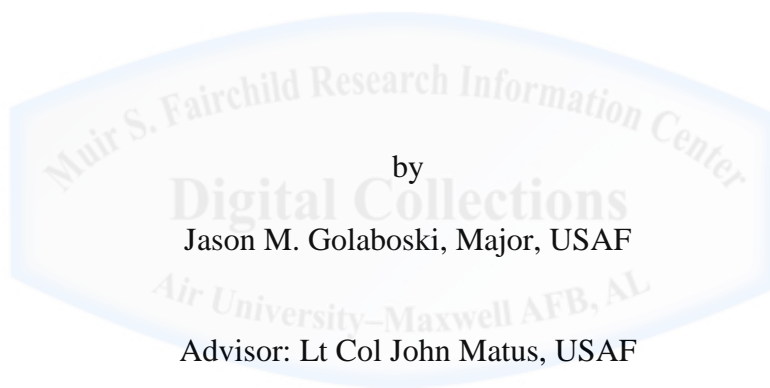


AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

DOD WEAPONS SYSTEMS ACQUISITION:
A CYBER DISCONNECT

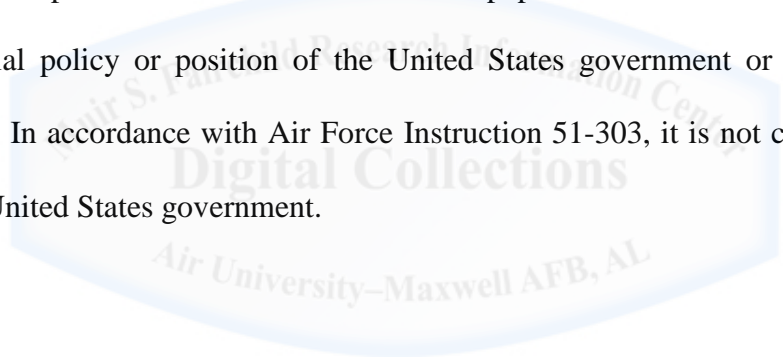


Maxwell Air Force Base, Alabama

14 December 2011

DISCLAIMER

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

A large, light blue, semi-transparent watermark is centered on the page. It features a hexagonal border. Inside the hexagon, the text "Air S. Hall Research Information Center" is written in a curved path at the top. In the center, the words "Digital Collections" are displayed in a large, bold, sans-serif font. At the bottom, the text "Air University—Maxwell AFB, AL" is written in a curved path.

ABSTRACT

The existing DoD acquisition process is too laborious and too cumbersome to meet the dynamics of evolving technology – technology which continuously drives the need for timely weapons systems deliveries, modifications and upgrades. Further, the nature by which military operations are conducted is constantly evolving. With the recent shift from conventional force-on-force operations to asymmetric tactics, the demand for information superiority from both state and non-state actors has become increasingly widespread. Within this new paradigm, cyber has emerged as a developing battle-space, equivalent to those of air, land, sea, and space – rendering it limitless in terms of both global opportunity and global vulnerability. Perhaps most important to consider is that within cyberspace, we are always behind the power curve, constantly chasing advancing software complexity and progressing adversary tactics and techniques for employing and defending against attacks.

