AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

BREAKING BAD:

REFORMING CYBER ACQUISITION VIA INNOVATIVE STRATEGIES

by

Matthew P. Flahive, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisor: Wg Cdr Graem M. Corfield, RAF

Maxwell Air Force Base, Alabama

April 2015

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Abstract

The acquisition of offensive cyber operations tools presents unique challenges and opportunities. For the development of cyber programs, the traditionally slow pace and high costs of Department of Defense acquisition can be improved upon via the implementation of innovative acquisition strategies. Within the current acquisition framework, techniques such as embedded certification teams, utilization of national laboratories, omnibus contracts and support contract vehicles can all be tailored to improve the process. Looking outside the current acquisition framework and organizational culture, cyber tools could be developed and acquired via crowdsourcing, outsourcing, fly-offs, and public-private partnerships. Analyses of these eight innovative techniques demonstrate that legitimate options to rapidly develop and acquire effective offensive cyber operations programs not only exist, but they are within reach today. By convincing the acquisition institution to further adapt its processes, and by mitigating certain security risks associated with these techniques, the acquisition community can leverage these innovative strategies to revolutionize cyber development for the Department of Defense.

Chapter 1

Introduction

"We will protect our investment in foundational capabilities like the nuclear deterrent, and we will grow our investment in crucial capabilities like cyber; space; and intelligence, surveillance, and reconnaissance."[1]

National Security Strategy, 2015

Problem Statement

The Department of Defense (DoD) requires the development and delivery of cyber programs at a speed and price that, to date, has been unfeasible through the current acquisition framework. The current acquisition system and culture are suboptimal for the needs of cyber programs. Costs spiral out of control due to requirements creep on lengthy projects that do not deliver quickly enough to be effective. Performance and schedule are unquestionably linked, and both falter because lengthy acquisition procedures result in delivered products being generations behind the latest technological advances. The DoD's acquisition system was not intended to be as responsive as is required for cyber systems; the system must be adapted to protect national interests.

An examination of today's acquisition methodology uncovers creative methods within the framework that can potentially improve the development and procurement of systems for offensive cyber operations. Furthermore, by understanding today's acquisition methods, it is suggested that one can identify innovative approaches outside the framework that can advance the DoD's offensive cyber operation capabilities.

Significance

For fiscal year 2015 (FY15), the DoD projects to spend nearly $5 billion across the spectrum of cyber operations, which equates to roughly 1% of the DoD's total budget. Exact dollars for each cyber sector are obscured due to security classifications, so the ratio of funds spent on offensive cyber operations as compared to the other sectors cannot be defined with absolute certainty.[2] Nevertheless, the significance of cyber programs within the DoD cannot be discounted given the multi-billion dollar annual budget. The cyber budget is certain to grow as the DoD, as well as the entire United States Government (USG), expands its dependence on cyber activities and formalizes its cyber strategies for wartime. Proper management of funding is crucial to realize the best "bang for the buck," and therefore acquisition strategies must be optimized for the intricacies of the cyber domain, to include opportunities afforded within the cyber domain that are simply not available to the land, sea, air, and space domains.

Similarly, the speed at which the DoD can acquire cyber systems using the current acquisition framework is inadequate. According to a 2009 report from the Office of the Assistant Secretary of Defense for Networks and Information Integration, cyber programs developed under the current acquisition framework take an average of 91 months to achieve initial operating capability.[3] Given the rapid advances within the cyber domain, 91 months to field a system is entirely too long. Programs developed by this framework and culture are technologically obsolete before they can be deployed. The DoD acquisition community must alter its approach, attempting innovative strategies and accepting risk, to deliver relevant cyber programs.

Scope

The scope of this paper will focus on the development and acquisition of offensive cyber operation programs by the USG. Cyber operations, also referred to as cyberspace operations,

include all defensive and offensive actions taken to achieve objectives either within or through the cyberspace domain. Defensive cyber operations mitigate vulnerabilities and counter threats either emanating from, or affecting, cyberspace assets. Offensive cyber operations can be described as "military operations and activities in cyberspace for cyber attack against and (or) cyber exploitation of adversary information systems and networks."[4]

The majority of cyber programs acquired by the USG are either defensive in nature, or they relate to infrastructure programs. Acquisition strategies for defensive tools, such as firewalls and antivirus software, will differ from acquisition strategies for infrastructure programs, such as network hardware and the DoD Enterprise Portal System. Along that same vein, acquisition strategies for offensive cyber operations can take an entirely different approach due to the nature of the mission. Some of the innovative techniques to be discussed within this paper could be leveraged for defensive tools and for infrastructure programs, but it would be presumptuous to assume that strategies designed for the intricacies of offensive cyber operations would automatically translate to the complexities of defensive tools or for infrastructure programs. Therefore, the scope of this paper will focus solely on offensive cyber operations, to address the concerns and offer solutions for this specific mission set.

