Cyber Acquisition

Policy Changes to Drive Innovation in Response to Accelerating Threats in Cyberspace

Thomas Klemas
U.S. Air Force

Rebecca K. Lively
U.S. Air Force

Nazli Choucri
Professor of Political Science
Massachusetts Institute of Technology (MIT)
Cambridge, Massachusetts, USA

ABSTRACT

The United States of America faces great risk in the cyber domain because our adversaries are growing bolder, increasing in number, improving their capabilities, and doing so rapidly. Meanwhile, the associated technologies are evolving so quickly that progress toward hardening and securing this domain is ephemeral, as systems reach obsolescence in just a few years and revolutionary paradigm shifts, such as cloud computing and ubiquitous mobile devices, can pull the rug out from the best-laid defensive planning by introducing entirely new regimes of operations. Contemplating these facts in the context of Department of Defense (DoD) acquisitions is particularly sobering because many cyber capabilities bought within the traditional acquisition framework may be of limited usefulness by the time that they are delivered to the warfighter. Thus, it is a strategic imperative to improve DoD acquisitions pertaining to cyber capabilities. This paper proposes novel ideas and a framework for addressing these challenges.

Keywords– DDoS, RQA, Adaptive Clustering, A-Kmeans.

I. INTRODUCTION

Almost everyone agrees that growing threats to cybersecurity are undermining the Nation's safety. Not a day goes by without reports on new breaches and exploitations. Indeed, an entire industry has developed around evaluating the impacts of cybersecurity incidents, reporting on trends, and assessing impacts. Far more compelling is the evidence that the United States is facing escalating cyber hostilities with increasing frequency from a growing number of diverse adversaries[1],[2],[3],[4],[5],[6]. The challenges posed by the near-instantaneity of cyber action have no precedent. Given the fluidity, complexity, and ambiguity of the cyber domain, framing an adaptive, dynamic, and reliable policy response amounts to a critical imperative. It is a necessity, not a choice.

NOTE: The views expressed in this paper are the authors' and do not necessarily represent the views of the U.S. Air Force (USAF), the DoD or the United States

Shaping and retaining advantage in the cyber domain requires a comprehensive approach that leverages all aspects of national power, including diplomatic, economic, informational, technological, and military elements. This paper focuses on the military dimension of national power and concentrates on one major factor—namely, equipping the force with innovative and necessary cyber tools through the acquisition process. Our purpose is to motivate cyber-specific enhancements to existing policy. More specifically, we seek to reduce, if not eliminate, powerful obstacles that prevent the rapid development and delivery of cyber capabilities that are crucial to defending U.S. systems and infrastructure.

This paper presents a logical basis for necessary changes to existing policy and empirical data which compel essential, cyber-specific changes to current acquisition processes. In addition, this paper proposes a specific approach to enhancing the process so that cyber acquisition can be responsive to the rapidly changing threat landscape. Considering the current cyber domain and the overall environment, we demonstrate that the current acquisition process is too slow to: (1) meet current and likely future cyber warfighter needs; (2) too slow to respond to cyber adversaries who are frequently moving faster than the United States; and (3) keep pace with the rapidly changing threat environment. These factors, among others, highlight the fundamental differences between cyber requirements and traditional acquisition.

We proceed as follows: Section II highlights the new strategic imperatives that create the context for both cyber and traditional acquisition and the general imperative driving the urgency of cyber acquisition reform. Section III explores the expanding roster of hostile states and criminal organizations and growing adversary progress and cyber strength, as reported in publicly available materials. Section IV describes cyberspace dynamics, including the impacts of dramatic information technology (IT) change, and then points to how these factors will continue to impact the defense posture of the United States. Finally, section V presents an acquisition policy framework which can address these compelling issues and contribute to U.S. cyber superiority.

II. NEW STRATEGIC PARAMETERS

There is a growing awareness that acquisition reform is crucial to the national defense and that traditional acquisition approaches are measured in completely different timescales than the pace required by cyber realm approaches. In fact, timelines for operational needs are quite short in the cyber domain. Some capabilities are needed within only a few weeks and are often used only one time by cyber warfighters. But traditional acquisition processes take many years, sometimes even more than a decade to complete.

Recent attempts to streamline the acquisition process[7] targeted improvements that would result in a 5- to 7-year process. In 2016, the DoD disclosed that the estimated median duration for Major Defense Acquisition Programs was more than 6.9 years[8]. However, Major Automated Information System life cycles had an estimated median of 3.2 years for programs after 2009[8].

It is noteworthy that both of these figures exceed most cyber need timelines, potentially by orders of magnitude. Based on these considerations, it is evident that traditional processes, even if improved to achieve the goals in[7], are not sufficiently rapid to keep pace with technological evolution or to acquire cutting-edge cyberspace capabilities. The mismatch of traditional acquisition timelines with cyber needs and useful lifespans virtually guarantees that the military will be equipped with aging cyber capabilities that may have limited usefulness or rapidly become obsolete [50]. So long as acquisition does not have the mechanisms to keep pace with needs, the military will be forced to utilize increasingly inferior capabilities[9]. All of this is embedded in the very reality of a process shaped by criteria other than time. More to the point, it sheds a dim view of a situation seen through the lens of timelines for warfighter needs.

"America's military has no preordained right to victory on the battlefield"[30]. This is especially true in the face of "rapid technological changes" and an environment where "inter-state strategic competition, rather than terrorism, is the primary concern in US National Security" [30]. Thus, "[t]his is truly a period in history in which we are falling behind if they are merely holding our position in the overall movement to forge new capabilities"[10]. However, existing acquisition processes were designed to develop warfighting systems that sometimes last for decades. They were not designed for any features of the cyber domain, nor for the extremely rapid cyber decision and action process. A number of U.S. airplanes have been operating for more than 40 years, an extreme example being the Boeing B-52, which may survive past 100 years[11]. For the most part, cyber power rests on speed and agility, not on stability and longevity. Cyber capabilities have a lifespan of weeks; months; or, at most, a few years, often only persisting that long through frequent upgrades.