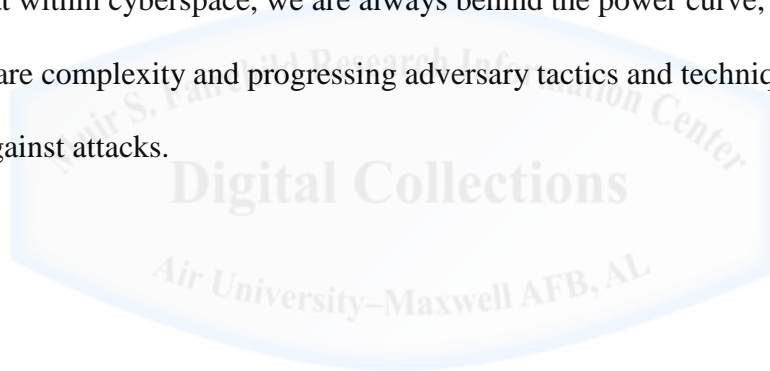


TABLE OF CONTENTS

Disclaimer	2
Abstract	3
Contents	4
Figures	5
Section 1: INTRODUCTION	6
Section 2: TECHNOLOGY AND THE THREAT	9
Section 3: UNDERSTANDING THE DEFENSE ACQUISITION PROCESS	11
Section 4: WHAT'S WRONG WITH THE CURRENT SYSTEM	14
Next-War-Itis	
Pursuit of the Ultimate Weapons System	
Software Complexity	
Planning, Programming, Budgeting, Execution and Government Oversight	
Collaboration	
Section 5: RECOMMENDATIONS TO FIX THE CYBER DISCONNECT	18
Model It After JIEDDO	
Reorganize To Increase Efficiency	
Budget Flexibility and Culture Change	
Implement an Evolutionary Approach to Increase Fielding Speed	
Conclusion	23
Endnotes	24
Bibliography	26

FIGURES

Figure 1 – DoD Decision Support Systems

Figure 2 – Defense Acquisition Milestones

Figure 3 – Joint Improvised Explosive Device (JIED) Capability Approval and Acquisition
Management Process



INTRODUCTION

“This era will be one of accelerating technological change. Critical advances will have enormous impact on all military forces. Successful adaptation of new and improved technologies may provide great increases in specific capabilities. Conversely, failure to understand and adapt could lead today’s military into premature obsolescence and greatly increases the risks that such forces will be incapable of effective operations against forces with high technology.”¹

Chairman of the Joint Chiefs of Staff
Joint Vision 2010

Imagine a scenario where the United States and China have exhausted all diplomatic and economic instruments of power, leaving military action as the last resort. On behalf of its global national security interests, the United States is forced to attack China on its own territory – a massive, well integrated region that includes a highly dynamic Integrated Air Defense System (IADS). Consider that the United States and its Allies have relied, since the end of the Cold War, upon the strategy to quickly overwhelm an adversary’s IADS using the ability to deliver massed precision firepower from the air as the weapon of choice.²

The reality of the situation, however, is that the rapid evolution of IADS software technology renders the majority of United States’ countermeasures useless. According to research, the United States Air Force (USAF) combat aircraft fleet, and all of the United States Navy (USN) combat aircraft fleet, will be largely ineffective against an IADS constructed with technology available today from Russian and Chinese manufacturers (e.g. systems currently deployed by countries such as China, Iran, Venezuela, and other nations with poor relationships with the Western alliance).³ If flown against such IADS, United States legacy fighters from the F-15 through to the current production F/A-18 E/F would suffer prohibitive combat losses attempting to penetrate, suppress or destroy such IADS.⁴ Further, most sources agree that until the USAF deploys a significant number of Next Generation Bombers, the only aircraft types in the existing United States arsenal capable of penetrating, suppressing and destroying the Chinese

IADS are the B-2 Spirit and the F-22 Raptor – though projections estimate that the current F-22 fleet of 187 aircraft would need to increase to between 500-600 aircraft (currently costing ~\$140M/aircraft) to provide a credible capability to conduct a substantial air campaign.⁵

However, despite the prospect of employing a fleet worthy of carving large enough holes in the Chinese IADS system to allow such an attack, the reality is that today's fiscal constraints prevent this kinetic option from being considered a valid course of action (COA). With that said, it is vital to understand that the Chinese IADS and Command and Control (C2) systems are comprised of interconnected networks, computers, servers, routers, and switches – making them vulnerable and susceptible to cyber attack. Combined with an increasingly reduced capability to attack such targets by traditional kinetic means, cyber provides the alternative.

