Accelerating Cyber Acquisitions: Introducing a Time-Driven Approach to Manage Risk with Less Delay

Thomas Klemas,
Sean Atkins, &
Rebecca K. Lively

United States Air Force

Nazli Choucri

Professor
Political Science Department
Massachusetts Institute of Technology

2021

Abstract

The highly dynamic nature of the cyber domain demands that cyber operators are capable of rapidly evolving and adapting with exquisite timing. These forces, in turn, pressure acquisition specialists to accoutre cyber warfighters to keep pace with both cyber domain advancement and adversary progression. However, in the Department of Defense (DoD), a vigorous tug of war exists between time and risk pressures. Risk reduction is a crucial element of managing any complex enterprise and this is particularly true for the DoD and its acquisition program [1]. This risk aversion comes at significant cost, as obsolescence by risk minimization is a real phenomenon in DoD acquisition programs and significantly limits the adaptability of its operational cyber forces.

Our previous research generated three recommendations for reforming policy to deliver performance at the "speed of relevance" [3]. In this paper we focus on one of the recommendations: "Manage rather than avoid risk—especially time-based risks". While this advice can apply to many areas of human endeavor, it has elevated urgency in cyberspace. Incomplete risk metrics lead to overly conservative acquisition efforts that imperil timely procurement of advanced cyber capabilities and repel innovators. Effective cyber defense operations require acquisition risk models to be extended beyond fiscal and technical risk metrics of performance, to include risks associated with the cost of failing to meet immediate mission requirements. This paper proposes a time-shifting approach to simultaneously (a) accelerate capability delivery while maintaining traditional rigor, and (b) achieve optimal balance between fiscal, performance, and time risks.

Keywords: Cyber; acquisition; innovation.

Citation: Klemas, T., Atkins, S., Lively, R. K., & Choucri, N. (2021). Accelerating cyber acquisitions: Introducing a time-driven approach to manage risk with less delay. *The ITEA Journal of Test and Evaluation, 43*, 194–202.

Unique Resource Identifier: https://www.itea.org/the-itea-journal/itea-journal-issue-abstracts/

Version: Author's final manuscript.

Accelerating Cyber Acquisitions: Introducing a Time-Driven Approach to Manage Risk with Less Delay

1 Barriers to Responsive Acquisitions

Cyberspace is a dynamic and uncertain competitive environment that presents unique challenges for defense. Over the last decade in particular, malicious cyber actors have advanced dramatically in sophistication. Co-adaptive threat operators are increasing their reach, frequency of attack, and potential impact [4] [5]. The overall risk is further compounded by the uncertainty that comes with persistent vulnerability. With foundations frequently resting upon technologies that were never designed for security, existing infrastructure still possesses undiscovered vulnerabilities, and new technology brings unknown new avenues for malicious exploitation. For cyber operators, this dynamic and uncertain nature of competition in cyberspace means that rapid technological responsiveness is a necessity. As such, a capable cyber defense fundamentally depends on the ability to rapidly integrate new cyber technologies to out-adapt adversaries. Often the needed capabilities already exist and are employed in the private sector. A key challenge then for military cyber defenders is quick acquisition and adoption of these innovations.

Our previous paper [2] presented three broad recommendations for reforming acquisitions policy to better meet the DoD's objective of delivering performance at the speed of relevance, especially in cyberspace. These are: 1. Manage rather than avoid risk—especially time-based risk, 2. Delegate authority to the lowest reasonable level, and 3. Treat different problems differently. This paper focuses primarily on the first recommendation and proposes specific approaches to improving the speed of cyber acquisitions. It argues that the time dimension of cyber acquisition is a specific risk-to-mission variable that should be better balanced against other existing risk considerations. In other words, sometimes it is okay to risk spending too much or buying something that might not meet high performance standards if it means that cyber operators have access to a technology in time to meet mission needs.

