknowledged the difficulties inherent in government procurement for small companies but sees rewarding opportunities as well. "We see opportunities to help fix things, like making it harder for terrorists to spy on the government online and harder for the government to surveil on citizens without the due process of law."

Minsky, who thinks the military might be interested in Rayvio's lightweight water purification technology, sees it as not just an opportunity for sales but a way to have a positive impact. "If soldiers in danger need a lightweight system to access clean water, then we can help," said Minsky.

How would you characterize the state of human capital flow between the federal government's national security apparatus and Silicon Valley?

The majority of executives generally characterized the flow of human capital between Silicon Valley and the federal government in the range of negligible to nonexistent. Interviews yielded some qualitative evidence of negligible flow from "east to west" (i.e. government to Silicon Valley) and virtually nonexistent flow from "west to east" (i.e. Silicon Valley to government).

With respect to the national security apparatus, interviews yielded qualitative evidence of some flow between federal government cybersecurity professionals (e.g. NSA) and Silicon Valley technology companies.

Executives generally viewed west to east flow as nonexistent except for rare cases of political poaching, in which senior technology executives are courted to assume high level government positions to promote the use of technology. U.S. Chief Technology Officer Meghan Smith's recent move from Google to the White House was the most cited example.

Responses to this question also indicated a strong perception that federal employees lack the requisite skills needed to engage productively with smaller, faster moving technology companies, like understanding the potential for the technology and how best to apply it in a government application.

Three prominent barriers to more robust human capital flows were identified:

- Fundamental cultural differences between Silicon Valley and the federal bureaucracy.

- Tremendous demand and competition for technology talent, like software and hardware engineers, and an inability of the federal government to compete effectively in this environment in terms of salary, benefits, and flexibility. More than that, said Mark Bregman, former chief technology officer at NeuStar, a cloud services provider, "In technology, the best people want to work with the latest and greatest stuff." Bregman thinks the federal government is no longer viewed as being on the leading edge of technology.

- Outside of a limited number of specialists, the federal government's perceived inability to generate human capital that could effectively compete for employment in Silicon Valley.

Does Washington need Silicon Valley more than Silicon Valley needs Washington?[1]

Executives were divided on this question, with strong feelings on both sides.

Some felt that Silicon Valley was doing “just fine” with limited engagement with the federal government in terms of both policy and business and were dubious of the potential for early stage companies to ever be successful doing business with the federal government.

Serial entrepreneur David Henkel-Wallace sees a “gain mismatch” between Silicon Valley and Washington, D.C. in part because the “clock speeds are different.” For example, “Approving a grant takes so long that it’s not really an appropriate way to fund a business.” That said, as a taxpayer, Henkel-Wallace recognizes it’s not in his interest for these processes to be fast if that means they become sloppy, corrupt, or wasteful. Henkel-Wallace sees an important role for government in helping “with the adjustment” that is needed as new technologies remove more human labor from the economy, a transition he expects will be difficult in the short-term but will pay great dividends to the nation and the government in the long-term.

In the meantime, Henkel-Wallace suggested that the government should focus on “reducing drag” for businesses and innovators, adding, “As long as nobody shoots down Fed-Ex planes and our currency is stable, then I don't need much from Washington.” Henkel-Wallace doesn’t view his position as criticism of the government and certainly does not intend to advocate a “laissez-faire” posture. In fact, he sees an important role for government in supporting innovation and sustaining a rules-based system but doesn’t think it’s realistic to expect significant changes in the way government does business with start-ups. His current company is considering doing some limited customization of their commercial off-the-shelf (COTS) technology for a government agency and says “it could be good for us,” but won’t “make or break a company.”

From a business perspective, executives felt they had access to a wealth of alternative markets both domestically and internationally, and thus there is no imperative to break into the federal space. In this context, barriers to doing business with the federal government were almost universally viewed as a loss for government as opposed to a loss for Silicon Valley.

Many executives saw an enduring need for government to have access to cutting edge technology and thus saw engagement with Silicon Valley as a critical success factor. The worst thing government could do, said Chao, is to continue to “buy dated technology only because it was the easiest technology to acquire.”

Others recognized the potential for government to “do damage” to Silicon Valley with misguided legislation, regulation, and policy, and that more active engagement on the policy front is needed. More seasoned entrepreneurs also recalled the fundamental role federal R&D investments played in creating the ecosystem, and hoped that a similar dynamic might emerge again in the future.

Senior government official interview results

Interviews with senior government officials were focused on identifying barriers to entry for nontraditional companies from an agency level as well as any best practices being implemented to address the challenge.

Most officials cited strong momentum within the Obama Administration to increase innovation and competition for government contracts by attracting new entrants, particularly in defense. Most visible, perhaps, is the DOD's "Better Buying Power" initiative which began in 2010 and, among other things, focuses on increasing innovation and competition within the defense industrial base. Most acknowledge that measuring progress of this initiative will be difficult, but there is clearly broad support at the highest levels of Pentagon leadership.

Officials cited internal culture and human capital as significant barriers to reform within their agencies or the agencies they worked with. Barriers included an aging federal workforce that lacks diversity in many respects, an inability to hire people in a timely fashion, and an inability to attract and hire the right talent to implement innovative technological solutions and champion reforms. One senior government official said, "There are a lot of people in very powerful positions with very outdated skill sets and a strong tendency to maintain the status quo."

Onerous restrictions on attending professional conferences also emerged as a factor in recruiting and retaining top technical talent. Some officials noted that top professionals in science, engineering, and technology want to interact with their peers at top conferences, and there is very little ability to do so within the federal government's highly restrictive conference posture. While there are some nominal cost savings with this approach, it comes at the cost of greater information flow, transparency, and interaction between the public and private sectors, particularly in emerging technologies where conferences play an important role in the innovation ecosystem.

Several best practices emerged from these interviews and will be addressed in greater detail in chapter six.

Traditional defense industrial base interview results

While not the primary focus of this report, interviews were also conducted with current or former executives in the traditional defense industrial base, with the intent of capturing their perspective regarding barriers to innovation and attracting new entrants.

Executives acknowledged decreased R&D investment across the industry driven by a number of factors, including federal budget uncertainty and the Pentagon's tendency to award contracts to the lowest bidder vice the best technological solution.

As far as attracting new entrants, executives generally characterized the imperative as dependent on the particular product. Cyril Draffin, former director of strategy at Northrop Grumman, said, "If you're talking about sophisticated hardware to go on a military aircraft when there are multiple suppliers, then the need to attract new entrants is not so pronounced; but if you're talking about developing state of the art technology in cyber, then attracting and using the skills of the rapidly evolving commercial sector is desirable." Draffin added that, "State of the art software companies are much faster, and they iterate more, whereas larger defense companies usually don't put out tested releases quickly."

Bob Kokorda, vice president Defense Systems and Services International at Sikorsky Aircraft, is confident in the company's ability to continue to innovate, particularly on the fundamentals of their platforms. Kokorda acknowledged that staying ahead in IT-intensive components like avionics is a continuous challenge, in part due to finding the right suppliers and the inherent nature of systems integration. "It's hard to stay state of the art on this front, as every year or so there is a new iteration on sensors or avionics, and the cost of integrating this equipment is very high due to extensive certification and testing requirements."

Kokorda sees higher barriers to entry at the platform level but sees promising opportunities for smaller, more agile companies at the component or payload level. "This is the space where new tech guys can break in, and if you have a disruptive application, this is a good place to go," said Kokorda. For its part, Sikorsky has a Sikorsky Innovations arm that is externally focused and seeking to identify and incorporate these types of new technologies.