Now consider that technology in the 21st century is growing at an alarming rate, and that it takes years to develop weapons systems using the traditional Defense Acquisition System. Thus, even attempting to blend a cyber COA with the current acquisition model leaves the United States playing catch-up to evolving Chinese technology. According to Army General Edward Hirsch, “The process (Defense Acquisition) is intentionally long and iterative, each step aimed at reducing the risk of failure and increasing the likelihood of meeting cost, schedule and technical promises.”⁶ Whereas one might expect the results of this process would be the delivery of successful weapons systems, Hirsch finds the opposite. “It now takes years – more than 110 months on average – for a major military program, once funded, to wend its way through this process. While the weapons program makes its way slowly and methodically through the nine steps (strategy development through system build through operations and sustainment), the defense strategy that gave rise to it moves on in response to new threats, shifting geopolitics, and changing imperatives.”⁷

Research Intent

The intent of this research is two-fold: first it will highlight the impediments within the Defense Acquisition System to demonstrate that today's model fails to meet the speed of cyber need (the disconnect); and second, it will recommend process improvements to ensure the DoD can deliver timely, effective capabilities when and where warfighters need them most (model it after JIEDDO).

This research will attempt to provide perspective from several different angles. First, it examines the limiting factors (LIMFAC) within the current Defense Acquisition System from the desire to design and construct the ultimate weapons system; to the fallacies within the Planning, Programming, Budgeting and Execution (PPBE) process; to how bureaucracy factors into what is supposed to be an apolitical environment. From a cost, schedule, and performance standpoint, should the DoD continue down the path of developing grand-scale, complex attack systems that double as deterrents, or should we examine more simplistic and reliable approaches?

Additionally, how much does programming, government oversight, and poor collaboration across the DoD and external agencies delay major weapons systems development, and how much disconnect does that present within the new cyber landscape? Lastly, this research provides recommendations for how the DoD might embrace a more flexible, rapid approach to enable the USAF to fly, fight, and win in cyberspace.

TECHNOLOGY AND THE THREAT

The world we live in today is high-paced, highly-technological, and highly-interconnected. Dr. Kamal Jabbour claims, “Rapid technology advances over the past several decades and the proliferation of computers into weapons systems has created a dichotomy of net-centric military superiority and a commensurate reliance on technology.”⁸ More so than ever before, the weapons systems we design are interconnected – critically dependent upon the information flow from external air, ground, space, and/or communications systems to operate. In conjunction, an analysis of the history of technology shows that differing from what one might expect, researchers anticipate that we “won’t experience 100 years of progress in the 21st century, it will be more like 20,000 years of progress.”⁹ Within a few decades, “machine intelligence will surpass human intelligence, leading to technological change so rapid and profound it represents a rupture in the fabric of human history.”¹⁰

The Threat

Similarly, it is critical to comprehend the tie between rapidly evolving technology and the threat Computer Network Operations (CNO) pose to the national security of the United States. CNO are deliberate actions taken to leverage and optimize networks or, in warfare, to gain information superiority and deny the enemy an enabling capability.¹¹ According to Joint Pub 3-13, Computer Network Attacks (CNA) are actions taken to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers or networks themselves.¹² Cyber attacks are used to cripple an adversary’s ability to operate effectively, while simultaneously protecting and preserving friendly battle-space superiority. State-level attacks can be employed to impose grave damage to a nation’s critical nuclear, electrical, communications, transportation, financial, and/or military systems. At a recent meeting of cyber

security experts held in Washington D.C., Richard Clarke, former cyber security advisor to President George W. Bush, stressed that, “Any National Security Advisor worth his or her salt would warn the president that we could not attack other countries because so many of them – including China, North Korea, Iran and Russia – could retaliate by launching devastating cyber attacks that could destroy power grids, banking networks or transportation systems.”¹³ Further, “Failure of one or more of these infrastructure components would have significant implications for our nation’s security and our way of life. In certain cases it could even result in mass casualties among the civilian population. For the military, the loss of its ability to communicate via satellite, to use the Global Positioning System (GPS), or to gather and fuse intelligence using cyberspace would be devastating as well. The potential loss of these capabilities could change the way America wages war – and not for the better.”¹⁴ This highlights the unmistakable tie between cyber as today’s most critical emerging threat; the need for (development) speed to remain ahead of the technology curve; and the disconnect imposed by using the traditional Defense Acquisition Process.