Chapter 2

Current Framework for Government Acquisition of Cyber Programs

"A problem two years ago is not a problem today, and what's a problem today we couldn't have imagined two years ago. So, anything that will help us build resiliency and get the compliance part of the system to be much quicker would be very helpful."[5]

William A. LaPlante, 2014

Offensive cyber operation tools can indeed be developed and acquired using the current DoD acquisition framework and culture, though the process is far from efficient within the cyber domain. In 2015, the acquisition of programs occurs by leveraging the defense acquisition system, the requirements process, and the Planning, Programming, Budgeting, and Executing (PPBE) process. Before determining whether streamlining these processes could be beneficial for the DoD, it is prudent to understand how each system and process operates today. This paper intentionally will not go into great detail for these processes, but will rather focus on providing a summarized overview of how these systems interoperate, to lay a foundation for potential improvements examined in the remainder of this paper.

Defense Acquisition System

The Defense Acquisition System derives from DoDD 5000.01. This directive defines the system as the process by which the DoD delivers systems to a user, with the intent of maximizing cost and schedule and performance. The system uses milestones and phases to keep a program moving along a defined path towards completion.[6]

A program office will first seek approval to enter the acquisition process by convincing senior acquisition executives that there is a requirement to develop a new system; this is done as part of the Materiel Development Decision and marks the start of the Materiel Solution Analysis phase, also referred to as "pre-Milestone A." Once the plan for the program is approved as part

of Milestone A by the Milestone Decision Authority (MDA), it enters the Technology Development phase. During this phase, the program office works to reduce technological risk and to determine technologies that should be incorporated into a full system, and finally demonstrates the technology with prototypes.

The effort, at this point, is steadily progressing towards Milestone B. Upon satisfying the MDA, the program is considered to be initiated. It now enters the Engineering and Manufacturing Development phase. This phase is for programs that have mature technology, approved requirements, and secured funding. During this period the system design will be integrated, and the system process as well as the manufacturing process will both be demonstrated. After successful demonstrations, the MDA will determine the program has achieved the requirements of Milestone C. This moment signifies that the DoD has committed to production.

The Production and Deployment Phase follows Milestone C. This phase is for systems that have been matured for production. During this time, low-rate production runs will be tested and then further developed to reach full-rate production along with deployment of the products. Initial Operational Capability will be achieved, and afterwards the program will flow into the Operations and Support phase. Within this final sustainment phase, which includes declaration of Full Operational Capability, is the end of the program through demilitarization and disposal activities.

This series of phases, milestones, program reviews and additional events eventually combines into a lengthy process. Officials intentionally slowed the process to prevent government funds from being wasted on immature programs or technologies. With regards to offensive cyber tools, however, this methodical approach would benefit from streamlining.

Requirements Process

Legislation signed in 2012 updated the procedures for identifying and vetting requirements for defense programs. The requirements process now includes models for accelerated acquisition programs as well as the rapid acquisition of urgent needs.[7] These adjustments open the door for acquisition professionals to optimize what is normally a very lengthy process for determining, approving, and pursuing requirements. What used to be a rule-focused requirements process now allows for an emphasis on process intent, and processes can be tailored to accept risk for more urgent delivery.

These improvements to the requirements process demonstrate that, within the current Federal Acquisition Regulation (FAR) framework, there exists potential to improve the vetting process for offensive cyber operational tools. Before claiming victory over an antiquated process, however, one must recognize that the defining and approving of requirements within the cyber domain becomes incredibly complex and highly-classified in tremendously short order. Though the process may be more flexible, the challenge of gaining buy-in from leaders lacking security access for technically-intricate fleeting opportunities does indeed create a bottleneck even within an improved requirements process.

PPBE Process

The other leg of the current acquisition framework is the Planning, Programming, Budgeting, and Execution (PPBE) process. The PPBE process enables the DoD to allocate and apply resources in the pursuit of a program.[8] The planning phase coordinates between Military Services and components to create an overarching strategy. The programming step builds the Program Objective Memorandum (POM), a time-phased allocation of funding in pursuit of a program. Budgeting is accomplished in conjunction with programming, as a Military Service

submits budget estimates alongside its POM. Execution spreads across multiple fiscal years, applying the funds that were programmed and budgeted in order to develop and deliver on the program that was planned for in the first phase.

Taken as a whole, the PPBE process establishes programmatic policies and strategies and goals, and then strives to achieve those goals within the limits of the federal funding available to the DoD. This process, however, spans many years and thus creates problems when programs must be completed rapidly. If the Military Service did not carve out enough funding for an emerging area during the PPBE process, then that Military Service will have great difficulty securing dollars to execute a development for the aforementioned emerging area.

Chapter 3

Acquisition Strategies Within the Current Framework

"We have to react instantaneously to many of the threats, we can't sit around and wait for a [Defense Acquisition Board] or a [Joint Requirements Oversight Council] for these things. We have to take it outside the conventional system for the major, long term weapons systems."[9]

Frank Kendall, 2012

The acquisition framework described in Chapter 2 of this paper reflects improvements over previous acquisition limitations. These improvements, along with some longstanding policies that offer flexibility, open the door for certain acquisition strategies that can be beneficial for the development of offensive cyber operational tools. Four methods merit investigation based on their potential to accelerate or enhance currently used methods: embedded certification and accreditation teams, national laboratories, omnibus development contracts, and support contract vehicles. This chapter will examine the benefits and limitations for these strategies, each of which exists wholly within the bounds of the defense acquisition framework in effect today.