While challenges in acquiring cyber solutions are not unique to the military, the DoD does face distinct obstacles with significant implications for the cyberspace operations community [5] [6]. Chief among these, and as has been described in detail by the Government Accountability Office [30], are current DoD acquisitions processes that are too slow to keep pace with the rapidly evolving threat-vulnerability landscape [2]. Not only do cyber operators need to adapt their tools and infrastructure to address adversaries that simultaneously co-adapt, but they also need to adapt to continual changes in the cyber terrain. For cyber operators defending from within their infrastructure, this means addressing changes in threat actor tools and approaches as well as

managing the evolving vulnerability of defended systems as new vulnerabilities are discovered and useful technology is invented and becomes available. Cyber defenders must also be prepared to address changes in network configuration and the integration of new tools. For cyber operators defending forward in gray or adversary red space or conducting Offensive Cyberspace Operations, this means overcoming challenges or quickly seizing opportunities associated with changes in adversaries' capabilities and systems [31].

From this perspective, acquisitions are about more than simply equipping cyber operators with effective tools. they are an extension of combat function, a form of movement and maneuver, and the current system is often too risk- constrained to enable forces to move at the speed their mission demands [7] [2]. The processes in place to address technical and fiscal risk have actually raised risk in terms of capability gaps that increase vulnerability and reduce opportunity. They have also created barriers to entry for innovators, for instance in dissuading smaller industry innovators from contributing to the military's capability. To be sure, Congress and the DoD have made great strides in the past several years to address some of these issues and numerous limited authorities and pilot programs are currently available. However, in many cases identifying available programs and exceptions is itself a barrier to cyber acquisition.

DoD's traditional risk management guidance is founded on sound principles for mitigating risks to cost, schedule, and performance [8]. When addressed in these types of risk management guides, time related "costs" are primarily concerned with program costs due to schedule over-runs. While important, this approach was built on the assumption that the acquisition process will begin sufficiently in advance of the warfighter's time of need and neglects to consider that the time of need could be as consistently close as it is in cyberspace or that the mission costs associated with failing to meet the time of need might be unacceptable from a holistic perspective.

We proceed as follows: Section II reviews the historical acquisitions and risk management processes. Section III identifies and examines the shortcomings of traditional processes given the dynamic environment of cyberspace operations and the imperatives of cyber warfighter needs. Section IV proposes alternative approaches for managing the time factor in risk considerations. Finally, section V concludes by highlighting the advantages of time-focused risk management to accelerate and sustain the DoD's competitive advantage in cyberspace.

2 Traditional Acquisition Risk Management

Defense acquisitions are largely guided by a hierarchical framework of regulations, offices, and processes, many aimed at risk reduction. At the top is the Federal Acquisitions Regulation (FAR) with further specialization accomplished by the Defense FAR Supplement (DFARS). Each military branch also has a further supplement, for example the Air Force FAR Supplement (AFFARS) and the Army FAR Supplement (AFARS). Additionally, the DoD 5000 series of regulations covers program management to include acquisitions. Each military service has also

produced specific regulations to guide contracting and yet further guidance might come from the command level (often at multiple echelons of command). The Defense Acquisition System also involves numerous offices with distinct authorities: Program Executive Officer (PEO), the Component Acquisition Executive (CAE), Defense Acquisition Executive (DAE), Procuring Contract Officer (PCO), Head of Contracting Activity (HCA), Senior Procurement Executive (SPE), Defense Contract Management Agency (DCMA) [8], and others. There is also the Joint Capabilities Integration and Development System (JCIDS) that is governed by the Chairman Joint Chiefs of Staff Instruction 3170.01 series and the JCIDS manual. It involves users, service chiefs, the Vice Chairman of Joint Chiefs of Staff, and the Joint Requirement Oversight Council (JROC) [9].