III. ACCELERATING THREATS

The current intensity of cyber incidents and sophistication of advanced cyber threats is a defining feature of the 21st century, and barriers to effective defense are high[1],[2],[3],[4],[5]. As a direct result, demands are mounting on U.S. cyber forces. Additionally, new malicious activities cause features of the cyber domain to change and sometimes create a need for new tools, new skills, and new training. In this section, we will substantiate that the cyber adversaries challenging the United States today are well resourced, increasing in number, constantly striving to improve and diversify their capabilities, growing bolder, displaying a high degree of freedom of action, and perhaps outpacing the United States in some regards.

A brief overview of cyber threat history, including recent malicious activities, intrusions, and responses, is necessary to provide context, justify the principal motivational elements, and distill key insights that will guide discussion and substantiate the proposed approach. Especially relevant is the fact that many of our adversaries are not hampered by an acquisition process anchored in institutional and historical experience and resistant to rapid adaptation to changing circumstances. Two of the countries that represent the greatest overall threat to U.S. interests – Russia and China – seem to display a remarkable level of hostile cyber intent.

The progression of Microsoft Cloud Azure Service reports[1],[2],[4] from 2016 to 2018 suggests a notable escalation in malicious activities on Microsoft Cloud virtual machines that seem to originate from Russian internet protocol (IP) addresses. The 2018 data reported an almost 16-percent rate of total incoming attacks which seem to originate from Russia, up from previous levels below 10 percent.

We have learned the surprising extent of Russian moves to interfere with U.S. elections, signaling an elevated degree of the Russian intelligence intent to penetrate and influence civil society. The Office of the Director of National Intelligence released[6], which describes some of the national intelligence analytical assessments regarding Russian interference in the 2016 elections. The analysis indicates that the campaign was well coordinated and financed, consisting of operations organized by the General Staff Main Intelligence Directorate which included exfiltration of a significant quantity of data from the U.S. Democratic National Committee and the leveraging of internet trolls from the Saint Petersburg–based Internet Research Agency, a close Putin ally with ties to Russian intelligence. These activities highlight the growing "grey zone" behaviors of state actors who take actions below the international law threshold which would permit a kinetic military response[12]. All was done without the use of one single bullet or the loss of one single life. An adversary has unilaterally changed the "rules of the game" and made civil society its operational target.

Beyond election interference, an alarming set of other significant cyber activities have occurred during the past several years that appear to have originated from the Russian Federation. Here we summarize just a few of the more prominent incidents, referenced from the Center for Foreign Relations data set[3]. In March 2015, Ukrainian officials were targeted by cyber espionage attempts. In September 2016, the World Anti-Doping Agency (WADA) computer systems were compromised and data was leaked regarding athletes in the 2016 Rio de Janeiro Olympics, presumably in response to the previous WADA report that outlined systematic Russian use of performance-enhancing substances during the 2014 Sochi Olympic Games. Shortly thereafter, several U.S. think tanks that focused on international relations and national security were targeted by compromise attempts. In July 2017, the NotPetya malware encrypted data in numerous European, Australian, and U.S. organizations, to disrupt financial operations (tax filings). During early 2018, numerous actions targeted Winter Olympics sports entities following the ban on Russian Winter Olympic athletes. Also during this period, several spear phishing attempts appeared to target a European defense agency and several foreign ministries.

Despite the prominence and targeting of malicious Russian activities, China's actions have also been prolific during the past several years. The same Microsoft Cloud Azure Service reports[1],[2],[4] referenced above found that almost 33 percent of all malicious activities on its virtual machines came from IP addresses in China in 2018, a dramatic upswing in activity from 2016 and 2017 and an indication of targeted aggression.

Considering only virtual machines that were penetrated, 54 percent communicated with IP addresses in China. While IP address attribution is not definitive, these statistics do suggest actors in Russia and China are principal cyber adversaries. China's state exploits have concentrated on business and industry and gained considerable notoriety. China has been rapidly growing its cyber operational capabilities. Especially important is the rapid rate of cyber skill development in a government-controlled labor force. A new social credit system introduced in China—whereby citizens are observed and rewarded for good behavior—all but assures China's almost total knowledge of and potential control over its citizens and facilitates the possibility of government-controlled, crowd-sourced activities[13],[14].

The Council on Foreign Relations incident data set[3] contains at least 85 major cyber incidents attributed to China since 2006. The incidents described in this section are just a few of the more recent activities linked to China and the Chinese Government. In April 2017, an operation called "Cloud Hopper" tried to penetrate internet service providers to access customer data in 15 countries, including the United States[16]. The global scope of this activity suggests the deployment of a significant level of resources. Notable for the use of multiple types of malware, including Remote Access Trojans and Microsoft file signatures, this campaign employed targeted phishing utilizing Microsoft Office documents that contained modifications to exploit system vulnerabilities and leveraged hundreds of variations of malware and customized, open-source tools to exfiltrate data, even compressing and encrypting the data to avoid detection.

The variety, customization, and diversity of techniques employed by China establish it as a very advanced threat actor. In October 2017, another group referred to as "Bronze Butler" staged numerous hacks targeting industry, manufacturing, and infrastructure in Japan, South Korea, Russia, and even entities within China, apparently for espionage purposes[17]. This group demonstrated advanced techniques, including the development of custom malware, elimination of traces of infiltration, and encryption of command and control communications. In June 2016, government systems and critical infrastructure were targeted within Myanmar, the United States, Canada, South Korea, Singapore, Germany, and India[18]. After that, in October 2017, entities associated with the maritime industry were targeted within Asia, the United States, the Philippines, and Hong Kong. Then, in November 2017, hackers from a Chinese internet security company attempted to steal trade secrets from Trimble, Siemens, and Moody's Analytics[19]. The internet security company associated with the hacking has been linked closely to the Chinese People's Liberation Army and is believed to receive state sponsorship for its activities. The intent in all but one of these cases appeared to be espionage and theft of intellectual property, signaling key differences between the Russian and Chinese actions during this period.