Embedded Cybersecurity Management Teams

In 2014, the Department of Defense updated its cybersecurity requirements for programs, replacing the DoD Information Assurance Certification and Accreditation Process (DIACAP) with the framework used by the National Institute of Standards and Technology (NIST). The DoD now abides by cybersecurity guidance derived from NIST risk management framework.[10] This risk management framework, however, still presents schedule bottlenecks for cyber programs, according to information assurance engineer Maj Gary Thompson.[11] Improving the cybersecurity management process by embedding NIST teams throughout the acquisition process would accelerate the development of cyber operational tools.

Creating an organization that has carte blanche authority to implement a solution, from a NIST risk management framework perspective, would minimize the cybersecurity review process that hampers cyber programs. Fielding a team with empowered representatives from accrediting agencies, such as the National Security Agency and AFNet, would address NIST concerns in parallel with the development of cyber tools. When addressing a specific threat or vulnerability, this could minimize regression testing requirements. For threats and vulnerabilities associated with a known attack vector, such as a flaw in a firewall that will be addressed in a future revision, this accrediting organization can expedite otherwise time-consuming processes so that cyber tools can be verified and validated quickly.

The risk management framework, to include gathering appropriate artifacts, generally takes about six months; the aforementioned team could potentially award permission nearly immediately. Though certain offensive cyber operational tools may not fall under the purview of processes like the NIST risk management framework, this notion to embed approval teams within the development cycle could be replicated for other functions. The concept can ensure that rapidly-acquired tools are unhampered by lengthy approval processes, because those approval processes occur throughout the lifetime of the tool's development instead of being added-on at the end of the process. The major drawback to this concept is institutional pushback from accrediting agencies, which may be less than eager to bypass their hierarchical processes by empowering their embedded representatives. By tackling the micromanaging culture of these institutions, significant schedule gains will be realized.

National Laboratories

The Department of Energy and the Department of Defense currently employ multiple national laboratories to provide technical expertise for nuclear capabilities and other, primarily

energy-focused, scientific domains. Sandia, Lawrence Livermore, and Los Alamos are three national laboratories devoted to working on nuclear concepts for the benefit of the national will. These laboratories, as pointed out by Capt Patrick Roberts, also perform software development for the Air Force Technical Application Center (AFTAC).[12] Utilizing the brainpower and expertise held within these national laboratories would provide vast benefits, namely the organic development of offensive cyber operational tools.

AFTAC, as well as other organizations within the DoD, send funding to national laboratories every year via the Military Interdepartmental Purchase Request (MIPR) process. The MIPR process does not require any bidding by companies, or competitions between developers. Rather, a DoD official only needs to justify the requirement for laboratory support (or from a Federally Funded Research and Development Company, also known as an FFRDC) in a document signed by the appropriately-empowered authority within the official's chain of command. This method makes the process of using a MIPR to fund development into a fairly painless and rapid endeavor, so long as the DoD official properly manages the project.

FFRDCs and national laboratories do a remarkable amount of work for the DoD today, and though lately the scrutiny on these institutions and the MIPR process has increased, this method would provide a program manager with a highly-skilled team in relatively short order. National laboratories are populated almost entirely by technical experts; given the labs' recent emphasis on software development, these scientists and engineers now possess experience making cyber systems that could be focused into the development of offensive cyber operations tools. It would be prudent to investigate the status of software and firmware development as a core competency for these FFRDCs and national laboratories, because the expedited MIPR

process could quickly utilize these educated cyber experts, thereby improving the DoD's ability to develop offensive cyber systems quickly and efficiently.

Omnibus Development Contracts

Multiple defense and intelligence-related organizations currently use omnibus development contracts to achieve their developmental goals. Officially referred to by the FAR as a "bundle" contract, the omnibus contract consolidates multiple requirements for supplies or services into one single contract solicitation. This merging under an omnibus contractual vehicle saves administrative costs and time, though it is only useful when there is effective commonality in the requirements being filled by the contract. By holding an omnibus competition for cyber-related activities, a government organization could determine which bidding companies are competent and competitive for future cyber efforts. This process vets potential developers, narrowing the pool to high-grade teams so the USG can maintain multiple options for a related set of requirements. In fact, USCYBERCOM (via the Defense Information Systems Agency) recently pursued an omnibus contract for defensive cyber activities.[13]

The true benefit of an omnibus contract comes from structuring related multiple requirements with "carrot and stick" approaches. By relaying overall intent to prospective bidders during "industry day" meetings, the government organization can outline its vision for cyber tools that it intends to develop. Competitions could then be held for rudimentary-level building blocks that serve as "stepping stones" for the USG's ultimate end goals. Prospective bidders will clamor over one another, using their corporation's internal research and development funds to pre-develop the "final goal" cyber tools, knowing that if they impress the government enough to win the "stepping stone" competition, then their company will be in prime position for a sole-source award for the lucrative "final goal" cyber tool. The extra wrinkle of the

omnibus competition is that similar efforts can be worked at the inexpensive "stepping stone" level by multiple companies, giving the USG multiple horses in the proverbial race to pursue the more difficult "final goal" cyber tool. This constant competition between qualified companies would result in tremendous gains for government organizations attempting to develop offensive cyber operation tools. Admittedly the concern over revealing the government's true intent (which is likely highly-classified) to multiple companies and engineers does increase the likelihood of a security leak, even among cleared companies. One can mitigate this risk by spreading invested government funds at reasonable levels across multiple independent cyber tools, in case one thread is compromised.