There are customizations depending on the acquisition category, cost, and tailoring, but, from the broadest perspective, the acquisition process itself consists of five phases [32]: (i) material solution analysis, (ii) technology maturation and risk reduction, (iii) engineering and manufacturing development (iv) production and deployment, and (v) operations and support, although Accelerated Acquisition Programs merge phases 2 and 3. Throughout these phases, there can be up to four decisions points: (a) material development decision, (b) capability development document, (c) development request for proposal release decision, and (d) full rate production decision or full deployment decision. In addition to the decision points, there are 3 milestone decisions: (i) milestone A, (ii) milestone B, and (iii) milestone C, although Accelerated Acquisition Programs can combine milestone A and B. Beyond the phases, decision points, and milestone decisions, there can be numerous major reviews that might include a preliminary design review, critical design review, production readiness review, initial technical review, alternative system review, system requirements review, system functional review, integrated baseline reviews, test readiness review, flight readiness review, system verification review, functional configuration audit, technology readiness assessments, operational test readiness reviews, physical configuration audit, full-rate production decision review, and in-service review.

More specific to Information Technology (IT) and cybersecurity, the DoD Risk Management Framework (RMF) outlines the process for identifying, implementing, assessing, and managing cybersecurity capabilities and services. It uses a risk-based approach to cybersecurity, leveraging security controls and authorizations of operation of Information Systems (IS) and Platform Information Technology (PIT) systems. However, while cyber risks are addressed in the RMF, the processes are aimed primarily at incorporating cybersecurity concerns “early and robustly in the acquisition and system development life cycle” [11].

In short, the Defense Acquisitions System involves a complex web of regulations, guidance, processes, reviews, decisions, and approvals that often prioritizes management of fiscal and performance risk over speed of delivery. As a result, the sheer magnitude of effort involved in the steps summarized above is daunting, and the system is far from being able to deliver capabilities in sufficient time to allow cyber operators to out-adapt threat actors.

Furthermore, the traditional system also represents a powerful barrier to entry for non-traditional innovators, such as start-ups or technology companies outside the established defense contractor community. Because leading edge cyber capabilities are often developed in these outside commercial ecosystems, the military loses out on leveraging them. A GAO report for the US Senate Armed Services Committee titled, "DOD Is Taking Steps to Address Challenges Faced by Certain Companies" [12] highlighted some of these challenges. It cited "[c]omplexity of DOD's process", "[i]ntellectual property rights concerns", "[u]nstable budget environment", "Government-specific contract terms and conditions", "long contracting timelines", and "inexperienced DOD contracting workforce" as barriers to innovation. In interviews with 12 companies that generally do no business with the DOD, the report found that it took one firm 25 full time employees, 12 months and millions of dollars to prepare a proposal for a DOD contract. In contrast, it took the same company just three part time employees, two months, and only thousands of dollars to prepare a commercial contract for a similar product. The GAO report identifies a variety of additional barriers and delaying elements that illustrate how burdens of time are embedded in the contractual process. In some cases, the time delay amounted to years and the costs were in the hundreds of thousands and even millions of dollars. Beyond the fact that the current process "creates obstacles to getting needed equipment and services", there is a significant potential to curtail participation by smaller, more agile, and more innovative contractors as a result of "suffocating bureaucratic requirements" [12].

A number of efforts have aimed to reform or adjust the Defense Acquisitions System to address these challenges, setting the foundation for potential improvement. The Office of the Secretary of Defense's "The New DoD Systems Acquisition Process" discussed the 2001 overhaul of the DoD 5000 series of regulations [13], addressing numerous problems with the earlier 1996 policy. The document describes six traditional acquisition models [14] that could be tailored to best suit specific needs, and these models include two variants: the "Defense Unique Software Intensive Program" and the "Accelerated Acquisition Program" [15] that were designed for use "when technological surprise by a potential adversary necessitates a higher-risk acquisition program." Quite recently, the DoD instruction on "Urgent Capability Acquisition" [33] provides updated guidance on an approach to speed critical operational capabilities to the warfighter in less than 2 years. Despite this attempted progress, employment of such approaches have thus far not proven to be readily accessible or fast enough for the operational cyber community.