As one of the few players in defense that also sustains a robust commercial business line, Sikorsky sees both their commercial and government markets as contributing to technological development, with the commercial market's focus on state of the art technology being a significant driver toward incorporating more innovative solutions.

Sean O'Keefe, former CEO of Airbus North America, sees little incentive for prime defense contractors to diversify to commercial markets under current conditions and also sees significant barriers to entry for non-traditionals. These companies "have other options and don't want to deal with carrying overhead just to be able to speak the government's language or to have lawyers ready to file a protest," said O'Keefe.

With respect to recent efforts to reform defense acquisitions, O'Keefe sees them as "more of an accommodation to existing players rather than any significant effort to attract new entrants." That said, O'Keefe is optimistic about the Pentagon's effort to work closely with Chairman Thornberry. Their cooperation has the potential to "clear the underbrush of conflicting regulations and processes" and "set the stage for new entrants and pathways to new solutions to emerging problems."

Notes

[1] This provocative question was intended to elicit general comments about the state of the relationship between policy makers in Washington, D.C. and the technology industry in Silicon Valley.

Chapter 5: Analysis

Few incentives, high opportunity costs: Why Silicon Valley has little interest in doing business with the Pentagon or anyone else in the federal government

The bad news

- Non-traditional companies face considerable barriers to entering the defense industrial base, barriers that are likely underestimated by lawmakers and policymakers in Washington, D.C.

- The most prominent barriers relate to the *process* being too difficult, too slow, and too opaque, characteristics that run counter to the type of business environment needed to foster innovation and attract new entrants.

- The size and specialized nature of the *market* relative to other commercial applications also generates significant barriers to entry for smaller companies focused on growth and broad market penetration.

- Fundamental *cultural* and *workforce* differences help sustain these barriers. Significant cultural barriers with human capital implications include:

    - Speed and growth versus bureaucratic, process-oriented, and arbitrary;

    - Disruptive innovation versus status quo;

    - Fail fast, fail often versus no tolerance for admitting failure;

    - Work the most challenging problems with the best people and the best technology versus work the most challenging problems with a highly restrictive personnel management system and access to limited technologies; and

    - Creative, iterative engineering practices versus "requirements based engineering" that constrains the manner in which a particular problem can be solved.

- Barriers result in a system inherently biased toward larger, more mature companies that have the resources to sustain longer development cycles and develop a specialized product line for government applications.

- Attracting a renewable source of new entrants to the defense industrial base from places like Silicon Valley will be much more difficult than most in Washington realize. The "meal" is unappetizing and there is little incentive to come to the table.

- There is little distinction between the desire to do business with the federal government's national security apparatus and the desire to do business with other government agencies. The "meal" is equally unattractive.

- Barriers to entry are viewed as prohibitive, with any potential financial benefits not worth the "pain and suffering" of attempting to navigate the procurement process.

- With some noteworthy exceptions like DARPA, NASA, and the NSA, Silicon Valley technology executives tend to view the government's ability to embrace and leverage emerging information technology as extremely poor. The failed rollout of healthcare.gov was often cited as exemplifying what technology executives already knew: the federal government, its procurement system, and its traditional contractors are not well suited to manage highly complex information technology projects.

- The Snowden affair still looms large in some sectors. Companies whose business model depends on storing and securing large amounts of customer data (i.e. business to consumer applications) continue to perceive association with the federal government's national security apparatus as a fundamental threat to customer trust and therefore an existential threat to their business.

- There is generally a high level of pessimism regarding the federal government's ability to provide greater flexibility and accommodation for nontraditional technology companies.

- Human capital flows between Silicon Valley and the federal government workforce are generally nonexistent and unlikely to change. There are some notable exceptions like cybersecurity professionals leaving the NSA for the private sector and senior tech executives taking political appointments in Washington, D.C. The lack of human capital flow helps reinforce the substantial cultural barriers.

- Age demography and turnover for DOD civilians is out of step with the broader U.S. economy and significantly out of step with the technology workforce in places like

Silicon Valley. This is significant, as DOD's 150,000-person acquisitions workforce is 90 percent civilian and dominated by personnel between the ages of 40 and 60. While this more experienced workforce brings a wealth of important knowledge and continuity to the acquisitions process, it likely comes at the expense of turnover and the associated injection of new ideas. This perception was reinforced by a number of Silicon Valley executives, who assessed the aging federal workforce as contributing to both cultural and procedural barriers to entry for non-traditional companies.

- The extensive use of veterans hiring preferences across the federal government, and in particular DOD, likely plays a significant role in elevating the average age of the workforce as well as its overall level of experience and lack of professional diversity (e.g. 44 percent of DOD's mission critical employees have a record of prior military service).[1] Even if more junior Silicon Valley professionals wanted to serve in the federal government, it might be exceptionally difficult for those without veterans status to compete effectively.

- There is a powerful perception that firms get government contracts because they have figured out how to get them, not because they are necessarily the best choice to solve a particular problem or provide a particular service. According to Jon DiLuna of Technical Assent, "The system rewards those that have the time, resources, and experience to navigate the bureaucracy, vice those that have the best product or most innovative solution." This reinforces a bias toward companies that one executive referred to as having "a core competency in compliance."

The good news

- The vast majority of executives interviewed had no ideological objections to doing business with the federal government in the national security space.

- Despite the smaller and more specialized nature of the defense market relative to the global commercial space, the scale is still larger than many other markets and generally attractive in this sense.

- Notable segments of those interviewed characterized themselves as patriotic, mission driven, problem solvers who want to help their country provided it does not damage their business in the process. Some also identified the potential "prestige" and "influence" associated with certain types of advanced technology work related to national security.

- Solving big, interesting, impactful problems using technology emerged as a strong characteristic of Silicon Valley culture. Several interviewees cited this cultural trait as ripe for creative exploitation by the federal government, which is clearly one of the world's leading purveyors of difficult, impactful problems waiting to be solved.

- With some notable exceptions, the Snowden affair is generally a red herring and appears to have very little impact on actual business decisions. Outside of specific sectors like cybersecurity, big data, and business to consumer applications, the Snowden revelations do not appear to have deterred early stage Silicon Valley companies from doing business with the federal government on matters of national security.

- This research did yield some success stories, including that of Liquid Robotics, where Roger Hine is more optimistic about his company's ability to secure future business from the Pentagon. Hine's goal is a 50-50 split between government and private sector business in which he hopes his autonomous Wave Glider platform can be used uncorrupted in either market and then be configured to carry whatever payload the customer needs, whether it be the U.S. Navy or an offshore oil and gas company. Hine is hopeful that this approach will yield a sustainable and diversified base of customers for the future.

Other interesting takeaways

- With respect to future prospects for doing business with the federal government in national security, two broad "camps" of early stage executives emerged:
  - More seasoned entrepreneurs who had attempted to do business with the government at earlier stages of their career were unlikely to try it again. They view the process as too difficult and the probability of success too low.
  - Less experienced entrepreneurs who had not yet attempted to do business with the government were more optimistic about their probability for success.

- It is important to note that the Snowden affair cut both ways. Some companies indicated a noticeable adverse impact on their business: customers withdrew their business due to perceived data insecurities. Conversely, some companies suggested that the Snowden affair was a boon to their business by raising awareness of data and network vulnerabilities and creating broad incentives to better secure them from both state and non-state actors.

- Executives acknowledged the potential of partnering with an existing prime contractor as a means to do business with the government. This was generally viewed as a decidedly unattractive and inefficient option for early stage companies equivalent to paying a tariff, particularly when other more lucrative markets are available where they could compete without such an encumbrance. This sentiment is a strike against those suggesting traditional prime defense contractors can simply partner with smaller, more agile emerging technology companies to deliver innovative solutions.