UNDERSTANDING THE DEFENSE ACQUISITION PROCESS

“There isn’t really an effective process for getting from the National Security Strategy to any specific acquisition. There is an intellectual disconnect. The National Security Strategy looks 4 years ahead and deals with the problems of today. The acquisition process, however, looks out 10 to 15 years.”¹⁵

Robert C. Rubel

Dean of Naval Warfare Studies, Naval War College

2008 Interview on the Weapons Acquisition Process: An Intellectual Disconnect

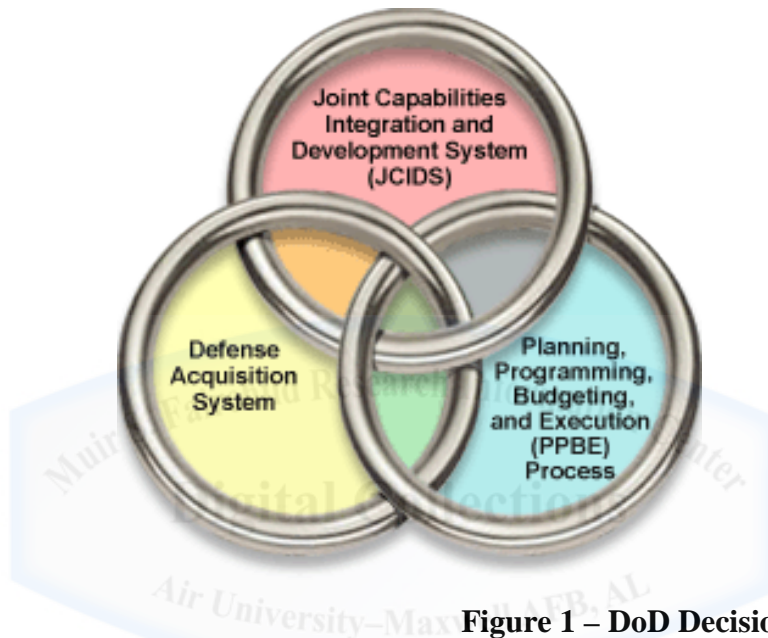


Figure 1 – DoD Decision Support Systems

Reference: Defense Acquisition Portal, Big “A” Concept, 6 December 2011

There are three key processes in the DoD that must work together to deliver the capabilities required by the warfighter: the requirements process; the acquisition process; and the PPBE process (see Figure 1).¹⁶ In broad terms, the purchase of a good or service by the DoD is defined as a procurement. In contrast, the term acquisition applies to more than just the purchase or procurement of an item or service – it encompasses the design, engineering, construction, testing, deployment, sustainment, and disposal of weapons and weapons systems.¹⁷

In accordance with validated Chairman of the Joint Chiefs of Staff (CJCS) objectives, DoD Directive 5000.01, DoD Instruction 5000.02, and the Joint Capabilities Integration and

Development System (JCIDS) serve as the foundational processes utilized by the DoD to acquire weapons systems. JCIDS was developed as a more efficient process for the DoD to identify capabilities gaps, define requirements, and to determine which materiel or non-materiel solution is best suited to fulfill the operational needs of the Combatant Commander (CCDR).

Additionally, DoD Directive 5000.01, the Defense Acquisition System, provides the policies and principles that govern the defense acquisition system, while DoD Instruction 5000.02, Operation of the Defense Acquisition System, establishes the management framework that implements these policies and principles.¹⁸ Lastly, the PPBE process serves to provide the CCDR the best mix of forces, equipment, and support within fiscal constraints – to include developing and finalizing the entire DoD budget for all acquisitions.¹⁹