Regulations and guidance have also permitted tailoring of the acquisition process for streamlining and increased flexibility when necessary [16]. For instance, Under Secretary of Defense for Acquisition, Technology, and Logistics Frank Kendall's Better Buying Power (BBP) 2.0 implementation directive advises that "the first responsibility of the acquisition workforce is to think and not to automatically default to a perceived 'school solution'" [17]. The latest version, BBP 3.0, continues to press the professional acquisitions workforce, allowing (even encouraging) program managers to customize regulatory-based reviews, processes, and information requirements to accommodate the unique characteristics of a program while still meeting existing

regulations' intent [18]. The extent to which programs take advantage of opportunities to tailor processes and documentation is not clear, but anecdotal evidence suggests that tailoring is far more limited in practice than this directive might indicate.

The Institute for Defense Analysis studied efforts to accelerate acquisitions, presenting their research in a report titled "Assessment of Accelerated Acquisition of Defense Programs" [19]. The report described how examples of acceleration success often involved direct intervention and even significant hands-on management by high-level leadership (to include the Secretary of Defense), excellent Congressional support, and great urgency of need (war time). Most of these programs, while extremely rapid relative to standard processes, are much larger in scale and in duration than the agile cyber acquisitions that the operational cyber community requires. Although the projects considered exhibited a strong success rate, their scale and "high profile" indicate that the approaches utilized may not be accessible for the operational cyber community.

Other Transaction Authority (OTA) Agreements can be utilized to accelerate and bypass some of the burden of the traditional acquisition process. As the FAR does not apply to OTA Agreements, they also enable research and prototyping activities with significant reduction of process requirements and extensive ability to customize capabilities. The streamlined process permitted by OTA can also make it easier to work with smaller entities that do not typically work with the government. However, these authorities are geared toward research and development efforts, not traditional procurement. In short, while efforts at acquisition reform and tailoring of traditional processes seem to address time considerations in risk management, these approaches often aren't utilized, are sometimes available only in limited pilot programs, and are not readily accessible to the operational cyber community. First, process exceptions are generally restricted to research activities. Second, high level leadership intervention is required to break risk-aversion barriers and this approach is not scalable to most efforts [20]. Third, the acquisition program managers that can customize risk management tools are often focused on the risks associated to the program, which are not always aligned with real-world operational risks [20].

The result is that the current acquisition system's process focus on eliminating risk to cost and performance leaves time-imposed risks to the mission largely unaddressed. Further, key innovators within the commercial sector continue to self-select out of competition for government contracts. This reality is especially significant for operations in cyberspace [21]. As the Defense Business Board notes, "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" [22]. The operational cyber community remains hampered by the pace of acquisitions. The next section builds on these foundations and presents an approach to enable increased emphasis on management of time-based risks that may provide a path toward.

3 Approaches to Manage Time Components Of Risk

So far we highlighted how traditional acquisition risk reduction mechanisms require extensive investments of time, and how they tend to increase the time-dependent risks associated with not delivering critical cyber capability on short order. In our previous paper [2], we put forth several key policy recommendations to address shortcomings of the traditional acquisitions process for cyberspace operations. In particular, we introduced a novel approach that considered time up-front as a real risk to be balanced with the other risks the acquisition system already considers. This approach would allow responsive and early iteration when the operational environment and strategy permit. Risk cannot be fully avoided, so it must instead be managed. This section examines specific ways to do so.

It is imperative to consider time as an increasingly important element of the acquisition system's risk calculus. This is clearly reflected in leadership statements and guidance. For instance, the DoD National Defense Strategy describes how the "current bureaucratic approach, centered on exacting thoroughness and minimizing risk above all else, is proving to be increasingly unresponsive," imploring that we must "[d]eliver performance at the speed of relevance" [24]. Similarly, the Defense Business Board [25] opined 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."

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 [2] [14]. The Section 809 panel report conclusion stated that, currently, capabilities "may be either unavailable to the department or egregiously tardy, leading to genuine threats to the nation's security [14]." As described earlier, this brings with it significant implications for competitive interaction in cyberspace.