The news has been so saturated with discussion of Russian election interference and Chinese cyber technology espionage activities that it is easy to overlook other incidents. However, recent history is replete with mounting reports of North Korean and Iranian intrusions, as well

as those of other nation-states. The Council on Foreign Relations incident data set[3] listed more than 20 incidents that gained news attention that was attributed to Iran between 2010 and 2018, 7 of which were between 2017 and 2018 alone. Additionally, about 20 incidents were attributed to North Korea between 2009 and 2018.

Perhaps slightly below the radar, Iran has been quite active. In March 2018, it was discovered that almost 150 U.S. universities, and a similar number in over 20 other countries, had been compromised as part of malicious activity by the Mabna Institute, an entity believed to have ties to the Iranian National Guard[20]. In June 2017, Iran-linked hackers attempted to infiltrate and compromise email accounts of British Parliament members[21]. Investigations revealed that hackers gained access to 30 accounts out of the more than 9,000 targeted. This event was noteworthy more for its boldness than its sophistication. In July 2017, Iran targeted universities; the defense industry; and IT companies in Germany, Saudi Arabia, Israel, Jordan, and the United States[22]. This intrusion was notable for the diversity of techniques employed to achieve its objectives and the introduction of custom tools, although the hackers were noisier than normal for advanced threat actors, which accelerated detection and response.

A few months later, in November 2017, another event, labeled "Muddy Water"[23], promulgated by a group known as "Unit 42," targeted numerous Middle Eastern nations with the apparent goal of espionage. The techniques employed, which did not seem to display tremendous diversity, leveraged open-source tools but evolved over time. However, these intrusions featured documents that were delivered to the targets and designed to entice users with customizations related to their geographic region or relevant organizations. Even more nefarious, in many cases, actual documents were stolen from compromised accounts, modified to introduce malware, and sent onwards to additional targets that were already expecting the original documents.

Significant activity during the past few years also appears to have originated from North Korea. The Center for Foreign Studies data set cites several such actors as having perpetrated cybercrimes in February 2018. One actor, known as "Group 123," targeted South Korea[24]. This actor initiated numerous campaigns that received publicity: "Golden Time," "Evil New Year," "Are you Happy?," "Free Milk," "North Korean Human Rights," and "Evil New Year 2018." Prominently featured in this campaign was spear phishing with maliciously modified documents. Another well-known example, "WannaCry," was ransomware that struck hundreds of companies around the world in May 2017, causing about $4 billion in losses[25],[26]. This activity exploited a known and patched vulnerability for Windows, but over 200,000 unpatched systems were still affected. Additionally, in September 2017, hackers targeted U.S. electrical companies with an apparent objective of early-stage surveillance[27]. Many of the actions attributed to North Korea seem designed for disruption (warning) or to show national determination, build wealth by theft or fraud, or conduct espionage. Clearly, the activities demonstrate a boldness that usually accompanies impunity.

Overall, the cyber aggression attributed to Russia, China, Iran, and North Korea exhibits a

pronounced freedom of action buttressed by advancing capabilities, enabling the increasingly complex scenarios demonstrated by these countries. On balance, the cyber domain appears to be a great leveler, emboldening states[1],[2],[3],[4],[5] and freeing them from limitations in kinetic capability. To all of this we must add the rapid growth of cybercrime and potential asymmetries inherent to cyber that suggest how many non-state actors can pose significant threats to national security. In these situations, the clear advantage of the aggressor and the significant stresses placed on the defense cannot be denied.

The record of threat actors and cyber intrusions constitutes powerful evidence of growing cyber needs that reinforce the disparity between such cyber needs and the timeliness of the acquisition process. This disparity amounts to a massive opportunity cost in the form of an institutional handicap imposed on warfighters and corroborates the notion that the current acquisitions process is not providing U.S. cyber warriors the resources they need to maintain superiority over adversaries. More to the point, this disparity is creating powerful constraints, potentially crippling the effectiveness of the cyber force. But there are added factors that reinforce this corroboration. .

IV. UNRELENTING CYBER TRANSFORMATION

In cyberspace, as in most competitive spaces, having a faster pace of advancement is an advantage. But in the cyber domain, the speed of innovation coupled with rapid procurement is far more than an advantage—it is a matter of basic survival. The United States has long been a leader in advanced technology. If other countries develop new, advanced capabilities more quickly or implement them more efficiently, we will find ourselves in dire circumstances. It goes without saying: in order to succeed in a sword fight, when your opponent strikes a blow, you must be at least fast enough to dodge or parry the blow in *real* time and have the requisite speed to respond or counterattack. At a minimum, you should not be equipped with a heavy, cumbersome, and blunt sword, or no sword at all.

To serve as a suitable analog for the cyber battlespace, the sword fight example must be extended so that both the swords and the fight environment are also continually changing to account for the constant and rapid evolution of cyber tools, networks, and computer technologies. Risks are amplified dramatically by the speed at which the cyber environment evolves, the frequency of security vulnerabilities, and the degree of asymmetry that is possible in this realm. In fulfilling its cyber missions, the DoD must not only protect against malicious activity, but also account for the rapid technological changes and equip cyber warriors with powerful capabilities that will provide critical leverage in battle.

Numerous technology-based technology shifts are occurring at this time. Cloud computing serves as an example of the speed at which the cyber environment is changing; it represents a dramatic paradigm shift with impacts on cybersecurity. Prior to the 2000s, the term “cloud computing” was not even used, but more than $33 billion was spent on cloud services in

the year 2015, making it the most expensive category in IT infrastructure[28]. Mobile device computing has also exploded[29]. Almost 95 percent of Americans own a cell phone, and smartphone ownership increased from 35 percent in 2011 to 77 percent in 2018, according to a Pew Research Center study. Correspondingly, mobile device vulnerabilities have also risen as malicious actors attempt to exploit the mobile devices, connections to the internet, connections to peripherals, and organizational infrastructure.