Support Contract Vehicles

Most military acquisition units hire support contractors to provide services, whether they are administrative or technical, for the purpose of maximizing the program office's efficiency. When designing an aircraft modification, the technical support contractors will analyze the prime developer's design work on behalf of the USG, but the technical support contractor will not actually accomplish the design work. With regards to software code, however, the difference between analyzing and accomplishing the software coding effort is extremely close. This creates an opportunity to employ support contractors to augment code, essentially repurposing the support contractor as a hired-gun developer working within the program office.

Support contract vehicles therefore could be used to build in-house development teams. It is very likely that certain forward-leaning rapid acquisition organizations use this method today. By changing the greater acquisition culture to be amenable to this concept, significant benefits can be achieved. The United State Air Force (USAF), in particular, has had tremendous difficulty with preparing its cyber experts with the skill sets needed to succeed in the global

cyber community.[14] The standard USAF practice to build leaders with career broadening opportunities and deployments does not foster the creation of in-house educated cyber warriors. Additionally, those warriors who develop these capabilities (frequently on their own time) oftentimes migrate to the most lucrative private sector, according to cyber officer Capt Nick Kulesza.[15] For these reasons, it has been very challenging for the USAF to field a significant in-house uniformed offensive cyber operations tool development team. Augmenting the USAF's cyber leaders with highly-educated support contractors, who can perform the heavy lifting while the USAF officers focus on the strategic vision and mission, would improve the military service's ability to operate in cyberspace.

Lt Col Dan Ward outlined an innovative acquisition method that, combined with support contract vehicles, could prove very effective for the development of offensive cyber operation tools. The Fast, Inexpensive, Restrained, Elegant (FIRE) method conceived by Ward "[fosters] innovation by establishing constraints… the data strongly suggests the best outcomes are produced by small teams working with short schedules, tight budgets, and deep commitments to simplicity."[16] Ward's emphasis on using small, agile teams to quickly develop non-complicated solutions fits perfectly with a construct suggested by Maj Ryan Mutch. Mutch argued that, for computer network attack capabilities, great success could be achieved with rudimentary hacking techniques. Modifying publicly-available attacks with an in-house team, presumably leveraging publicly-acknowledged exploits, can be achieved with relatively few labor hours. If the in-house development team does not need to concern itself with delivering the exploit, rather just developing it, then a small team of support contractors could use the FIRE method to churn out simplistic attacks very rapidly.[17]

This involves what Mutch described as adopting the special operations forces' mantra of "living off the land" into a cyber-context. One must accept a paradigm shift from today's expectation that solutions must be flawlessly elegant, and instead be willing to live with some mistakes so that the FIRE-based teams can quickly create an array of powerful tools. Highly-educated cyber experts can leverage low-end exploits very well, and they do not need high-end exploits to achieve significant effects. Just as a special operations tactician can work with any weapon he finds on the ground, the FIRE-based team will thrive by being able to customize any exploit it finds in the dark recesses of cyberspace.

By combining Ward's FIRE method for using small teams, Mutch's notion of "living off the land" to task highly-educated people to modify low-end publicly-available exploits, and support contract vehicles to supplement the USG's technical manpower, an effective acquisition strategy for the development of offensive cyber operation tools falls into the lap of the acquisition officer. Assuming that the acquisition officer has the gumption to structure a support contract vehicle to augment the program office with in-house developers, this strategy is entirely within the realm of the possible using the current acquisition framework. This method merely requires openness to a different and more forward-leaning approach, namely focusing on highly-educated small teams augmenting existing programs with assembly-line speed and efficiency. With this strategy, tremendous offensive cyber capabilities could be achieved quickly and at relatively low-cost. Further examination of this strategy, particularly to estimate potential gains or losses associated with its implementation, would help the USG quantify the worthiness of this acquisition approach.

Chapter 4

Acquisition Strategies Outside the Current Framework

"Changes to the Federal Acquisition System therefore should be focused on strengthening the cybersecurity knowledge, practices, and capabilities within the Federal government's network and domain. The implementation approach should leverage the existing system of voluntary international standards development and the Cybersecurity Framework. The government should start by changing its own practice that increase cyber risk and focus on the types of acquisitions that present the greatest cyber risk and in which investment of scarce resources will provide the greatest return overall."[18]

Report published by the Department of Defense, 2013

Whereas Chapter 3 examined acquisition strategies for offensive cyber tools that fall within the current framework, Chapter 4 steps outside the box to examine methods that either violate present-day rules or that challenge the mindset and culture of risk-averse leaders. The acquisition community has been adaptive and responsive over the past decade, slowly but surely changing its bureaucracy for the better. Drastic changes may be unlikely in the near-term, though a "Cyber Pearl Harbor" would certainly entice the Department of Defense to adopt more flexible acquisition concepts. If significant changes to policy or culture are to occur, four prospective strategies merit consideration: crowdsourcing, outsourcing, cyber fly-offs, and public-private partnerships.