Additionally, as indicated by the National Defense Strategy [24], many of the limitations of the current acquisitions are intertwined. Thus, although this paper focuses on the necessity that we accept and manage additional technical and fiscal risk in order to limit time-induced risks – other options such as delegating authority to lower levels and treating different problems differently are also reasonable approaches to trim the "current bureaucratic approach" [26] while, at the same time, elevating time-induced risk priorities by accelerating the process. However, cost and performance risks are still important and many would balk at completely eliminating or largely de-emphasizing processes meant to address these risks. A rushed capability that is costly and fails to perform as needed is just as undesirable as one that is not delivered at the speed of relevance. Thus, we conclude that in many cases it is necessary to harmonize the traditional risk management processes with more agile approaches to accelerate cyber acquisitions, reduce time-based risks,

and realize a more responsive posture for cyberspace operations. A related motivation to seek a new approach for cyber acquisitions is to reduce the barrier to entry for non-traditional commercial innovators that already have a proven track record for agility.

To achieve the delicate, but important, balance between technical, fiscal, and time-based risk management, we propose a time shifted data-driven approach. Instead of ensuring certain risk management and acquisition process constraints are satisfied at every specified point in time, the idea is to satisfy these constraints in a statistical sense over a longer term perspective. If we adopt this approach, then a number of process activities can be shifted to before or after their current process placement, thereby retaining important technical and programmatic rigor of the traditional acquisition system while allowing flexibility that accelerates operationally necessary capabilities. Program managers, and contracting professionals can still reduce risk by considering and utilizing these step informally during the acquisition, but the more time consuming, formalized process can be time-shifted to a post-purchase, auditing stage to maximize speed of delivery. No approach is perfect. We understand that a consequence of shifting risk reduction processes is that there will occasionally be purchases that fail to fully address needs and delaying some acquisition process elements might introduce more risk than the time that they take to implement, but on average, we hope that the addition of this approach will enable cyber acquisition processes to be better attuned to the need.

We argue that it is possible to shift some process elements backward in time or to perform them in advance or seek exceptions for certain classes of capabilities. In essence, this is equivalent to building tailored acquisitions templates to serve for any future acquisitions that can fit within pre-approved classes. We propose that it is also possible to shift acquisition process elements to later points in time, that is, after a procurement decision. The post-procurement shift can be similar to an auditing function and serve to provide metrics associated with acquisition authorities. This shift is connected to our second previous recommendation [2]: delegating acquisitions to the lowest level possible. To add long-term rigor to the post-decisional auditing shift, metrics can be collected on delegated decision makers to enable statistical performance evaluation. Such considerations point to the possibility of finding ways of constructing flexible but rigorous risk-management processes that operate across a broader span of time. We note that in implementing such a framework, it would be necessary to ensure that the audit itself does not create a culture of risk-avoidance--perhaps by including time from need to acquisition as a post-acquisition metric and recognizing that perfect acquisitions are not possible.

Time shifting of selected acquisition process elements means that those activities no longer perform a time-intensive gating function for a particular program. In the context of our proposed paradigm, shifting selected risk reduction processes until after procurement results in quicker adaptive iteration that comes with fast failure (and thus cost avoidance). It also enables increased statistical data for auditing of procured capability types and acquisitions choices, thus shifting auditing steps from performing a gating function for individual programs to a role of evaluating performance of acquisition personnel or centers in a more time-averaged sense.

Using such an auditing capability, it might also be possible to certify certain acquiring activities as lower risk than others, thus affording them more flexibility. This could be reflected by using the performance statistics of acquisition organizations to identify teams that should be entrusted with additional rapid acquisition authorities (or perhaps selected as locations for various pilot programs). Auditing and evaluations could also determine the level of trust afforded particular acquisition agents and teams, enabling adjustment of their authority based on their recorded history of outcomes. Moreover, agents and teams with poor track records of performance can be identified and selected for additional training or for reductions in rapid acquisition authorities.

A potential approach that time-shifts process elements earlier involves treating certain categories of cyber acquisitions as general classes rather than as specific individual requirements. Such a process would then reduce the process burden for a broader swathe of anticipated cyber acquisitions. Blanket purchase agreements have been utilized to address some of these issues and perhaps this concept can be extended and leveraged further to accelerate cyber acquisition. In practice, this sort of approach would reduce time-based risk to mission while also addressing fiscal and performance risk by: (1) limiting bureaucratic process elements for umbrella classes and (2) enabling delegation of specific acquisition decisions to the lower level operational units at a reduced fiscal and performance risk rate.