- Federally funded research and prototyping in the defense enterprise remains highly regarded. DARPA in particular continues to enjoy a strong reputation as an innovation outlier within the federal government. Among those interviewed, technology executives who had worked with DARPA generally viewed the model favorably but regretted the difficulty transferring technology to more practical, lucrative, and scalable applications downstream. Indeed, the challenge of "crossing the chasm" in defense was generally viewed as extreme relative to commercial markets, where feedback loops are much faster and the gap between prototyping and "program of record" is perceived to be much smaller.

- Barriers to entry for non-traditionals and barriers to change inside of government are likely far more formidable than most policymakers in Washington, D.C. realize. These are not new problems but rather problems that have been exacerbated and illuminated by the dynamics of the Information Age.

- When it comes to engaging Silicon Valley companies, there is a strong perception that policy makers are biased toward larger, more visible players like Google. As a publicly traded company with more than 50,000 employees and $360 billion in market capitalization, Google is no longer considered an early stage technology company. It is important to remember that the Silicon Valley technology ecosystem is much larger than the Apples, Googles, and Facebooks of the world and that significant innovation and intellectual property are being generated by much smaller companies with negligible resources and avenues for engagement with policymakers.

- There remains broad support for federally funded R&D activities (both defense and non-defense) as a critical element to sustaining innovation in the United States.

How did we get into this situation?

In order to understand how to improve the current dynamic between Silicon Valley and Washington, D.C., it is important to have some perspective on the driving forces that led to the current situation.

First, let us consider the traditional prime defense contractors. These contractors are not bad or incompetent. The United States' base of prime contractors are responsible for some of the most significant innovations of the 20th century and are generally viewed as the best in the world at what they do. These firms have a business model and are trying to execute it in a manner that delivers the best technology to the U.S. military while also delivering the best results to their shareholders.

This can be exceptionally difficult in a highly uncertain market subject to significant financial and political risk. Current industry trends like stock buy backs in lieu of future capability investments are a reflection of the Department of Defense and federal government's unpredictability, particularly in the wake of sequestration. In other words, there is flagging confidence in the prospects for stable funding streams and new programs that might justify more productive defense industry investments in future capability.

Regardless, a healthy base of prime defense contractors will always be needed and will always be relatively small due to the highly specialized market for pure public goods like missiles, warships, and warplanes. They are being asked to build things they cannot sell to anyone else but DOD! The notion of dramatically restructuring the core base of major systems integrators is just not realistic.

Major systems integration is difficult, expensive, and time consuming work, and few companies have the capability to do this within the strict framework of the defense acquisition system. That said, large portions of defense procurement do not involve major system integration. Additionally, the trend toward "payloads over platforms," discussed earlier in this report, naturally lends itself to diversifying the defense industrial base with smaller and more agile suppliers to help remain on the frontier of emerging technologies.

Second, consider the role of the federal government, the Department of Defense, and associated acquisitions policies. Acquisition legislation, regulations, and policy exist for good reason, and in most cases are written in blood, wasted taxpayer dollars, lost political capital, or some combination thereof. Talk of modernizing, streamlining, and simplifying the process makes sense, but it is also important to remember what is at stake. When a pilot fires a missile in combat he or she has to know that it is going to work. Tolerance for failure in this context must be extremely low; lives and national security depend on it. Additionally, reasonable controls are needed to prevent defrauding the government or making large investments in companies that are unlikely to be successful.

But not every system is a missile, and the acquisition process should be flexible enough to know the difference. Furthermore, we must acknowledge the cumulative effects of decades of adherence to a strict rules-based, compliance-based, and highly risk-averse system, and the culture and workforce it has engendered. That is, we have a system that favors a consolidated, insular defense industrial base that is simply unable to accommodate smaller, more agile, and more diversified advanced technology companies engaged in 21st century global competition.

To be clear, defense is not alone in this regard. This research shows little discernible difference between security and non-security related business with the federal government. They are generally equally distasteful to the Silicon Valley executives interviewed for this research.

So does it all come down to Silicon Valley?

Not really. Despite its unmatched clout as the world's leading innovation engine, Silicon Valley is no panacea when it comes to fixing defense acquisitions and ensuring military technological superiority. While data on "failure" rates for Silicon Valley startups vary widely, the general academic consensus is that the majority fail.[2] Some studies have even estimated the failure rate to be as high as 75 to 90 percent, but the true definition of failure in the context of a tech startup remains unsettled. In other words, there are plenty of bad ideas in Silicon Valley, too.

Additionally, commercial market incentives will never fully align with those in the defense sector. Entrepreneurs seeking billion dollar exits will not find themselves selling to DOD. Furthermore, solving rapidly evolving problems for mass market consumption may not always lend itself to tackling bigger, more complex, and more consequential ones.

Dan Kaufman, currently director of the innovation office at DARPA, said that Silicon Valley is doing some really "cool stuff, I can order up a car on my cell phone, do cool things with 140 characters, but these are not going to defeat an advanced enemy fighter jet." Kaufman, of course, recognizes that the innovation ecosystem in Silicon Valley extends well beyond Uber, Twitter, and the latest social media application, but is making a broader point that it is "naïve to think that technology companies like Google or anyone else can solve all of the tough problems we will face in defense in the future. Even these companies have failures, and they certainly aren't the only innovators out there."

For these reasons a more balanced and measured view is needed on the idea of bringing more Silicon Valley companies into the defense fold. Specifically, we must recognize that reform is desperately needed while also managing expectations about which companies will ultimately engage in this market and what they can achieve.

Notes

[1] "Fiscal Years 2013-2018 Strategic Workforce Plan Report," United States Department of Defense, July 25, 2013, http://dcips.dtic.mil/documents/SWPWholeReportCDv2.pdf, accessed April 2015.

[2] Rory Carroll, "Silicon Valley's culture of failure … and 'the walking dead' it leaves behind," *The Guardian*, June 28, 2014, http://www.theguardian.com/technology/2014/jun/28/silicon-valley-startup-failure-culture-success-myth, accessed April 2015.

CHAPTER 6: POLICY RECOMMENDATIONS

A RANGE OF IDEAS TO ATTRACT NEW ENTRANTS AND IMPROVE THE SYSTEM

"Innovation—any new idea—by definition will not be accepted at first. It takes repeated attempts, endless demonstrations, monotonous rehearsals before innovation can be accepted and internalized by an organization. This requires courageous patience."

—Warren Bennis

This research has yielded a number of promising policy recommendations, many of which emerged directly from the in-depth interview process. These recommendations offer a wide range of alternatives, from the proverbial low hanging fruit to much more difficult proposals that may not be executable in the current political environment.

It must be said that any attempt to meaningfully reform defense acquisitions and attract new entrants will require several years of sustained effort and multiple waves of executive and congressional action. Cultural change takes time.

As the largest procurement system in government, DOD acquisition reform could provide the added benefit of positively influencing other acquisition systems across the federal enterprise. While DOD's system is unique and specialized in many respects, federal acquisition regulations across agencies are generally quite similar, as are the challenges. In other words, DOD is certainly not the only agency struggling to break down barriers to increase innovation and competition for contracts.

Overarching thematic policy recommendations

- Recognize that this is a whole of government problem. While the primary focus of this project is national security and defense acquisitions, the research clearly shows Silicon Valley companies face formidable barriers to entry across the entire federal enterprise. The federal acquisitions system is not just a national security liability but also a liability to the overall effectiveness and responsiveness of government.

- Change the narrative. The concept of "acquisition reform" neither resonates with the public nor sufficiently captures the associated national security implications. The fundamental imperative for reform is sustaining our ability to effectively and responsively govern and defend the nation.