Crowdsourcing

Crowdsourcing combines skills from a diverse and usually unrelated set of contributors. The Search for Extraterrestrial Intelligence (SETI) leveraged crowdsourcing to fuse the computing powers of millions of citizens across the globe for the purpose of finding electromagnetic signals that may have emanated from a life source outside the planet. Crowdsourcing changed the game for SETI, and now the private cybersecurity industry has taken steps to emulate this successful method.

Entrepreneurs within the cybersecurity realm leverage crowdsourcing techniques to develop solutions to threats such as malware and viruses.[19] In recent years, investors created an entirely new market by assembling intelligence products for potential threats identified by crowdsourcing methods, and selling these products to corporations such as financial institutions. These business ventures assemble teams of white-hat hackers who mastered the leading edge of technology. Using a similar acquisition strategy, the USG could put a clever twist on these crowdsourcing companies' actions by shifting the focus from threat detection into offensive cyber tool development.

By dabbling in the crowdsourcing pool, the DoD could tap-in to a vast and highly-educated labor force with expertise in the latest cyber technology advances. This would not be the first time the USG found expertise in "obscure" locations – in the 1940s, scientists and engineers were recruited from hostile nations to aid the Manhattan Project. Crowdsourcing of offensive cyber tools can similarly benefit by identifying the "right" people from a previously untapped pool of talent. Offering those people access to the USG's significant capabilities, so long as they can be granted a security clearance, can permit crowdsourcing to deliver an arsenal of offensive cyber tools. Conversely, splitting desired offensive capabilities into unrelated and unclassified subroutines could mask a highly-classified DoD cyber initiative, and effectively enable the DoD to leverage the power of crowdsourcing via security cutouts.

Crowdsourcing drawbacks center on security concerns. Enemies could infiltrate teams and neuter offensive tools from the inside. Potentially friendly white-hat hackers, upon realizing their efforts contribute to the United States military regime, may be dissuaded from contributing due to their wariness of the USG over cyber-privacy concerns. These drawbacks, however, affect any cyber acquisition strategy. Though the problems may be amplified based on crowdsourcing's

dependence on the cyber community, crowdsourcing nevertheless offers great potential to a cyber development team willing to experiment with this popular system.

Outsourcing

Crowdsourcing and outsourcing both rely on development teams external to the primary organization's control. Whereas crowdsourcing presents a fairly new technique to leverage external resources, outsourcing enjoys a history of collaboration with the military industrial complex. During the war campaigns in Iraq and Afghanistan, the United States military outsourced certain specific tasks to contractors, and private companies fought aspects of the war that the DoD could not touch due to public condemnation concerns.[20] Not only does outsourcing enable operations in politically-divisive settings, it can also reduce overall costs while providing access to the latest technology. For these reasons, outsourcing of offensive cyber tool development could translate into great rewards.

Outsourcing development efforts differs from the standard acquisition method of hiring developers in that outsourcing affords the developer much more freedom. When the USG outsources a task, it essentially throws the task "over the fence" and lets the development company figure out a solution with minimal government input. Given the independent nature of many cyber experts, the value of this "developmental freedom" inherent to outsourcing cannot be overemphasized. So long as the outsourced company delivers a functioning product in the end, it will receive its payment and the USG will receive its offensive cyber tool.

Outsourcing of development could fall within the realm of permissible acquisition activities given the current framework. That said, the outsourcing of offensive cyber operations crosses boundaries that would necessitate legal and policy changes. The USG strictly controls state-sponsored cyber operations, and entire operations could not be outsourced within the

current construct. If the USG were to amend its policies on this topic, outsourced cyber operations could open a wide array of possibilities heretofore unavailable to the nation. The DoD and related organizations would be able to take offensive cyber actions without dirtying their virtual hands. NIST risk management framework procedures, outlined as part of Chapter 3, could be bypassed. The DoD could deny involvement because operations could be pursued entirely outside of DoD networks, yet the USG could still keep its finger firmly on the pulse of the operation. Risk for the operation itself would shift to the contracted company, though ultimate responsibility and accountability would be retained by the USG. The outsourcing of cyber development and actual cyber operations presents new opportunities that merit further analysis.

Cyber Fly-Offs

A generation ago, competitive challenges for government contracts, oftentimes referred to as fly-offs, were fairly commonplace in many military domains. Vehicle, munition, and aircraft competitions determined which company's design would be funded to production. For example, in 1974 the USAF competed the A-7 and A-10 aircraft designs to select an airframe for the close air support mission. Pilots tested both models against specific objectives such as acquire attack, reacquire, and evasive maneuvering. The A-10 won, and operational units received the first A-10 aircraft two years later.[21] Cyber fly-offs could function similarly to the aforementioned aircraft fly-offs, delivering better tools to the offensive cyber unit.

As was the case with outsourcing operations, some aspects of cyber fly-offs do indeed fall within the legal framework of the FAR, but institutional apprehension regarding fly-offs due to fear of protests and cost escalation make it a nearly impossible proposition within the current acquisition culture. The emphasis on reducing costs within the acquisition community deters many from pursuing fly-offs because they oftentimes dictate that the USG must contract multiple

companies to pursue the same set of requirements. This shortsighted fear aside, possibly a bigger concern is a protest of the USG's decision between competing designs. Though not technically a fly-off, the KC-X tanker competition experienced significant delays due to protests over selection methodology. Fortunately, a cyber fly-off should be easier to assess objectively in order to avoid a KC-X debacle over evaluation criteria and methodology.