Clearly, many, if not most, of the activities noted in section III and the technological transformations described early in section IV bear directly on national security. And more change is on the horizon with advances in artificial intelligence and quantum computing. Thus, it is incumbent on the DoD to remain at the edge, if not transcend, the current frontier of cyber capabilities to defend against and even respond to cyber-enabled aggression. To address the cyber domain, section V will explore alternative acquisition constructs that have demonstrated success and other approaches. .

V. ENHANCING CYBER ACQUISITION

This paper demonstrates that many factors, including warfighter needs, adversary progress, and rapid environmental change, demand a faster cyber acquisition process. General George S. Patton is often quoted as saying, "A good plan violently executed now is better than a perfect plan executed next week." General Patton's demand for strong and immediate progress is particularly apropos for cybersecurity. For the United States to simply keep up with cyber change is insufficient. We must lead, developing cutting-edge technology and approaches, despite the breakneck speed of cyber environmental dynamics, because this is the only way to ensure that the United States maintains superiority over our adversaries. The only way to achieve the required advances is to address the acquisition shortcomings. Thus, it is imperative that the United States adopt an approach suitable for rapid cyber acquisition that addresses operational needs.

The previous sections substantiate that cyber needs, posed by the existing environment and threats, mandate a much shorter life cycle than other capabilities. This section will present the recommended policy changes intended to enable cyber acquisition to meet cyber warrior needs. While cyber is not the only acquisition category in which the warfighter needs to outpace the existing acquisition constructs, cyber is at the shortest extreme of the acquisition needs timescale. Accordingly, cyber acquisition is a useful case study for acquisition approaches designed to meet cyber needs.

There is no dispute that the current federal acquisition system is too slow, especially for cyberspace capabilities. DoD leadership has mandated change, Congress wants to see change, and it seems that the DoD is taking steps to enact change. Reference[30] makes this imperative clear—we must "[d]eliver performance at the speed of relevance." However, despite the clear impetus for change, it is difficult to determine how best to change. With a system as complex

as the federal acquisition system, it is challenging to identify the root cause (or root causes) of the problems. Indeed, over 300 studies have been completed in the last 3 decades[9], resulting in hundreds of findings of inefficiency and recommendations for reform.

This section first discusses some of the recognized problems with the current acquisition system, especially with regard to cyberspace; next, discusses some of the promising DoD acquisition pilot programs for delivering innovation more quickly; and, ultimately, makes three broad recommendations for reforming policy to better meet the DoD objective of delivering performance at the speed of relevance, especially in cyberspace. The three recommendations are as follows: (1) Manage rather than avoid risk—especially time-based risks; (2) Delegate authority to the lowest reasonable level; and (3) Treat different problems differently.

A. The Existing System is Flawed

> "Current [DoD] processes are not responsive to need; the Department is over-optimized for exceptional performance at the expense of providing timely decisions, policies, and capabilities to the warfighter[30]."

As the above quote demonstrates, DoD leadership has identified a link between acquisition reform and national security—recognizing that our current processes put the warfighter at risk. However, while the DoD clearly recognizes that there is a problem, determining the necessary reforms to solve the problem is not as straightforward. That's not to say that the DoD and Congress are not trying to identify the problem and implement fixes. Since 1986, over 300 formal studies into the DoD acquisition system have been directed, both by the DoD and by Congress. Some of the findings of these studies are discussed below and represent some of the common complaints about what is wrong with the acquisition system.

For example, in[31], Congress directed the DoD to establish an advisory panel composed of recognized experts in acquisition and procurement policy from the public and private sectors. The Section 809 Panel is charged with reviewing acquisition regulations applicable to the DoD "with a view toward streamlining and improving the efficiency and effectiveness of the defense acquisition process and maintaining defense technology advantage" and providing related recommendations[31]. Thus far, the Section 809 Panel has released one interim report[32] and two extensive volumes of findings and recommendations[33],[34]. A third and final volume is scheduled for release in January 2019. Some of the Section 809 Panel findings are discussed below.

Unfortunately, most of the problems discussed below are not new. This paper cites reports going back as far as 1998, not because there is not more current literature, but because many of the points were as salient then as they are now. Several reports and studies draw similar conclusions. For example,[9] quotes 1982 congressional testimony by Dr. Alice Rivlin (then the director of the Congressional Budget Office) and concludes that "[s]he could give that same testimony today, not change a single word, and still be accurate"[9].

The current system emphasizes rigid adherence to written process and systems over measurable outcomes and speed. This is not surprising where the volume of regulations, restrictions, and documentation is so vast and acquisition personnel are not trained to operational needs[30] because acquisition personnel focus on their area of specialty: the complex acquisition system. This emphasis leads to undesirable outcomes. For example, the "operations community is stuck with dead-end, stove-piped systems which are support nightmares and risk critical missions because, in part, the formal requirements process demands little more than that[35]."

The Section 809 Report makes similar findings in[32], concluding that the acquisition system "creates obstacles to getting needed equipment and services" both by making the DoD an unattractive customer to nontraditional contractors and through "suffocating bureaucratic requirements"[32]. As a result, the panel concluded that equipment needed today "may be either unavailable to the department or egregiously tardy, leading to genuine threats to the nation's security"[32].

Additionally, the complexity of the system is increasing, cost is increasing, and outcomes are declining.[32] cites the 1986 Packard Report finding which essentially provided that excellence cannot be achieved with so many layers of bureaucracy. In response, the Section 809 Panel concluded that, "compared to 1986, there are far more layers at DoD, to include even larger staffs, and too many regulations to count"[32]. The panel found that the "inescapable conclusion when viewing DoD acquisition as a whole . . . is that process wins out over results" and that "too frequently ancillary public policy objectives, often driven by statutes or executive orders, receive equal or greater priority than mission[32]."