- Initiate a national conversation to better define acceptable cost, schedule, and performance risks in the context of improving our ability to innovate. In an excessively risk-averse, requirements-based, and compliance-focused acquisition system, we have decreased competition, reduced system speed and agility, and ultimately made few appreciable improvements in cost, schedule, and performance. One could even make the case we have actually increased risk in the process by substantially limiting our access to a select few contractors rather than effectively leveraging the full depth and breadth of innovation in the U.S. economy.

- Acknowledge the need for difficult civil service reform. Cultural barriers to reform in government cannot be overstated, and they are intrinsically linked to human capital. A lean, agile, and innovative acquisition system requires a workforce with the same traits. This culture can be changed but will require bold leadership.

- Similarly, acknowledge the need for difficult military personnel reform. While the defense acquisition workforce is predominantly composed of civilians, military leadership plays a critical role throughout the acquisition process, and reforms will similarly be needed to attract top talent.

- Restore some semblance of certainty and rationality to the federal budget process. Fiscal uncertainty and instability ultimately stifle innovation, increase acquisition costs for major projects, and discourage new entrants from competing. Efforts to reform the system can be quickly undermined by fiscal gamesmanship.

Higher political risk, higher reward policy recommendations

- Modernize the civil service by increasing management flexibility, diversity, and the ability to attract top talent. Previous acquisition reform efforts have failed in large part because there was no corresponding effort to modernize the workforce and change the culture. This is not only a national security imperative but an imperative for effective governance. Comprehensively addressing civil service reform would take another body of work much broader in scope than this project, but the Partnership for Public Service's 2014 report "Building the Enterprise: A New Civil Service Framework" has a host of sensible recommendations.[1]

Modernizing the veterans hiring preference should also be considered, including either eliminating or relaxing preference for retired veterans already drawing full benefits. Such a change would appropriately focus the preference on younger veterans whose transition to civilian work often carries more risk and uncertainty than those who do so with the added benefit of a robust retirement package. It would also benefit the skewed age demographics across the federal workforce.

- Modernize military compensation by creating a more flexible system to attract and retain a more diverse array of talent. While the civil service clearly plays a larger role in the acquisitions process due to both its size and longevity of service, modernizing the military workforce is also critically important to attracting the talent needed to effectively lead complex acquisitions. The January 2015 "Report of the Military Compensation and Retirement Modernization Commission" offers a number of positive recommendations in this regard.[2]

- The president and Congress should execute a comprehensive budget deal to address the rising cost of entitlements and the associated erosion in discretionary spending. Acquisition reforms will never be effective without more sensible and predictable federal budgeting.

- Ensure that the United States remains the world's most innovative economy, as this is critical to sustaining military technological superiority as well as our broader economic and national security. Leaders across government, and in particular the national security space, should advocate for federal action in three areas: sustaining robust federal R&D programs; ensuring an abundant supply of highly-skilled workers by promoting STEM education and reforming immigration laws to allow more highly-skilled foreign workers to be employed in the United States; and safeguarding the integrity and efficiency of the U.S. patent system. More detailed discussion of these imperatives can be found in a 2013 Brookings Institution report "Patenting Prosperity: Invention and Economic Performance in the United States and its Metropolitan Areas."[3]

Lower political risk, moderate reward policy recommendations

Absent political momentum for higher impact reforms, the following low hanging fruit can be leveraged to inject new flexibility and creativity into the acquisitions process, ultimately lowering barriers to entry. Some of these policy reforms require legislative action, while many others simply require more aggressive and creative use of authorities agencies already have.

Human capital recommendations:

Increase opportunities for the private human capital marketplace to "touch" the federal workforce in a meaningful way. This includes injecting fresh perspective that comes with personnel turnover by increasing the use of term appointments for critical technology interface positions.

This could pay significant dividends in positions where particular skills sets are valued, such as managing complex information technology projects and where contemporary private sector experience is needed. All federal agencies have the authority to create term positions on a year-to-year basis, and the tool offers a unique ability to attract top talent from the private sector on a short term-basis. Unfortunately, the tool is rarely used as it can create some risks for agencies, and there is a general belief that these positions are less attractive to potential civil servants.

Term appointments have a strong record of success in attracting top talent from the private sector, particularly in some of the most innovative organizations in government like DARPA and the newly created U.S. Digital Service.

Deployed effectively, term appointments offer the unique opportunity for top private sector talent to flow in and out of government. This creates both a potentially exciting public service opportunity for mission-driven people as well as a mechanism for ensuring their rapid return to the private sector to remain on the leading edge of technology and innovation. This model of employment is fundamental to the success and tremendous reputation of DARPA.

It is difficult to attract and sustain leading technological talent in the federal government full-time, particularly in IT. It would also be inefficient to try within the traditional civil service framework because: skill sets would quickly erode outside of an individual's field of expertise in the private sector; and it is difficult for federal entities to sustain effective utilization of top people as many efforts are related to a specific project that is temporary in nature, such as the deployment of a new enterprise software application.

Although all agencies have this authority on a temporary basis (e.g. appointments of one to four years), none have it granted on a project basis. This additional legislative authority would be helpful to the acquisitions process, where unique talent may be needed to help manage a technically complex program with an unknown timetable. The federal government often hires contractors for this work but typically from a limited ecosystem of suppliers. The government should be able to hire federal employees the same way and leverage the corresponding authority to attract new talent. This should be pursued via a legislative change proposal using the National Defense Authorization Act as the appropriate vehicle. Since DOD has by far the largest civilian workforce and acquisitions portfolio in government, such a change could set a positive example for innovation across the federal enterprise.

Increase use of Direct-Hiring Authority (DHA) to attract top talent. The Office of Personnel Management (OPM) can give DHA to federal agencies to fill vacancies when a critical hiring need or severe shortage of qualified candidates exists.[4] This "fast track" authority, as it is sometimes called, allows managers to hire any qualified candidate they select and bypasses a host of rules and hiring preferences that other civil service positions must follow, including the veterans preference.

Outside the DHA process federal hiring rules engender a highly centralized, rules-based process that, in addition to being frustratingly slow, grants very little flexibility and decision making authority to the management or business unit level. Additionally, special provisions like veterans hiring preferences, while certainly a social priority for the nation, substantially limit the diversity of skills and experiences for incoming employees, particularly in national security agencies. DHA gives managers more say in shaping the workforce they need and is particularly useful where highly skilled technical competencies are needed.

DHA has been used in government for decades in federal scientific research and medical positions as well as the acquisitions profession. More recently it has also been employed to hire cybersecurity professionals. OPM can grant DHA to an agency but rarely does because an agency must show "scarcity" in a particular skill set, and the likelihood of success is perceived as low. In most cases, DHA is granted on a temporary basis and then lapses after an agency addresses the scarcity problem.

DHA offers a potential tool to close the gap between the public and private sectors, particularly in information technology project management. It would be difficult to argue against almost any federal agency's claim of having a "severe shortage" or "critical need" for more contemporary skills and qualifications in information technology. DHA, coupled with term appointments, provides an outstanding vehicle to bring in top talent and should be extensively incorporated into the defense acquisition workforce's human capital management plan.

Use the Senior Executive Service (SES) as originally intended. Broaden their development, exposure, agility, and reach by rotating personnel between agencies. Agencies would benefit from new and innovative ideas from outside traditional stove pipes and could better compete for top talent within the SES corps. As Ron Sanders wrote in The Federal Times, "… executive mobility remains one of the most important elements of the SES's original vision, and one of its biggest disappointments. With only a few exceptions—the U.S. Intelligence Community's civilian 'joint duty' requirement for one—the SES corps remains organizationally and functionally stove-piped."[5]

Increase opportunities for peer-to-peer exchanges among government and industry professionals. Such an initiative should include relaxing onerous restrictions on attending professional conferences, particularly for personnel in fast moving and highly technical acquisitions and project management professions. While there are some nominal cost savings with the current approach, it contributes to a lack of transparency that adversely impacts the federal government's ability to retain top young talent, particularly in emerging technologies. Conferences play an important role in the innovation ecosystem, and facilitating peer-to-peer interaction is important to retaining leading technology professionals.