There are a number of potential mechanisms to achieve these goals. Here we note only a few. It may be possible to create a new class of acquisition model, similar to the Major Defense Acquisition Program (MDAP) or Major Automated Information Systems (MAIS), but specifically designed for cyberspace operations timelines. Another mechanism could be to introduce a series of templates that are specifically tailored for types of cyberspace operations acquisitions. Here we must note that these, and other potential approaches, would greatly benefit from training a corps of cyber acquisition professionals that are comfortable with whichever new paradigm is ultimately leveraged. These individuals could be selected from programs that have already shown success in streamlining acquisitions for other programs.

Our previous paper [2] highlighted the growing pressures to speed up cyber acquisitions given warfighter needs, the increasing rate of adversary activity and progress, and the rapid pace of technological evolution. The calls to accelerate acquisitions have been escalating for some time now. Multiple previous National Defense Authorization Acts (NDAAs) specifically request the exploration of new approaches for agile software and cyber acquisition [27] [28][29]. The next section highlights specific candidate processes for time-shifting, focusing on increasing potential innovation.

4 Selected Time-Shift Candidates

To recap, in Section II we showed how traditional acquisitions include many systems and processes intended to reduce technical and fiscal risks to the greatest possible extent, but with

much less emphasis on managing time- based risks. In Section III, we presented time-shifting approaches that may be useful for management of acquisitions in situations where operational time-based risks are important considerations. In this section we explore process elements from the traditional acquisition approach that may be good candidates for time-shifting. Then we suggest some ways to achieve such an objective. Our purpose here is to highlight examples of the overall approach. More specifically, we identify process elements where -- through abbreviating and decoupling -- time-shifting can better balance the risks to cost, schedule, and performance against time-based risk to mission.

First, a number of steps associated with lifecycle supportability are potential candidates. These involve sustainment, lifecycle cost estimations, and consideration of intelligence information requirements. Depending on timing and need these can be abbreviated or decoupled up front and shifted to the right with limited risk imposition to cost, schedule, or performance. The operational capabilities required can often be one-off, short term solutions where future supportability is a non-issue or where the solutions must be customized to the operational objective. If a solution may meet a longer term need, then the supportability may be formally conducted after the initial purchase.

Second, additional candidates can be found in the requirements identification and validation process steps. These involve a structured process for ensuring there is an actual and impactful mission requirement and capability gap to address. These steps can be shifted or eliminated if the operational requirement has been identified at the operational level and the capability type is covered in an umbrella class, as described in section III. This is an especially attractive option in situations where the overall cost of the procurement is low. Some constraints on this flexibility can be introduced, for example, in the amount spent or in follow-up evaluations after implementation to ensure the capability was in fact needed.

Third, requirements due to conditions of vulnerability to cyber-attack present another opportunity. These involve vulnerability assessments that can be costly in terms of time. In many cases, the desired capabilities already have a demonstrated history of security outside of DoD or have been subject to tests that decrease the likelihood of exploitation. Additionally, often there are capabilities that have a demonstrated record of security in the private sector that are needed to replace capabilities that have a demonstrated record of vulnerability in use within the DoD network. In such situations, the time-risk of evaluating the cybersecurity risk may be an even greater risk to the network. These outside evaluations and history or performance can be utilized as indicia of reliability to support a time-shift of the formal DoD evaluation of the procured product.

Fourth, are the analysis of alternatives (AoA) and design process steps. These steps involve analyzing all possible alternatives to buying a new capability and the subsequent solution design process. Depending on timing and need, these can be abbreviated and shifted through delegation. In times of temporal necessity, those closest to the operational level have, in all likelihood, already

conducted at least an informal AoA sufficient to meet the immediate mission demand. Further, much of the quick-turn solutions required already exist in the commercial world and the military just needs to implement them, eliminating the need for design processes.