Other risks associated with a cyber fly-off competition are that the losing company may make its tool available to an adversary, particularly if a disgruntled developer on the losing side hits the unemployment line and takes his talents and subroutines outside the country. Consequences of such an action are much more severe than if a KC-X engineer or an A-7 designer left their companies, due to the nature of offensive cyber operations, but the likelihood of this risk can be mitigated through effective security clearance vetting and other security countermeasures. Overall, the benefits of a cyber fly-off appear to outweigh the costs and the associated risks, as this potential acquisition strategy inspires competition similar to that of the omnibus contract strategy.

Public-Private Partnerships

Public-private partnerships (PPPs) use cooperative arrangements between government entities and private sector entities for the purpose of conducting defense-related work using DoD facilities and equipment. They help the USG achieve readiness in certain mission areas, providing key support capabilities that reduce the cost of operational readiness.[22] By definition, the mutually-beneficial partnership delivers value to both the public sector and the private sector. Traditionally the military only utilizes PPPs for logistics-related mission sets. Establishing PPPs within the cyber domain could pay significant dividends, particularly due to the relevance of cyber activities to both the public and private sectors. Whereas stealth bombers utilize

technology and equipment that has minimal application outside of the military, many industries rely upon cyber tools. The financial industry, with its deep pockets, invests handsomely in cyber operations; a partnership that shares or repurposes hardware and software and technological breakthroughs across the military and financial sectors could be a game-changer for both sides of the partnership.

Additional opportunities beyond the standard thinking of the DoD could be realized with creative PPPs. The information exchange inherent to a cyber PPP aligns with the intent of the National Infrastructure Protective Plan, which promotes public-private cyber information sharing efforts. A cyber acquisition strategy utilizing a PPP will certainly meet reluctance, if not all-out resistance, from acquisition leadership due to classification concerns and the risk of creating additional avenues for adversaries to infiltrate military networks. These fears amplify with the introduction of offensive cyber operation tools into the PPP.

In 2015, Maj Tom Purdie laid the groundwork for a PPP between IBM and the LeMay Center for Doctrine Development and Education at Maxwell AFB. The warfighting center at Maxwell will get use of a Watson system for a tremendously reduced price, and IBM will get to remotely use the computing power of the system during non-duty hours.[23] This PPP framework is but one example of a way the DoD can acquire hardware that could be leveraged for offensive cyber operation tool development, while establishing a mutually-beneficial relationship with the private sector supplier. PPPs could similarly be pursued with entities to develop software testing automation as well as network penetration testing. Collaborations with private industry partners within the cybersecurity and financial industries could create conditions where offensive cyber tools can be refined while also delivering a benefit to the private partner.

Chapter 5

Conclusion

"Moreover, the Pentagon must always have a watchful eye on the horizon, anticipating needs and gaps in capabilities before they become dire. These findings should drive rapid research and development, particularly experimentation with new or improved technologies and the building of prototypes. Investing in science and technology early on ensures that the Pentagon will have something on the shelf when it needs it, so that it does not have to start from scratch when it is too late."[24]

Ashton B. Carter, 2014

Summary

Acquisition of offensive cyber operations tools presents many challenges, but also many opportunities. Within the current acquisition framework, potential exists for tremendous gains by leveraging an array of strategies that abide by the FAR and align with established acquisition doctrine. Also exciting are creative development strategies made possible through changes to the current acquisition framework, though the established organizational culture of DoD acquisition would likely balk at the reforms required to pursue those methods. Nevertheless, reasonable options exist to rapidly develop and acquire effective offensive cyber operations programs; the traditionally slow pace of DoD acquisition need not prevent the USG from strengthening its position in the cyber domain.

Within the current acquisition framework, four strategies merit consideration. Embedded cybersecurity management teams would insert empowered authorizers in the heart of the development process, allowing programs to gain necessary approvals in parallel with other activities. Leveraging national laboratories for software development can provide program managers with highly-trained cyber engineers on short notice. Omnibus contracts can incentivize defense-focused corporations to push cyber boundaries. Support contract vehicles, with

progressive interpretations of contractual scope, can deliver in-house development teams that create an arsenal of cyber exploits with great speed.

Exploring possibilities either outside the current acquisition framework, or so far removed from acquisition doctrine that a cultural shift would be required for implementation, finds four additional strategies that can yield significant gains. Private cybersecurity companies use crowdsourcing techniques, which signals that crowdsourcing of cyber development could be a potential avenue for the USG to explore. The DoD outsources certain mission areas, such as physical security in high-risk global hotspots, to private firms because of their efficiency and effectiveness; outsourcing offensive cyber operations would require clever legal maneuvering, but could deliver remarkable dividends. The "fly-off" acquisition technique lost popularity due to cost considerations, though cyber fly-offs could rejuvenate this dormant acquisition method. Finally, public-private partnerships between either the DoD and financial institutions, or the DoD and hardware developers, could give the USG access to tools greater than it can afford by itself in today's reduced budget climate.