Reference[9] reached a similar conclusion, finding that the "DoD's acquisition system continues to take longer, cost more, and deliver fewer quantities and capabilities than originally planned"[9]. Neither the Section 809 Panel nor the Defense Business Board (DBB) found fault in acquisition personnel themselves. Instead, the conclusion reached by both emphasized the unintentional nature of the bureaucratic creep swallowing efficiency and innovation within the DoD[32],[35]. As stated by the DBB, the DoD acquisition system has "unintentionally evolved [to be extremely complex] over many years of well-intended policy and legislative changes"[9].

And, while the concept of bureaucratic delay and complexity impeding acquisitions is not new, the results are magnified when applied to the cyber acquisition landscape, where accelerated technology change highlights DoD inefficiencies. Even in 1998, the DoD recognized the need for improving the speed of technology acquisitions, finding that "[t]oday, to be static is to become obsolete and at risk. Yet DoD management and oversight processes massively impede the dynamism DoD so desperately needs"[35]. This limitation has not changed, as noted in[9], which finds that "[c]yber and IT modernization cannot succeed under the current system due to the accelerated advances of technology and rapidly changing threats to those technologies. Cyber and IT modernization cannot succeed because the cycle times or 'spins' within Cyber

and IT are far shorter than the time scale used by defense acquisition processes"[9].

Unfortunately, knowing that there is a problem and certain underlying causes for the problem is not always sufficient to bring about solution implementation. And, in an acquisition system that is already riddled with regulations, suggesting more regulatory change to address the problem has a high likelihood of unintended consequences. Indeed, if finding a solution was as easy as identifying the problem and a few of the underlying causes, there would not be reports dating back to 1986 describing many of the same issues the DoD acquisition system still faces today. However, as the next section discusses, the DoD is making inroads on pilot programs investigating potential solutions. Indeed, useful ideas gleaned from these efforts inform the policy recommendations discussed at the end of this paper.

B. DoD and Congress Want to Fix the System

In recent years, the DoD and Congress seem to be trying a new and innovative approach to solving the acquisition problem. Rather than just commissioning studies or rewriting regulations, the government has been implementing many different pilot programs for specific types of acquisitions. Essentially, the government is embracing innovation in the very policies that it is using to promote innovation—by trying many different things that might fail at little cost, but that will produce great benefits if they succeed. What's more, it appears that senior leadership is encouraging maximum use of these programs. For example,[36] states, "Our new authorities provide so many tools to be creative; using them should routinely be our default 'fast path.'" One of these expanded authorities, Other Transaction Authorities (OTA), is discussed in more detail below.

OTAs are basically an exception to the entire acquisition system. Whenever something goes wrong, it seems that the government adds more oversight and regulations to ensure that the same thing never happens again. In turn, this additional regulation and oversight slows down everything else in the acquisition system. For this reason, it seems that some of the best solutions are the ones that simply ignore the existing system altogether.[1] OTA is one such authority. While OTAs have been around since 1994[37], Congress increased their availability for use by expanding their applicability in 2015[38] and authorizing simplified follow-on contracts for successful prototypes in 2016[39]. As a result, OTAs have become a new go-to tool in the DoD and have led to rapid acquisitions of needed capability. For example, the USAF used OTA to move certain planning operations from a whiteboard to a software-based solution, saving over $500,000 per day with only a $2.2 million investment[40].

While increased use of OTA seems to be one of the most hope-inspiring changes to government acquisitions in some time, recent events demonstrate that even this innovation authority is still subject to some of the same onerous oversight as more traditional methods. For example, a recent OTA award by the Department of Defense Innovation Unit Experimental (DIUx) for cloud migration services was protested before the Government Accountability Office (GAO)[41]. Generally, GAO does not review OTA agreements. However, in this case, GAO

1 Interestingly,[9] suggests just that – zero-basing the entire system. As nice as it sounds to scrap all existing regulations and oversight and start over from scratch for all acquisition programs, there is a high likelihood of unintended consequences and confusion. Additionally, Congress is unlikely to endorse a solution that substantially limits congressional oversight.

expanded its jurisdiction to include review of whether an agency's use of OTA is appropriate. This decision sets a precedent that OTA agreement awards can be reviewed by the GAO.

Moreover, this GAO decision essentially opens up all OTA awards to bid protests, even by those who were not original bidders on the OTA. And, even when GAO bid protests do not have merit, they generally delay contract award and performance by at least 100 days. Moreover, responding to a GAO bid protest is extremely time-consuming and is likely to set back all other efforts by the government organization that is responding to the protest. In his analysis of the GAO decision, military acquisition policy expert Bill Greenwalt urged the DoD to fight the decision, stating that if the decision is allowed to stand, it will "ensure that China will dominate the future military application of quantum computing, artificial intelligence and machine learning, data analytics, biotechnology, robotics and autonomous operations"[42]. Greenwalt's analysis is based on the willingness of innovative, nontraditional contractors to do business with the DoD if doing so means litigating "one's way through a legal morass and hir[ing] an army of Washington consultants and lawyers to navigate through a constantly changing compliance process"[42].[2]

C. Policy Considerations for Improving Cyber Acquisitions

As the above section demonstrates, the DoD has had some success in streamlining and improving acquisitions. However, there is more work to be done, and the competing priorities of efficiency and oversight will continue to make progress challenging. This section discusses three ideas that can speed up acquisitions today and that can be used to analyze proposals for changes to policy and law to determine whether they are likely to help or hinder innovation and speed up cyberspace acquisitions.

1) Manage Rather than Avoid Risk—Especially Time-Based Risks

a) What's the idea?