Importantly, each one of these candidate-types for reducing process burdens provide an opportunity to accelerate cyber acquisition, and also to reduce at least some of the barrier for non-traditional cyber innovators posed by the cumbersome pre-contract processes.

5 Conclusion

In this paper, we propose innovations to the traditional acquisition process that enable more responsive cyber procurement. These are designed to integrate capability delivery time into risk management. The goal is to accelerate cyber acquisition programs to rapidly address vulnerabilities, threats, and opportunities to better meet cyberspace operational needs.

The cyber domain compresses time and shapes risk in powerful and unprecedented ways. Our suggested acquisition process adjustments are designed for these cyber realities and address the need to sustain competitive military cyber performance on a broad scale over long periods of time. Our approach provides the basis for adapting as needed while maintaining the rigor and intent of the existing process, learning and building upon its defining principles. In doing so, it offers a way to manage the joint performance, fiscal, and time risk imperatives. To further improve these acquisition process outcomes, we also suggested training a corps of operational cyber acquisitions professionals.

Acknowledgment

The authors would like to thank Steve Anderson for the vision and inspiration that resulted in this collaboration, out of which our efforts arose.

References

[1] Office of the Under Secretary of Defense for Acquisition Technology and Logistics Washington D.C., Risk Management Guide for DoD Acquisition. Sixth Edition (Version 1.0). Department of Defense (Aug. 2016). http://www.acqnotes.com/Attachments/DoD%20Risk%20Management%20Guidebook,%20Aug%2006

[2] Choucri, N., Klemas T. and Livley, R. Cyber Acquisition: Policy Changes to Drive Innovation in Response to Accelerating Threats in Cyberspace. Army Cyber Institute, West Point. (November 14, 2018). https://www.hsdl.org/?view&did=818911.

[3] Garamone, Jim. DoD Restructures Acquisition, Technology Office to Improve Military Lethality, Speed. DoD News, Defense Media Activity, (Aug. 2, 2017) https://dod.defense.gov/News/Article/Article/1265231/dod- restructures-acquisition-technology-office-to-improve- military-lethality-sp/

[4] Donald Trump, National Cyber Strategy of the United States of America. The White House, Washington D.C., (Sept. 2018). https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[5] National Intelligence Strategy of the United States of America, United States. Office of the Director of National Intelligence, (2019). https://www.hsdl.org/?view&did=820509

[6] Under Secretary of Defense, Acquisition, Technology, and Logistics, "Performance of the Defense Acquisition System: 2016 Annual Report", Washington, DC, Department of Defense.

[7] A Conversation with General John Hyten, Vice Chairman of the Joint Chiefs of Staff.. Center for Strategic and International Studies. (21 January 2020). https://www.csis.org/analysis/conversation-general-john-hyten-vice-chairman-joint-chiefs-staff.

[8] Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs. Office of the Deputy Assistant Secretary of Defense for Systems Engineering. (January 2017). https://www.acq.osd.mil/se/docs/2017-RIO.pdf

[9] Defense Acquisition University. Defense Acquisitions Guidebook. https://www.dau.mil/tools/dag

[10] Carter, Ash. 2019. Inside the Five-Sided Box, Dutton. p. 14

[11] Risk Manage Framework. Last modified November 8, 2018. http://acqnotes.com/acqnote/careerfields/risk-management-framework- rmf- dod-information-technology

[12] Military Acquisitions: DoD Is Taking Steps to Address Challenges Faced by Certain Companies. United States Government Accountability Office. (July 20, 2017). https://www.gao.gov/assets/690/686012.pd

[13] The New DoD Systems Acquisitions Process. Office of the Under Secretary of Defense for Acquisitions & Sustainment. www.acq.osd.mil/dpap/Docs/5000rewritebrief.pdf

[14] Section 809 Panel. Advisory Panel on Streamlining and Codifying Acquisition Regulations: Section 809 Panel Interim Report. (May 2017). https://section809panel.org/wp- content/uploads/2017/05/Sec809Panel_Interim-Report_May2017_FINAL-for- web.pdf

[15] Department of Defense. Enclosure 13: Urgent Capability Acquisition. DoDI 5000.02. Washington D.C.: Department of Defense (January 7, 2015). https://www.dau.mil/guidebooks/Shared%20Documents%20HTML/DoDI%205000.02.aspx#toc285

[16] Defense Acquisition University. Adaptive Acquisition Framework: Tailorable Traditional. https://aaf.dau.edu/aaf/tailorable- traditional/

[17] Kendall, Frank. Better Buying Power 2.0:A Guide to Help You Think. Washington D.C.: Department of Defense. (November 2012).