In April of this year, DOD announced it would take steps to better leverage its 20-year old Corporate Fellows program.[6] Under this program, 15 to 20 senior military officers are embedded in commercial companies "who have earned a reputation for insightful long-range planning, organizational and management innovation, and implementation of new information and other technologies." According to the Corporate Fellows website, fellows "have been assigned to such diverse and innovative businesses as: Amgen, Boeing, CNN, Caterpillar, Cisco, Citicorp, DuPont, FedEx, General Dynamics, Honeywell, Hewlett-Packard, IBM, Lockheed Martin, McKinsey, Merck, Microsoft, Northrop Grumman, Oracle, Pfizer, Raytheon, Sears, Southern Company, Sun, 3M, United Technologies, and more."[7]

Defense Secretary Carter unveiled the new approach during a trip to Silicon Valley, stating, "Right now we don't effectively harness what they've learned when they come back … so we're going to try expanding that fellows program into a two-year gig—one year in a company and one year in a part of DoD with comparable business practices." He added, "That way, we have a better chance to bring the private sector's best practices back into the department."[8]

Unfortunately, the current list of sponsoring companies is heavily biased toward large, established companies, many of which are already traditional players in the defense industrial base. In order to leverage the program to build cultural understanding and break down barriers with emerging technology companies, DOD must seek out new partnership opportunities for its Corporate Fellows within this sector.

Expand unique models of attracting and deploying top technical talent to the federal government like the U.S. Digital Service (USDS), the General Service Administration's "18F" Program, and the Presidential Innovation Fellows. USDS and 18F were created in the wake of healthcare.gov's disastrous deployment and use term appointments to attract top private sector talent for challenging and high visibility "business to consumer" information technology projects across the federal enterprise.[9] The model involves deploying teams of USDS and 18F workers to specific agencies to assist with IT project management using the latest techniques from the private sector. While still in its infancy, USDS and 18F offer a promising model that can be implemented within existing federal authorities and is worth exploring at a larger scale in the national security enterprise.

Modeled after the White House Fellows program, the Presidential Innovation Fellows program pairs talented young technologists and innovators with top civil servants at the highest levels of the federal government with the goal of more effectively leveraging technology to serve the public. While this program by its nature is intended to be small and highly selective, it affords an opportunity to increase transparency and collaboration between top technologists and senior government officials.

DOD also announced it was establishing a USDS branch that will initially focus on improvements in electronic health record management. It remains to be seen whether programs like USDS, 18F, and the Presidential Innovation Fellows are sustainable in the long-term. However, in the near-term, they offer a mechanism for promoting change and innovation within the framework of existing authorities. Absent some of the broader reforms discussed previously, these programs offer some promise in the near-term.

Acquisition and contracting recommendations:

<u>Focus greater resources and flexibility in transitioning emergent commercial technologies to operational applications, including by establishing a DOD strategic investment arm based on the intelligence community's In-Q-Tel model.</u> Most small companies simply do not have the resources to survive the transition from early stage prototyping to program of record. Agencies like DARPA have a strong reputation for identifying high risk, potentially game-changing technologies and leveraging the knowledge and innovation in non-traditional companies to test it. Unfortunately, the transition rate for these technologies is very low, in part because of the inherent risk associated with the technology itself and also because of the cumbersome acquisitions process and difficulty matching the technology with a program "sponsor." DARPA will continue to be the "gold standard" for high-risk innovation in defense, but new models are needed to improve technology transfer of leading edge but perhaps lower-risk technologies on the cusp of commercial adoption.

One highly regarded model within Silicon Valley is In-Q-Tel, the IC's not-for-profit investment arm. Launched in 1999, In-Q-Tel was "created to bridge the gap between technology needs of the U.S. Intelligence Community and emerging commercial innovation."[10] The group invests in innovative, venture-backed startups capable of providing what it calls "ready-soon innovation" (i.e. technology that could be fielded within 36 months) vital to the IC mission. The vast majority of In-Q-Tel investments are in companies that have no record of doing business with the government.

Unlike the higher-risk research model of DARPA, In-Q-Tel only invests when an identified "sponsor" or "end user" has been identified in the IC to deploy the technology. In-Q-Tel invests side by side with the venture capital community, leveraging "outside funding to help develop sustainable technologies using off-the-shelf products instead of custom-built solutions."[11] In-Q-Tel is what the private sector would consider a "strategic investor," focused on accelerating product development in a particular direction and adding "mission-critical capabilities" necessary for the IC's applications. In-Q-Tel can be quite attractive for startups because unlike other venture funding it is "non-dilutive" capital, meaning In-Q-Tel takes no ownership stake in the company.

To establish its own investment arm, DOD will require special legislation and unique human capital. Effective strategic investment requires extensive experience in emerging technologies and venture capital practices, and it is unlikely these people can be found or trained organically within DOD or any other agency.

On April 23, 2015, Defense Secretary Carter announced a pilot project with In-Q-Tel to find innovative solutions to some of the Department's most challenging problems, stating DOD "will make a small investment with In-Q-Tel to leverage the nonprofit's proven relationships and apply its approach to DoD."[12] Partnering with In-Q-Tel on a pilot project is an outstanding first step and should help generate the knowledge and experience needed to establish a pure-defense strategic investment arm in the future.

If implemented effectively, the scale and resources DOD brings to the table would make it a larger player than In-Q-Tel within the emerging technology sector and provide much needed presence and transparency in places like Silicon Valley. It would also send a strong strategic signal both inside and outside DOD that new models are needed to better engage emerging technologies. Like In-Q-Tel, DOD could establish strong presence on the ground in Silicon Valley, with the goal of interfacing with companies interested in doing business in defense. Finally, operating such an investment arm would generate significant knowledge and best practices that could be incorporated across the broader acquisitions enterprise to incentivize new entrants.

The principal challenge here will be transferring the technology to achieve scale. DOD must demonstrate that entrepreneurs can be successful in such a model even if their technology potentially impacts or destabilizes an existing or emerging program of record.

<u>Expand the use of "other transaction" (OT) authority within the Department of Defense.</u> OT authority offers a highly flexible business tool not strictly governed by the Federal Acquisition Regulations (FAR) and is generally limited to smaller prototyping and research applications.

That said, the Department has the authority to execute an OT up to $100 million with appropriate senior leadership approvals.

OTs inject agility and flexibility into the acquisitions system and significantly lower barriers to entry for smaller non-traditional companies looking to break into defense applications. The use of OT authority generally requires at least one non-traditional defense contractor to participate in the project and is intended to incentivize their participation. The contractor benefits from a simplified business transaction, as does the acquirer, who also garners whatever unique technical benefits the non-traditional participant brings to the table.

OTs also offer the ability for DOD and the contractor to negotiate whatever terms they want (simple or otherwise). Such an approach is consistent with the general practice in emerging software markets, where flexible terms facilitate more fluid partnerships between customer and supplier. This is particularly important because challenges are often not well-understood initially and will almost certainly evolve over time, as will the particular technological approaches used to address them.