Consider time up-front as a real risk (balanced with other risks the acquisition system already considers) and understand that it is better to fail fast and early when your strategy permits it. Risk cannot be fully avoided, so it must instead be managed. Moreover, mitigating every single risk at the expense of speed is not actually a safe option—it is just a very slow failure. This idea is central to[30], which states, "The current bureaucratic approach, centered on exacting thoroughness and minimizing risk above all else, is proving to be increasingly unresponsive"[30]. This idea is also identified in[9], which finds that "[m]ultiple layers of legislation and DoD internal reforms have had the unintended consequence of orienting the process to avoiding mistakes rather than timely delivery of warfighter capabilities at a reasonable cost."

b) What can we do today?

The good news is that there is nothing in existing regulations that explicitly requires that DoD acquisitions be slow and risk-averse. Indeed, there are high-performing organizations

2 The DoD Inspector General is also investigating a different DIUx purchase in an after-the-fact audit[43]. However, this type of audit might be preferable to increased oversight up-front as it allows DoD leadership to fairly assess acquisition risks in a way that does not slow down the acquisition efforts. Nothing that the DoD Inspector General has done here appears to have interfered with the aggressive acquisition schedule achieved by DIUx[44].

within the DoD that move quickly within the existing regulations. One example of this is the Special Operations Forces Command (SOCOM). While the SOCOM acquisition model is widely believed to operate on different principles than the rest of the DoD, this belief is largely unfounded[45]. Instead, SOCOM culture emphasizes speed of delivery within its acquisition process. Additionally, SOCOM "accepts more risk in program execution than is typical of the larger services"[45]. This is at least in part due to the overall small size of most SOCOM projects. Indeed, James Geurts, former SOCOM acquisition executive, is quoted as saying, "Velocity is my combat advantage. Iteration speed is what I'm after, because if I can go five times faster than you, I can fail four times and still beat you to the target . . . That's really what we're going after here"[45]. The USAF seems to be encouraging this as well. A recent memo to the acquisition workforce states, "Prototyping makes discovery your friend, allowing smart risk-taking and design exploration prior to subsequent procurement and fielding decisions. So it's okay to fail here—fully or partially—because subsequent steps provide a safety net. As long as the risk versus reward of pursuing Y makes sense, you're ready for the next step"[36].

c) What should we consider in the future?

Future policy should go further to emphasize risk management rather than risk avoidance. Training and policy should emphasize the tailoring of acquisition strategies to balance risk appropriately to the overall goal and budget. Additionally, a policy should differentiate between by-law requirements and policy requirements so that waivers can be sought as quickly and efficiently as possible when a particular effort would benefit from an exception to policy. As emphasized in[30], the DoD "is committed to changes in authorities, granting of waivers, and securing external support for streamlining processes and organizations" and policy should be written to encourage such requests[30].

2) Delegate Authority to the Lowest Reasonable Level

a) What's the idea?

Aggressively delegate authority to the lowest reasonable levels and design programs to be smaller and thus allow lower delegation. Decision-makers who are closest to the requirements are likely to be in the best position to evaluate available options and strategies and manage overall risk. Additionally, decision-makers at lower levels are more accessible if changes to the acquisition strategy are needed or if requirements change. Not delegating means that people who do not really "get" the problem are often in charge of leading the procurement. This leads to rigidity in requirements. While certain requirements might be considered "nice to have" in the field, they can be treated as deal-breakers for very senior leaders who are leading the overall acquisition.

b) What can we do today?

Senior leaders often have the discretion to delegate but choose not to do so. To enact these

changes today, senior leaders should aggressively delegate within the limits of existing policy. Decision-makers at lower levels should seek delegation from their leadership. Once again, the SOCOM acquisition culture provides a good example. In February 2018, SOCOM acquisition executive James H. Smith explained, "We've been fortunate to have an amazingly consistent leadership philosophy for the last 20 years: Clearly communicate our expectations for risk management and empower the team to make decisions at the appropriate level"[45]. The rest of the DoD should follow that example.

c) What should we consider in the future?

While Congress has created many flexible authorities and funding mechanisms, they are often held only at the highest level of the Services; not delegated or available to lower-level decision-makers; and, thus, inaccessible to operational commanders. Congress could include a requirement that new authorities be delegated to lower levels. Additionally, law and policy could be crafted to carve out clear and mandatory exceptions to oversight and review requirements for certain types of small projects. The Section 809 Panel offered three suggestions for a more agile structure: 1. "[R]epeal statutorily mandated offices"; 2. "[E]liminate military service- and departmental-level oversight that is not value-added"; and 3. "[R]eorganize the acquisition enterprise from program-centric to portfolio-driven"[34].

Finally, Congress and senior leaders are hesitant to eliminate policies that offer oversight into lower-level efforts and safeguards that lower the risk of fraud or simply bad decisions. However, Congress and policymakers should consider implementing oversight mechanisms, such as post-award audits, that do not interfere with efficiency and innovation. While these mechanisms have the disadvantage of not being able to prevent harm from specific acquisitions, they boast more accurate data rather than speculation.

3) Treat Different Problems Differently

a) What's the idea?

While on its face this idea might sound tautological, it is not. The recognition that different requirements have different risks and need different acquisition approaches is not ingrained within the DoD. Interestingly, from 1965 through 1996, DoD IT purchases were treated differently than other requirements[46]. However, beginning in 1996, IT acquisition policies were consolidated with non-IT policies, ironically for the purpose of streamlining the process[46]. The end result is that the DoD purchases software in the same way that it purchases fighter jets, submarines, and janitorial services, and this process can take "7–10 years from planning to delivery"[47]. This finding was echoed by the Section 809 Panel, which found that "[t]he acquisitions system is inflexible and takes a one-size-fits-all approach. Dissimilar products or services are acquired using the same processes"[33]. And, even though acquisition policy is designed to be tailored, studies have shown that "there is a long-standing reluctance to deviate from standard weapon system acquisition processes, and acquisition personnel are not trained or led to differentiate the unique aspects of IT acquisition"[46].