[18] Kendall, Frank. Better Buying Power 3.0. Washington D.C.: Department of Defense. (September 2014) https://www.acq.osd.mil/fo/docs/betterBuyingPower3.0(9Apr15).pdf

[19] Van Atta, Richard, R. Royce Kneece, and Michael Lippitz. Assessment of Accelerated Acquisition of Defense Programs. Institute for Defense Analysis. (September 2016) https://apps.dtic.mil/dtic/tr/fulltext/u2/1028525.pdf

[20] McKernan, Megan, Jeffery A. Drezner, and Jerry M. Sollinger . Tailoring the Acquisition Process in the US Department of Defense.Rand Corporation. (2015). https://www.rand.org/pubs/research_reports/RR966.html

[21] Department of Defense. Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs. (January 2017), 21. https://www.acq.osd.mil/se/docs/2017-RIO.pdf

[22] Defense Business Board, Report to the Secretary of Defense. Linking and Streamlining the Defense Requirements, Acquisition, and Budget Processes. Report FY 12-02. (2012).

[23] Department of Defense. Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs. (January 2017), 31. https://www.acq.osd.mil/se/docs/2017-RIO.pdf

[24] Mattis, James. Summary of the 2018 National Defense Strategy. (January 2018). http://nssarchive.us/national-defense-strategy-2018/2018-national-defense-strategy-summary/

[25] Defense Business Board. Report to the Secretary of Defense. Linking and Streamlining the Defense Requirements, Acquisition, and Budget Processes. Report FY 12-02, (2012).

[26] Section 809 Panel. Advisory Panel on Streamlining and Codifying Acquisition Regulations: Section 809 Panel Interim Report. (May 2017). https://section809panel.org/wp- content/uploads/2017/05/Sec809Panel_Interim-Report_May2017_FINAL-for- web.pdf

[27] U.S. Congress, House, Committee on Armed Services. H.R.2810 - National Defense Authorization Act for Fiscal Year 2018. 115th Cong., 2017, H.R. 2810, (December 12, 2017). https://www.congress.gov/bill/115th- congress/house-bill/2810/text

[28] U.S. Congress, Senate, Committee on Armed Services. National Defense Authorization Act for Fiscal Year 2017 (to Accompany S.2943). 114th Cong., S.2943, (November 30, 2016). https://www.congress.gov/bill/114th- congress/senate-bill/2943/text

[29] U.S. Congress, House, Committee on Armed Services. John S. McCain National Defense Authorization Act for Fiscal Year 2019. 115th Cong., 2018, H.R. 5515, (August 13, 2018). https://www.congress.gov/bill/115th- congress/house-bill/5515/text

[30] Government Accountability Office. DOD ACQUISITION REFORM: Leadership Attention Needed to Effectively Implement Changes to Acquisition Oversight. Report to Congressional Committees. (June 2019). https://www.gao.gov/assets/700/699527.pdf

[31] Joint Publication 3-12, Cyberspace Operations. (June 8, 2018). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

[32] Defense Acquisition University, Defense Acquisition Life Cycle Wall Chart v1.3. (Feb 13 2019). https://www.dau.edu/tools/Lists/DAUTools/Attachments/203/Defense%20Acquisition%20Life%20Cycle%20Wall%20Chart%20v1. 3.pdf

[33] Department of Defense, Office of the Under Secretary of Defense for Acquisition and Sustainment, Urgent Capability Acquisition, DoD Instruction 5000.81, (December 31, 2019)