The eight strategies described in this paper introduce risks to the acquisition process. With the current mandate to do more with less, acquisition leadership must be willing to push its comfort levels by exploring the path less-traveled, bringing these strategies fully into play. Cyber activities quickly escalate with regards to security classifications, thus any acquisition strategy for offensive cyber operation tool development must take significant security precautions; methods like crowdsourcing and public-private partnerships would require shrewd security cut-outs to prevent unauthorized disclosures.

If one can coax the acquisition institution to further adapt its processes, and one can mitigate security risks associated with these techniques, then these innovative acquisition strategies will revolutionize cyber development for the DoD.

Recommendations for Future Research

This study examined acquisition strategies from an abstract, qualitative perspective. Within the objective culture of the acquisition community, change is unlikely without a quantitative analysis. For example, newfangled concepts like crowdsourcing and PPPs must be supported by hard numbers if they are to be accepted by acquisition leadership. It is recommended that any further analysis of these concepts should focus on evaluating potential cost savings and schedule reductions associated with each particular strategy.

Legal ramifications of some of the suggested strategies should be examined further. In particular, the prospect of outsourcing an entire offensive cyber operation could be challenged on legal grounds, so this acquisition strategy would need to develop an adjoining legal strategy to permit its employment. Private military companies certainly exist and operate today; examination of their legal framework and relevant case studies could provide useful for potential outsourcing of offensive cyber operations.

Concluding Thoughts

Acquisition reform over the last decade improved the DoD's ability to equip the warfighter. To achieve great gains in the cyber domain, however, new and "outside the box" strategies must be adopted. For example, the combination of support contract vehicles with the FIRE approach with the "highly-trained individuals modifying low-end exploits" method could coalesce into a powerful tool for the DoD. Similarly, crowdsourcing (with effective security controls) in conjunction with PPPs can exponentially expand the talent pool the DoD can utilize.

The framework and ideas exist to modify the acquisition process to thrive with regards to cyber operations; it is the duty and responsibility of DoD acquisition professionals to push forward and make the system better.

Glossary

AFTAC	Air Force Technical Application Center
DIACAP	DoD Information Assurance Certification and Accreditation Process
DoD	Department of Defense
FAR	Federal Acquisition Regulation
FIRE	Fast, Inexpensive, Restrained, Elegant
FFRDC	Federally Funded Research and Development Center
MDA	Milestone Decision Authority
MIPR	Military Interdepartmental Purchase Request
NIST	National Institute of Standards and Technology
POM	Program Objective Memorandum
PPBE	Planning, Programming, Budgeting and Execution
PPP	Public-Private Partnerships
SETI	Search for Extraterrestrial Intelligence
USAF	United States Air Force
USG	United States Government

Bibliography

"A-7/A-10 Close Air Support Fly-Off." *National Museum of the US Air Force.* December 31, 2008. http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=3201 (accessed March 23, 2015).

Basulto, Dominic. "Crowdsourcing America's Cybersecurity Is An Idea So Crazy It Might Just Work." *The Washington Post*, February 5, 2015.

Butler, Matt J. *Rapid Delivery of Cyber Capabilities: Evaluation of the Requirement for a Rapid Cyber Acquisition Process.* Wright-Patterson AFB, OH: Air Force Institute of Technology, 2012.

Carter, Ashton B. "Running the Pentagon Right." *Foreign Affairs.* January/February 2014. http://www.foreignaffairs.com/articles/140346/ashton-b-carter/running-the-pentagon-right (accessed February 16, 2016).

Chamberland, Denis. "Contractors on the Battlefield: Outsourcing of Military Services." *National Defense Magazine.* March 2011. http://www.nationaldefensemagazine.org/archive/2011/March/Pages/ContractorsontheBattlefieldOutsourcingofMilitaryServices.aspx (accessed March 23, 2013).

Clark, Colin. "Acquisition on FIRE, or How a Lt Col Can Make a Difference." *Breaking Defense.* August 22, 2014. http://breakingdefense.com/2014/08/acquisition-on-fire-or-how-a-lt-col-can-make-a-difference/ (accessed March 23, 2015).

Corrin, Amber. "Defense Budget Routes At Least $5B to Cyber." *Federal Times,* March 5, 2014.

Defense Acquisition University. *Planning Programming Budgeting and Execution Process.* n.d. https://acc.dau.mil/CommunityBrowser.aspx?id=488289 (accessed March 15, 2015).

Defense Information Systems Agency. "USCYBERCOM Omnibus IDIQ Contract Solicitation." *FedBizOpps.* September 11, 2014. https://www.fbo.gov/?s=opportunity&mode=form&id=63a08d1386b0426debf21c53cd8572db&tab=core&_cview=0 (accessed March 23, 2015).

Floyd, Dave, and Tom Gorman. "Public-Private Partnerships." *Defense AT&L*, January-February 2013: 32-35.

Golaboski, Jason M. "DoD Weapons Systems Acquisition: A Cyber Disconnect." Maxwell AFB, AL, 2011.

Goolsby, Rebecca, Lea Shanley, and Aaron Lovell. *On Cybersecurity, Crowdsourcing, and Social Cyber-Attack.* Arlington, VA: Office of Naval Research, 2013.

Gulick, Ed. "AF Acquisition Chief Nominee Testifies." *U.S. Air Force.* January 17, 2014. http://www.af.mil/News/ArticleDisplay/tabid/223/Article/473130/af-acquisition-chief-nominee-testifies.aspx (accessed February 16, 2015).