OTs offer a proven vehicle to attract non-traditionals and have been used effectively by innovative organizations like DARPA and NASA for decades. Unfortunately, their use is not widespread across DOD, and there are limits on the size and extent of their application. There is also significant stigma attached to the broader adoption of OTs due to their association with the failed Army Future Combat Systems project and the resulting congressional scrutiny.[13] Within the heavily rules-based, compliance-focused and risk-averse acquisitions system, significant cultural barriers hinder more widespread adoption of OTs in defense, particularly when a cadre of traditional suppliers may be readily available to conform to the mainstream system.

Representative Thornberry's proposal to make OT authority permanent for DOD may help incentivize its broader use by providing a clear signal from Congress as to its inherent value. However, Representative Thornberry also proposes to generally limit the use of OT authority to small business or non-traditional defense contractors. This seemingly innocuous provision will limit innovative cost sharing, partnering, and consortium building between small businesses and established system integrators and should be stricken from the bill.

Establish an OT-based cyber and IT "fast track." A fast track option that utilizes existing OT authorities and establishes a standard, simplified transaction vehicle designed to attract and incentivize non-traditional contractors to submit proposals for R&D and prototyping projects should allow companies to keep their intellectual property and would commit the government to executing selected transactions quickly, say within 45 days of receiving proposals. Such a mechanism would help advance a posture of speed, aggressive prototyping, and measured risk-taking within DOD while also attracting new businesses to the market.

One promising model is the U.S. Air Force's PlugFest PLUS program, a targeted effort to use an industry best practice (i.e. the plugfest) and an innovative OT arrangement to accelerate IT acquisitions and attract non-traditional companies. Plugfests are used in the private sector to validate and verify open system interoperability inside a specific enterprise. In other words, "participating vendors 'plug' their off-the-shelf hardware and/or software into a standards-based, instrumented, technology 'Plug Test' harness."[14] The Air Force's program allows participating companies to demonstrate their capability and prove interoperability with an existing information system.

The contract vehicle is an open consortium under OT authority, and successful PlugFest PLUS participants may be automatically deemed consortium members, potentially obviating the need for a white paper or formal proposal that typically accompanies an OT arrangement. According to the Air Force, this approach allows awards to be "made in a matter of weeks following PlugFest Plus events."[15] The Air Force is still in the early stages of implementing this program, but the construct is based on an existing industry best practice and fully leverages one of the most flexible contracting vehicles within the Department of Defense.

Plugfests are inherently less attractive if the interoperability standard is measured against a specialized and insular DOD system architecture baseline. Using such a baseline will inherently limit the breadth and depth of the participating technology ecosystem.

Sustain and expand efforts like the DOD's Innovation Outreach program within the Rapid Reaction Technology Office. This program's stated goal is to identify innovative technologies from non-traditional suppliers and connect them with government "sponsors" in need of technological solutions across the defense and broader national security enterprise. Innovation Outreach provides a conduit to connect the keepers of defense problems with innovative problem solvers.

Technology transfer rates are still low, with approximately 10 percent of companies that present to sponsors being funded for technological experimentation and prototyping and an even smaller percentage going forward for operational deployment. However, Innovation Outreach is one of few programs in government specifically focused on matching non-traditional companies to sponsors, and helping them through the process.

Promote the use of agile software development in the federal government by more effectively leveraging existing flexibilities in the Federal Acquisition Regulations (FAR). Federal IT projects are often executed using outdated development practices and narrow interpretations of acquisition regulations, practices that contribute to high rates of failure. Utilizing modern software development techniques will make the government a more attractive customer for leading edge technology firms, some of which cited the government's outdated requirements generation and project management process for software solutions as a significant barrier to entry.

The recently published "Digital Services Playbook"[16] and "TechFAR,"[17] innovative products from the newly formed U.S. Digital Service, identify best private sector practices for delivering digital services and highlight existing flexibilities in the FAR to help agencies implement them. The "TechFAR" specifically focuses on utilizing agile software development, "a technique for doing modular contracting and a proven commercial methodology that is characterized by incremental and iterative processes where releases are produced in close collaboration with the customer. This process improves investment manageability, lowers risk of project failure, shortens the time to realize value, and allows agencies to better adapt to changing needs."[18] Acquisitions personnel should be trained on how to best leverage these existing flexibilities within the FAR and be incentivized to implement these more innovative contracting methods.

Purchase commercial goods to the greatest extent possible, acknowledging not just the streamlined acquisition procedures associated with this approach but also the associated benefits of supplier diversification. Over-specialization with defense-specific requirements not only slows the acquisitions process but also discourages participation from non-traditional contractors who have an incentive to preserve platform uniformity to support efficient sales in both government and commercial markets.

Promote the use of open source, cloud-based software frameworks that are commonly used in the private sector to deliver similar services. Widely adopted open source platforms encourage a broad base of potential suppliers and avoid the "vendor lock-in" that can occur with some proprietary solutions. This approach can help transition government toward smaller, more modular–purchasing practices being widely adopted in the private sector (e.g. "software as a service"). The idea is to put resources and purchasing authorities in the hands of business unit leaders who can use operating funds, vice capital expenditures, to purchase cloud-based software services. Once lines of businesses figure out which solutions work best, then organizations can look toward gradual, iterative standardization. There are risks and drawbacks to this approach, but they are modest in comparison to the cost, schedule, and performance risks associated with the complex practice of pursuing enterprise-wide, proprietary IT solutions.

Increase opportunities to bias the government toward smaller, more innovative technology companies. While a host of "set-aside" preferences (e.g. 8A preferences) already exist within the federal government's procurement system, new incentives are needed to make it easier for non-traditional technology companies to enter, particularly where missions demand cutting-edge solutions. The Obama Administration has explored an "Innovation Set-Aside" program that would give agencies the authority to consider a small number of sole-source contracts for demonstrated innovative technological solutions.

Such a program should be tested in DOD, and targeted companies should be below a certain size threshold (e.g. 300 employees), have never done business with the government before, and operate in specific mission-critical sectors like cybersecurity. To temper political opposition to new preferences, authorities for such a program could be granted on a temporary basis to allow for testing and evaluating.

Develop a strategy to increase transparency and visibility of technology challenges and opportunities within the defense enterprise, with specific focus on communicating to non-traditional companies. New ideas and mechanisms are needed to market defense enterprise problems to smaller, more agile problem solvers in the nation's broader emerging technology community. Traditional information conduits like fedbizopps.gov will continue to reach primarily traditional contractors because they are most familiar and comfortable with navigating existing systems, and doing so is part of their core business. The strategy must be flexible and iterative, and a number of potential conduits must be tested and measured, including sustained personal engagement from the Pentagon's most senior leadership.

Initial steps for developing a new marketing and communications strategy:

Enlist the U.S. Digital Service to aid in the development of a modern, user-friendly website to communicate the most exciting, fastest moving, and innovative solicitations in which non-traditional contractor engagement is most desirable and most likely to be successful. Such a website would not have to replace fedbizzopps.gov but rather complement it. DARPA implements a similar practice by carrying short, hard-hitting, simplified solicitation descriptions on its website, with a disclaimer that gives precedence to fedbizopps.gov as the "official" point of entry for government procurement opportunities.

Expand defense-sponsored government challenges to include smaller, micro-challenges with lower barriers to entry, particularly in software and information technology, and promote them using a similarly innovative website as outlined above. These challenges could be specifically targeted toward smaller, more agile companies instead of larger corporations or university consortiums. One CEO commented, "The prize could be a medal instead of cash and would be cheaper and work just as well." Such micro-challenges would lower barriers to entry not just among potential competitors but the prize sponsors as well, including simple data analytics problems or questions that could easily be posted online with the associated data.