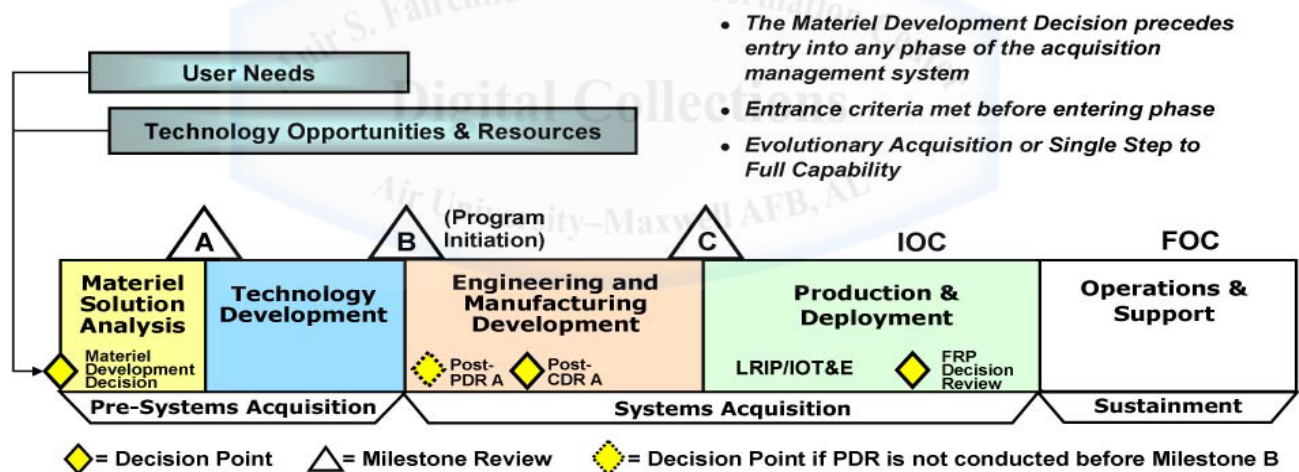
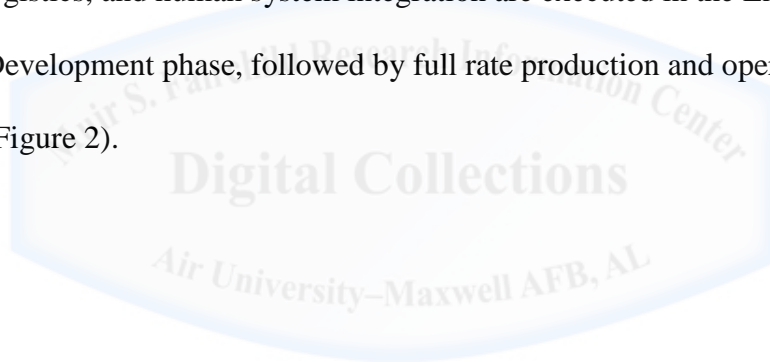


Figure 2 - Defense Acquisition Milestones
Reference: DoD Instruction 5000.02, 8 December 2008

The acquisition process commences with a Materiel Development Decision (MDD). This is the point at which recommendations are made to the Joint Requirements Oversight Council (JROC), and where Services present their requirements in the form of an Initial Capabilities Document (ICD). The ICD includes a preliminary Concept of Operations (CONOPS); a

description of the capability needed; the operational risks; and a justification to the JROC for a materiel solution (physical systems development) over a non-materiel solution (tactics, techniques, procedures, or training).²⁰ Within the Materiel Solution Analysis phase the Milestone Decision Authority (MDA) assesses an Analysis of Alternatives (AoA), or potential materiel solutions, to satisfy the requirements specified in the ICD. This analysis provides a thorough examination of critical technology elements, materiel solutions, integration risk, manufacturing feasibility, and overall life-cycle costs associated with respective development options.²¹ After the Materiel Solution Analysis phase, the Technology Development phase centers on reducing technology risk and prototype development. Systems development and integration; operational supportability; logistics, and human system integration are executed in the Engineering and Manufacturing Development phase, followed by full rate production and operations in the latter two phases (see Figure 2).