These distinctions go further than just IT versus traditional weapon systems. Within IT itself, there are nuanced differences—for example, the distinction between traditional IT acquisitions and support to cyber operations. As explained by the DBB, while traditional computer applications are "created to perform a function," cyber capabilities "act on and change the functioning of software and hardware"[9]. Accordingly, cyber capability development "is to traditional software acquisition as writing a book is to buying a book"[9]. There are also fundamental differences between acquiring hardware and acquiring software because software generally requires frequent updates and patching, while hardware is largely static after purchase.

b) What can we do today?

Today we can take advantage of existing permissions to tailor acquisitions based on requirements, avoid treating template documents as mandatory, and ask for waivers to mandatory policies that are not value-added for the particular acquisition. For example, [48] makes it clear that acquisition teams should assume that strategies and procedures that are "in the best interest of the Government[,]...not addressed in the FAR, [and] not prohibited by law" or policy represent a "permissible exercise of authority." This idea is supported by[36], which states, "The key is common-sense tailoring to the needs of your prototype and potential subsequent procurement."

c) What should we consider in the future?

Many of the current priorities for reform are seemingly contradictory. For example, in October 2017, Secretary of Defense Jim Mattis sent guidance to all DoD personnel highlighting three lines of effort to enable the DoD to "remain the world's preeminent fighting force[49]. The final line of effort, which was directed at DoD business reforms, included several efforts, such as developing a "culture of rapid and meaningful innovation" and protecting infrastructure[49]. While on its face, these requirements may seem contradictory (How can you move fast if you need to ensure every minor acquisition won't damage infrastructure?), if you apply the above principle of treating different requirements differently, they do not have to contradict each other. The bottom line is this: We cannot fix everything in one unified system. With over 300 studies and hundreds of recommendations, we must recognize that different problems need different solutions that balance different risks. Accordingly, future reform efforts should more explicitly address differing risk profiles, and blanket prohibitions or requirements which apply to all DoD acquisitions should be avoided or eliminated whenever possible.

ACKNOWLEDGMENT

The authors would like to thank Steven Anderson for his vision and leadership, which led to this collaboration out of which our efforts arose.

NOTES

1. Anthe C. et al, "Microsoft Security Intelligence Report." Vol. 21. Redmond VA: Microsoft Corporation, 2016.
2. Microsoft Security, "Microsoft Security Intelligence Report." Vol. 23. Redmond VA: Microsoft Corporation, 2018
3. Council on Foreign Relations, "Cyber Operations Tracker". https://www.cfr.org/interactive/cyber-operations, 2018.
4. Avena, E. et al, "Microsoft Security Intelligence Report." Vol. 22. Redmond VA: Microsoft Corporation, 2017.
5. "The VERIS Community Database." http://veriscommunity.net/vcdb.html.
6. Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections." Intelligence Community Assessment ICA 2017-01D, 2017.
7. Judson, J., "US Army looks to cut typical acquisition timeline in half.", Defense News. https://www.defensenews.com/land/2017/12/07/army-looks-to-cut-typical-acquisition-timeline-in-half/, December 7, 2017.
8. Under Secretary of Defense, Acquisition, Technology, and Logistics, "Performance of the Defense Acquisition System: 2016 Annual Report", Washington, DC: Department of Defense, October 24, 2016.
9. Defense Business Board, "Linking and Streamlining the Defense Requirements, Acquisition, And Budget Processes." Report FY12-02. April 09, 2012.
10. Rogers, M., "Statement of Admiral Michael S. Rogers Commander United States Cyber Command Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities.", https://docs.house.gov/meetings/AS/AS26/20150304/103093/HHRG-114-AS26-Wstate-RogersM-20150304.pdf, March 4, 2015.
11. Adams E., "How on God's Green Earth is the B-52 Still in Service?" Wired. https://www.wired.com/2016/04/gods-green-earth-b-52-still-service/, April 19, 2016.
12. Sari A, "Legal Aspects of Hybrid Warfare." Lawfare, https://www.lawfareblog.com/legal-aspects-hybrid-warfare, . October 02, 2015.
13. Ma A., "China has Started Ranking Citizens with a Creepy 'Social Credit' System - Here's What You Can Do Wrong, and the Embarrassing, Demeaning Ways They Can Punish You.", https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4, April 08, 2018.
14. Mistreanu, S., "Life Inside China's Social Credit Laboratory." Foreign Policy. https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/, April 03, 2017.
15. FireEye, "Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S. Engineering and Maritime Industries.", https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html, March 18, 2018.
16. PwC, "Uncovering a new sustained global cyber espionage campaign." https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html, 2017.
17. Counter Threat Unit Research Team, "BRONZE BUTLER Targets Japanese Enterprises.", https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses, October 12, 2017.
18. Zetter, K., "Revealed: Yet Another Group Hacking for China's Bottom Line." Wired, https://www.wired.com/2016/06/revealed-yet-another-chinese-group-hacking-countrys-economic-bottom-line/, June 14, 2016.
19. Keppler, N., Freifeld K., and Walcott J., "Siemens, Trimble, Moody's Breached by Chinese Hackers, U.S. Charges.", https://www.reuters.com/article/us-usa-cyber-china-indictments/siemens-trimble-moodys-breached-by-chinese-hackers-u-s-charges-idUSKBN1DR26D, November 27, 2017.
20. Graff, G. M., "DOJ Indicts 9 Iranians for Brazen Cyberattacks Against 144 US Universities.", https://www.wired.com/story/iran-cyberattacks-us-universities-indictment/, March 23, 2018.
21. BBC, "Iran blamed for Parliament cyber-attack.", https://www.bbc.com/news/uk-41622903, October 14, 2017.
22. Muncaster, P., "CopyKittens: Report Details Possible Iranian Threat Group.", https://www.infosecurity-magazine.com/news/copykittens-a-new-report-details/, July 25, 2017.
23. Lancaster, T., "Muddying the Water: Targeted Attacks in the Middle East.", https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/, November 14, 2017.
24. Mercer, W. and Rascagneres P., "Korea in the Crosshairs.", https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html, January16, 2018.
25. Wikipedia, "WannaCry ransomware attack.", https://en.wikipedia.org/wiki/WannaCry_ransomware_attack, Accessed November 30, 2018.
26. Symantec, "Ransom.Wannacry.", https://www.symantec.com/security-center/writeup/2017-051310-3522-99, May 24, 2017.
27. Fire Eye, "North Korean Actors Spear Phish U.S. Electric Companies.", https://www.fireeye.com/blog/threat-research/2017/10/north-korean-actors-spear-phish-us-electric-companies.html, October 10, 2017.