Better leverage Federal Advisory Committees like the Defense Science Board and Defense Business Board to advise on mechanisms to reach and attract non-traditional contractors. As a first step, committee membership should be diversified to ensure stronger representation from experienced early stage technology company executives and venture capitalists. In the case of the Defense Business Board, such diversification would require changing the committee's charter, as it currently limits members to those with "a proven track record of sound judgment in leading or governing large, complex private sector corporations or organizations …"[19] A more aggressive alternative would create a stand-alone advisory committee with a unique charter to focus exclusively on breaking down barriers for early stage technology companies. Such a move would help signal the Department's commitment to the effort.

Reinvigorate defense participation and representation at leading technology conferences. Among other things, this will require lowering approval thresholds and funding authorizations to the lowest level possible, particularly in innovative programs where contemporary engagement with the private sector is vital to sustaining relationships and currency in the field.

Defense Secretary Carter recently announced the creation of an "experimental Silicon Valley partnership called the Defense Innovation Unit, or DIUX" to "scout emerging and breakthrough technologies and build direct relationships to DOD." The unit would be staffed by active duty military personnel as well as reservists who live and work in the Silicon Valley area.[20] While few DIUX details are available, establishing DOD presence in Silicon Valley is a step in the right direction. Most critical will be equipping such an entity with the talent and processes needed to not only identify "breakthrough" technologies but follow through with a mechanism to leverage them in a manner that is mutually beneficial to both the government and the companies in question.

Finally, retire the term non-traditional contractors, and replace it with one that better reflects innovation imperatives. Regardless of size, companies that do not have a history of doing business with the federal government are referred to in acquisitions parlance as non-traditional contractors. Emerging technology companies in places like Silicon Valley would fall into this category, as would in fact the majority of companies in the United States.

Non-traditionals can be afforded special contracting consideration to incentivize their participation, including the OT authority previously mentioned. However, there are few incentives for acquisition professionals to seek out non-traditional participants, particularly when there are traditional suppliers ready and available to conform to the mainstream system.

The system and terminology reinforce an unfortunate dichotomy: it is easy to associate special or negative traits with the term non-traditional while at the same time placing inherent value on traditional or conformist acquisition architectures.

Also, the term non-traditional makes little sense outside the context of government procurement. To illustrate this point, consider the president's proposed FY 2016 defense budget, which calls for approximately $180 billion in spending on procurement and R&D. While certainly not an apples to apples comparison, consider this in the context of the United States' $17 trillion GDP. Does it really make sense to refer to the other $16.82 trillion of the U.S. economy as non-traditional?

Finally, consider the nature of the words themselves. Merriam Webster defines non-traditional as "not bound by traditional ways or beliefs," with synonyms like "broad-minded, non-conventional, non-orthodox, open-minded, progressive, radical and unconventional," and antonyms such as "conservative, conventional, hidebound, non-progressive, old-fashioned, orthodox, stodgy, and traditional."[21] Which terminology would you prefer if your goal is an agile and innovative defense industrial base?

Perhaps it is time to modernize both the term itself as well as the mindset associated with it in the culture of the acquisitions bureaucracy. When Pentagon leadership speaks of attracting more non-traditionals, they are referring to smaller, more agile, more innovative companies like those in the emerging U.S. technology sector. The term should have a positive connotation and reflect the attributes and benefits the system hopes to achieve through engaging with this type of contractor. Some terms suggested during the course of this research to replace "non-traditional" include: advanced, leading edge, next generation, 21st century, agile, or emerging contractors.

Notes

[1] "Building the Enterprise: A New Civil Service Framework," Partnership for Public Service and Booz Allen Hamilton, April 2014, http://ourpublicservice.org/publications/viewcontentdetails.php?id=18, accessed April 2015.

[2] "Report of the Military Compensation and Retirement Modernization Commission," January 29, 2015, http://www.mcrmc.gov/public/docs/report/MCRMC-FinalReport-29JAN15-LO.pdf, accessed April 2015.

[3] Jonathan Rothwell, José Lobo, Deborah Strumsky, et al, "Patenting Prosperity: Invention and Economic Performance in the United States and its Metropolitan Areas," The Brookings Institution, February 2013, http://www.brookings.edu/~/media/research/files/reports/2013/02/patenting-prosperity-rothwell/patenting-prosperity-rothwell.pdf, accessed April 2015.

[4] "Hiring Authorities," United States Office of Personnel Management, http://www.opm.gov/policy-data-oversight/hiring-authorities/direct-hire-authority/#url=Fact-Sheet, accessed April 2015.

[5] Ron Sanders, "Back to the future: A blueprint for 'modernizing' the SES," *Federal Times*, December 3, 2014, http://www.federaltimes.com/story/government/management/blog/2014/12/03/back-to-the-future-a-blueprint-for-modernizing-the-ses/19842535/, accessed April 2015.

[6] Cheryl Pellerin, "Carter Seeks Tech-sector Partnerships for Innovation," *DoD News*, United States Department of Defense, April 23, 2015, http://www.defense.gov/news/newsarticle.aspx?id=128655, accessed April 2015.

[7] Office of the Deputy Chief Management Office, "Secretary of Defense Corporate Fellows Program," United States Department of Defense, http://dcmo.defense.gov/corporate-fellows-program/index.html, accessed April 2015.

[8] Pellerin.

[9] The U.S. Digital Service, "The Story Of The U.S. Digital Service," The White House, https://www.whitehouse.gov/digital/united-states-digital-service/story, accessed April 2015.

[10] In-Q-Tel, "About In-Q-Tel," https://www.iqt.org/about-iqt/, accessed April 2015.

[11] Ibid.

[12] Pellerin.

[13] Bill Greenwalt, "Built Fast, Effective Acquisition: Avoid The System We've Got," *Breaking Defense*, April 25, 2014, http://breakingdefense.com/2014/04/build-fast-effective-acquisition-avoid-the-system-weve-got/, accessed April 2015.

[14] The Association for Enterprise Information, "What is PlugFestPLUS," http://www.afei.org/events/5A09/Pages/What.aspx, accessed April 2015.

[15] Ibid.

[16] The United States Digital Service, "U.S. Digital Services Playbook," https://playbook.cio.gov/#play1, accessed April 2015.

[17] Office of Science and Technology Policy, "The TechFAR Handbook for Procuring Digital Services Using Agile Processes," Executive Office of the President of the United States, https://github.com/WhiteHouse/playbook/blob/gh-pages/_includes/techfar-online.md, accessed April 2015.

[18] Ibid.

[19] Defense Business Board, "The Charter, Defense Business Board," United States Department of Defense, July 3, 2014, http://dbb.defense.gov/Charter.aspx, accessed April 2015.

[20] Pellerin.

[21] Merriam Webster, "nontraditional," thesaurus, http://www.merriam-webster.com/thesaurus/nontraditional, accessed April 2015.

CONCLUSION

Clearly there is no silver bullet when it comes to diversifying the MIC with new entrants from places like Silicon Valley. The MIC will never be disrupted in the early 21st century sense of the term, as a significant inventory of purely public defense goods will almost certainly be needed for the foreseeable future, as will the defense industrial base that can build them. There will always be a core base of consolidated defense companies with limited ability or incentive to diversify to other commercial markets.

That said, the boundaries between traditional public goods and private goods in defense will continue to blur, particularly as technologies like drones, advanced robotics, artificial intelligence, and cyber weapons continue to penetrate deeper into global society. Today, Silicon Valley startups are pursuing technologies like nanosatellite networks for global ship tracking, as well as a privately financed, engineered, and deployed replacement for GPS. Once almost exclusively the domain of public investments, there is a growing commercial market for these and other technologies and associated capital and private sector innovation to pursue it.