Hagan, Gary. "Overview of the DoD Systems Acquisition Process." DARPA, May 4, 2011.

Hawthorne, Skip. "Re-Issuance of DoD Instruction 5000.02." December 5, 2013.

Improving Cybersecurity and Resilience through Acquisition. Department of Defense and General Services Administration, November 2013.

Lee, Robert M. "Disruptive by Design: Saving the Air Force Cyber Community." *AFCEA.* February 1, 2015. http://www.afcea.org/content/?q=disruptive-design-saving-air-force-cyber-community (accessed March 23, 2015).

Lin, Herbert S. "Offensive Cyber Operations and the Use of Force." *Journal of National Security Law & Policy* 4, no. 63 (2010).

McFarland, Katrina. "Testimony Before the Senate Armed Services Committee Subcommittee on Readiness and Management Support." February 26, 2014.

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. "Department of Defense Policies and Procedures for the Acquisition of Information Technology." Washington, DC, 2009.

Panzarino, Matthew. "This is How Apple's Top Secret Product Development Process Works." *The Next Web.* January 24, 2012. http://thenextweb.com/apple/2012/01/24/this-is-how-apples-top-secret-product-development-process-works/ (accessed February 16, 2015).

Perera, David. "DoD Abandons DIACAP in favor of the NIST Risk Management Framework." *FierceGovernmentIT.* March 18, 2014. http://www.fiercegovernmentit.com/story/dod-abandons-diacap-favor-nist-risk-management-framework/2014-03-18 (accessed March 23, 2015).

Shalal, Andrea. "Military Acquisition Rules Hamper U.S. Ability to Counter Cyber Threats." *Reuters,* May 19, 2014.

Shiffman, Gary, and Ravi Gupta. "Crowdsourcing Cyber Security: A Property Rights View of Exclusion and Theft on the Information Commons." *International Journal of the Commons* 7, no. 1 (February 2013): 92-112.

Taylor, Aaron T. *Partnering with the Cyber Industrial Base and Developing Acquisition Practices.* Maxwell AFB, Alabama: Air University, 2009.

The White House. "National Security Strategy." Washington, DC, January 2015.

Walker, Molly Bernhart. "Kendall: Cyber Acquisition is Unique." *FierceGovernmentIT.* February 8, 2012. http://www.fiercegovernmentit.com/story/kendall-cyber-acquisition-unique/2012-02-08 (accessed February 16, 2015).

Notes

1. White House, "National Security Strategy," 8.

2. Amber Corrin, "Defense Budget Routes At Least $5B to Cyber," *Federal Times*, March 5, 2014.

3. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Report on Department of Defense Policies and Procedures for the Acquisition of Information Technology," March 2009: 36.

4. Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy* 4, no. 63 (2010): 64.

5. Ed Gulick, "AF Acquisition Chief Nominee Testifies," U.S. Air Force, January 17, 2014.

6. Gary Hagan, "Overview of the DoD Systems Acquisition Process," DARPA, May 4, 2011.

7. Skip Hawthorne, "Re-Issuance of DoD Instruction 5000.02," December 5, 2013.

8. Defense Acquisition University, "Planning Programming Budgeting and Execution Process."

9. Molly Bernhart Walker, "Kendall: Cyber Acquisition is Unique," *FierceGovernmentIT*, February 8, 2012.

10. David Perera, "DoD Abandons DIACAP in favor of the NIST Risk Management Framework," *FierceGovernmentIT*, March 18, 2014.

11. Maj Gary Thompson (MILSATCOM Systems Directorate), in discussion with the author, 5 February 2015.

12. Capt Patrick Roberts (Air Force Technical Application Center), in discussion with the author, 4 February 2015.

13. Defense Information Systems Agency, "USCYBERCOM Omnibus IDIQ Contract Solicitation," *FedBizOpps*, September 11, 2014.

14. Robert M. Lee, "Disruptive by Design: Saving the Air Force Cyber Community," *AFCEA*, February 1, 2015.

15. Capt Nick Kulesza (Air Force Institute of Technology), in discussion with the author, 5 February 2015.

16. Colin Clark, "Acquisition on FIRE, or How a Lt Col Can Make a Difference," *Breaking Defense*, August 22, 2014.

17. Maj Ryan Mutch (Air Force Institute of Technology), in discussion with the author, 12 February 2015.

18. Department of Defense and General Services Administration, "Improving Cybersecurity and Resilience through Acquisition," November 2013: 9.

19. Dominic Basulto, "Crowdsourcing America's Cybersecurity Is An Idea So Crazy It Might Just Work," *The Washington Post*, February 5, 2015.

20. Denis Chamberland, "Contractors on the Battlefield: Outsourcing of Military Services," *National Defense Magazine*, March 2011.

21. National Museum of the US Air Force, "A-7/A-10 Close Air Support Fly-Off," December 31, 2008.

22. Dave Floyd and Tom Gorman, "Public-Private Partnerships," *Defense AT&L*, January-February 2013: 32-35.

23. Maj Tom Purdie (Air Command and Staff College), in discussion with the author, 3 March 2015.

24. Ashton B. Carter, "Running the Pentagon Right," *Foreign Affairs*, January/February 2014.