NOTES

28. The Economist Intelligence Unit, "Ascending Cloud: The Adoption of Cloud Computing in Five Industries.", https://perspectives.eiu.com/technology-innovation/ascending-cloud-adoption-cloud-computing-five-industries-0, March 01, 2016.
29. Pew Research Center, "Mobile Fact Sheet.", www.pewinternet.org/fact-sheet/mobile, February 5, 2018
30. Mattis, J., Summary of the 2018 National Defense Strategy. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf, 2018.
31. US Congress, "Performance of incurred cost audits (§ 863) & Modifications to the advisory panel on streamlining and codifying acquisition regulations (§883)." National Defense Authorization Act for Fiscal Year 2018. https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf, 2018.
32. Lee, Hon. Deidre A. et al, Advisory Panel on Streamlining and Codifying Acquisition Regulations Interim Report. Arlington, VA: Section 809 Panel. https://section809panel.org/wp-content/uploads/2017/05/Sec809Panel_Interim-Report_May2017_FINAL-for-web.pdf, 2017.
33. Aherm, D. G. et al, Report of the Advisory Panel on Streamlining and Codifying Acquisition Regulations Vol. 1. Arlington, VA: Section 809 Panel. https://section809panel.org/wp-content/uploads/2018/01/Sec809Panel_Vol1-Report_Jan18_FINAL.pdf, 2018.
34. Aherm, D. G. et al, Report of the Advisory Panel on Streamlining and Codifying Acquisition Regulations Vol. 2. Arlington, VA: Section 809 Panel. https://section809panel.org/wp-content/uploads/2018/06/Sec809Panel_Vol2-Report_June18.pdf, 2018.
35. O'Hern Jr., W. L., Defense Science Board Task Force on Open Systems, Washington DC: Defense Science Board. https://apps.dtic.mil/dtic/tr/fulltext/u2/a358287.pdf, 1998.
36. Roper Jr., W.B., "Memorandum for the Acquisition Workforce, Seven Steps for Incorporating Rapid Prototyping into Acquisition." http://acqnotes.com/wp-content/uploads/2018/05/Air-Force-Incorporating-Rapid-Prototyping-into-Acquisition.pdf, 2018.
37. US Congress, "Authority of the Advanced Research Projects Agency to carry out certain prototype projects (§845)." National Defense Authorization Act for Fiscal Year 1994. https://www.congress.gov/103/bills/hr2401/BILLS-103hr2401enr.pdf, 1993.
38. US Congress, "Amendments relating to authority of the Defense Advanced Research Projects Agency to carry out certain prototype project (§812)." Carl Levin and Howard P. ''Buck'' Mckeon National Defense Authorization Act for Fiscal Year 2015. https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf, 2014.
39. US Congress, "Amendments to other transaction authority (§815)." National Defense Authorization Act for Fiscal Year 2016. https://www.gpo.gov/fdsys/pkg/PLAW-114publ92/pdf/PLAW-114publ92.pdf, 2015.
40. Wallace, M., "The U.S. Air Force learned to code-and saved the Pentagon millions." July 05. https://www.fastcompany.com/40588729/the-air-force-learned-to-code-and-saved-the-pentagon-millions, July 5, 2018.
41. U.S. Government Accountability Office, "Decision in matter of Oracle America Inc. (B-416061).", https://www.gao.gov/assets/700/692327.pdf, May 31, 2018.
42. Greenwalt, B., "GAO Decision Threatens US Military Dominance; Reject It.", https://breakingdefense.com/2018/06/gao-decision-threatens-us-military-dominance-reject-it/, June 27, 2018.
43. Inspector General, "Audit of Defense Hotline Allegations Concerning Tanium Software (Project No. D2018-D000CU-0124.00.", https://media.defense.gov/2018/Jul/02/2001938140/-1/-1/1/D2018-D000CU-0125.000.PDF, April 2, 2018.
44. Business Wire, "World Wide Technology Wins First-Ever DIUx Contract to Deliver Endpoint Management Services to Federal Government Agencies.", https://www.businesswire.com/news/home/20171031005858/en/World-Wide-Technology-Wins-First-Ever-DIUx-Contract, October 31, 2017.
45. Capobianco, J., "Strengths and Myths of What Makes Special Operations Forces Acquisition Special.", https://www.army.mil/article/205259/strengths_and_myths_of_what_makes_special_operations_forces_acquisition_special, May 14, 2018.
46. Campbell, W. H. et al., Achieving Effective Acquisition of Information Technology in the Department of Defense. https://www.nap.edu/download/12823, 2010.
47. Schoeni D., "Long on Rhetoric, Short on Results: Agile Methods and Cyber Acquisitions in the Department of Defense." Santa Clara High Technology Law Vol. 1 Issue 3: Article 1, https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1596&context=chtlj, January 1, 2015.
48. Federal Acquisition Regulation. n.d. "Statement of guiding principles for the Federal Acquisition System (§1.102)." https://www.acquisition.gov/far/html/Subpart%201_1.html#wp1130779.
49. Mattis, J., "Memorandum for All DoD Personnel." https://dod.defense.gov/Portals/1/Documents/pubs/GUIDANCE-FROM-SECRETARY-JIM-MATTIS.pdf, 2017.
50. Yasin, R., "Military seeks faster cyber acquisition turnaround", Federal News Network, https://federalnewsnetwork.com/cyber-exposure/2018/04/military-seeks-faster-cyber-acquisition-turnaround/, April 23, 2018.