The pace and scale of globalization and commercialization make it more difficult than ever before to predict the next game-changing technology in defense, making it imperative that the MIC fully leverage the strength and depth of the rapidly evolving U.S. technology sector, particularly in places like Silicon Valley, the world's leading ecosystem for technological innovation.

Without question, the current MIC remains heavily consolidated—with traditional prime contractors having little diversification into other commercial markets, and R&D investment rates well below those of other advanced industries. Additionally, the current culture and framework for defense acquisitions favors larger, traditional contractors, creating a self-reinforcing dynamic that favors the status quo. While current Pentagon and congressional leadership have all expressed a strong desire to increase competition, diversity, and innovation within the MIC, it is still widely perceived as incompatible with smaller, more agile, and more diversified non-traditional companies.

With a specific focus on the perspective from executives leading early stage Silicon Valley technology companies and venture capitalists that invest in this space, this research shows barriers to entry into the defense industrial base are formidable, if not prohibitive, particularly relative to other technology markets. These barriers significantly limit the government's access to top human capital, innovative intellectual property, and potentially disruptive technologies emerging in other segments of the economy. The source of these barriers is nuanced and is not based on any particular security or political ideology but rather a commitment to making business decisions that facilitate the speed and growth necessary to survive in technology markets.

In fact, the majority of technology executives and venture capitalists interviewed had a general willingness and even a strong desire to do business with the federal government on matters of national security. In some cases global commercial markets are larger and more liquid, but defense still brings significant capital to the game, and this is attractive to any entrepreneur. Moreover, these are executives and technologists who like to solve tough problems, and there are plenty of tough, interesting, and meaningful problems to be solved in defense.

However, the vast majority of these executives also could not envision a viable scenario in which doing business in defense, or the rest of the federal government for that matter, made sense commercially. The DOD is simply perceived as a bad customer, one that is skewed in favor of larger, traditional players. These traditional "primes" have the expertise to navigate a very complex and opaque acquisitions system as well as the resources to wait out the long and highly uncertain sales cycles.

Unfortunately, some will never enter the defense market, especially when any association with the national security enterprise fundamentally threatens their customer trust. When your business model depends on customers trusting your technology, your cloud, your security, anything that might erode that is an existential threat. In these markets the cost of eroding customer trust far outweighs any possible benefit from defense revenue. It is possible this dynamic could change in the future, but there is no sign of it in the near-term.

For most others, particularly early stage companies, the Snowden disclosures are a red herring. Most of these companies do not discriminate among customers ideologically and are instead focused on making the best decisions to grow their business. For these companies, the biggest barriers to doing business in defense have nothing to do with Snowden and everything to do with the difficulty of the process and fundamental differences between the defense market and competing commercial markets.

This research suggests any ideological opposition in Silicon Valley regarding business in defense is significantly overstated: what matters is the ability to grow their business. In other words, they are willing to engage provided they can do business in a manner that does not significantly slow them down and doesn't compromise the integrity of the platform or product they are trying to sell commercially. Sadly, most executives and venture capitalists interviewed just don't see any way for them to "win" in the current system.

It is also important not to overstate the potential impact of early stage Silicon Valley companies on innovation in the MIC. Large, highly complex "pure defense" platforms requiring system integration should not be awarded to an early stage technology firm, and they never will be. However, perhaps one of its payloads or software systems can be, and it will provide the agile technology refresh needed to ensure its continued technological superiority going forward.

Beyond major platforms, information technology systems as well as smaller-scale hardware platforms (e.g. drones, robotics) will continue to play a larger role in both defense operations and its formidable logistics and management tail. This environment is ripe for disruptive innovation, particularly as the private sector moves swiftly into emerging global markets fueled by strong capital investment and research and development. In addition, the speed and complexity of the cybersecurity threat demands faster prototyping, acquisitions, and system deployment, traits that are consistent with the "fail fast, fail often" culture in emerging commercial technology markets.

Early stage Silicon Valley technology companies are well positioned to make significant national security contributions provided the culture and framework of the current acquisition system can adjust to accommodate them. Failing to fully leverage the most innovative and far reaching segments of the U.S. economy will threaten our national security in the long-term. In the Information Age, the pace of global technological progression is governed by Moore's Law, not the Federal Acquisition Regulations, and failing to keep up will ultimately cost lives, treasure, and global influence.

The fundamental question is, in adding layer after layer of regulation, oversight, and reporting requirements to foster fair competition and mitigate cost, schedule and performance risk, have we actually increased our risk by distorting the rules of the game such that the rest of the economy won't even play? Veteran Silicon Valley CEO Tom Lounibos summed it up this way, "Despite all the processes that government has in procurement, they probably incur the same risk we do, except we do 'fast fail,' and they do 'long process and slow fail,' and it costs them more in the end in every respect."

In summary, the bad news is that the challenge of attracting new entrants from Silicon Valley is larger than most policy makers in Washington realize. The good news is that the potential opportunities for defense innovation are just as large if progress can be made. Non-traditional entrants will bring a whole ecosystem of other non-traditional suppliers with new ideas and technologies.

The other piece of good news is that there appears to be momentum for change at the highest levels of Pentagon and congressional leadership. However, there is little in either branch's approach to suggest sufficient change to overcome the strong system bias against non-traditional companies. Defense Secretary Carter's recent visit to Silicon Valley was a step in the right direction, as was his announcement of a number of prototype initiatives to increase engagement and collaboration between DOD and emerging technology companies. Much more will be needed on this front, and chapter six offered a wide range of policy recommendations in a number of different areas, including significant civil service reforms to address fundamental cultural barriers.

Chapter six also offered a number of policy recommendations related to contracting and acquisitions, with several specific recommendations and best practices that should be adopted more broadly. The size and complexity of the defense acquisitions process make wholesale system rewrites and overhauls both politically difficult and functionally fraught with risk. Smaller, more iterative changes make more sense to allow for experimentation, appropriate feedback, and adjustment, and a number of recommendations are offered on this front.

DOD is not unique in the federal government when it comes to having difficulty attracting non-traditional companies. In fact, one could argue that DOD's vast science and technology enterprise give it more interaction and engagement with smaller technology companies than any other agency. DOD is therefore well positioned to lead the rest of government toward enhanced competition and increased innovation, traits sorely needed across much of the federal procurement enterprise.

At the end of the day, the defense acquisition system must adapt to better balance the need for oversight with the need to transform the military into what Representative Thornberry calls "the world's fastest incorporator" of new technology.

What if we can't change the system?

As mentioned in chapter one, the success of the second offset depended largely on the nation's underlying industrial, economic, and academic superiority relative to the rest of the world and the MIC's ability to effectively leverage it. In the current globalized economy, the U.S. advantage on these fronts will inevitably be less pronounced. Globalization and commercialization will continue to drive the pace and direction of new technologies. Absent change, the outdated defense acquisition system risks becoming even further displaced from the commercial norm, as does the defense industrial base that operates within it.

Some of the changes suggested in this report are really, really hard. If they were easy, acquisition reform would not be a perennial topic in Washington, D.C. policy circles. It is therefore vital to hedge against the risk of being unable to change. The best way to do this is to ensure the United States continues to have the world's most innovative economy. Without this foundational element of national security, any discussion of sustaining technological superiority on the battlefield is folly.

ABOUT THE AUTHOR

Commander Jason Tama is a United States Coast Guard officer with 20 years of experience in a broad array of operational and staff assignments. He most recently served at Coast Guard Sector San Francisco where his engagement with emerging technology companies provided the inspiration for this project.

Commander Tama holds a bachelor of science in mechanical engineering from the United States Coast Guard Academy, a master of science in naval architecture and offshore engineering from the University of California, Berkeley, and a master of business administration from the MIT Sloan School of Management. He was also a Marshall Memorial Fellow.