WHAT'S WRONG WITH THE CURRENT PROCESS

“DoD’s processes for setting requirements, providing funding, and managing acquisitions do not work together, resulting in a disconnect between the programs that are started and the funding that is available; DoD’s process for determining weapon system requirements (JCIDS) does not evaluate projects from a joint or department-wide perspective and does not have the flexibility to quickly respond to emerging warfighter needs; and DoD’s process for funding programs (PPBE) creates an unhealthy competition for funds that encourages sponsors of weapon system programs to pursue overly ambitious capabilities and to underestimate costs.”²²

Government Accountability Office (GAO)
2009 Recommendations to the House Armed Services Committee

Next-War-Itis

There is continued concern that the United States places a higher value on developing capabilities to win future campaigns than it focuses on today’s issues. Former Secretary of Defense Robert Gates coined the term “next-war-itis,” and claims that his own agencies pressed for the creation of complex and expensive machinery for possible conflicts far into the future, but were not sufficiently attentive to providing affordable weapons that the military can use right now.²³ This is obviously extremely concerning for the cyberspace community, as weapons systems relevance is rapidly made obsolete by exponential technology growth – and the longer systems take to get fielded, the longer vulnerabilities are allowed to persist.

Pursuit of the Ultimate Weapons System

Using the metaphor of a Star Wars Death Star, Lt Col Dan Ward avows that “any enormous project that is brain-melting complex, ravenously consumes resources, and aims to deliver an undefeatable ultimate weapon is well on its way to becoming a Death Star, and that’s not a good thing.”²⁴ In his article, Ward supports the argument that large, complex weapons systems typically have critical vulnerabilities that if discovered and exploited, jeopardize entire systems. He also addresses the issue of operational performance – which is typically limited and

poor. He states that time and again, war-winning weapons tend to be simple, inexpensive, reliable and small.²⁵ Whereas the ultimate weapons system may be designed as a deterrent to “intimidate opponents into submission,” or to constrain an adversary’s attack; the smaller “finesse” weapons earn their keep by remaining useful and practical.²⁶ Such is true within the cyber domain.

Capabilities shortfalls in support of recent CDR requests from Iraq and Afghanistan drive a demand for improvements to the long-standing weapons system acquisition process. According to the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD AT&L), due to the evolution of cyber warfare missions, the speed of requirements definition, technology and capability development, and integrated testing, is critical to success.²⁷

Software Complexity

Software may be the most critical component within today’s weapons systems – and most often presents the highest risk to an acquisition program’s cost, schedule and performance. In a 2007 GAO report to Congress, Katherine Schinasi noted that new military systems are more technologically complex than ever before, and they rely increasingly on unproven technologies.²⁸ She asserts, “Defense programs are now so massive and so fanciful we don’t know how to get there.”²⁹ Unfortunately this is true. Too often, weapons acquisitions tend to be technology driven, favoring higher risk, and cutting-edge technologies in search of the higher pay-off. Robert Glass, visiting professor at Griffith University in Australia, agrees and discusses that we “undertake giant, unique developments that take years of effort and hundreds of people to produce.”³⁰ This in turn leads to future problems within the acquisition process. Because of the complexity of the systems, and the unprecedented software that comprises their core, Glass asserts that we cannot test under actual operational conditions, nor in the environments they are intended to be used in.³¹ Thus when testing is insufficient, a system cannot enter into production – rather it is thrust back

into a process of modification and re-test until either sufficiently reducing operational risk or actually meeting technical thresholds – all of which continue the cycle of chasing evolving technology.

Planning, Programming, Budgeting, Execution and Government Oversight

A 2009 GAO report to the House Armed Services Committee stresses that the DoD's process for funding programs (PPBE) creates an unhealthy competition for funds that encourages sponsors of weapon system programs to pursue overly ambitious capabilities and to underestimate costs.³² According to Joint Vision 2010, the current United States strategic vision relies almost exclusively on software technology – a reliance which emphasizes the necessity to pursue technology driven solutions. Though in many situations a practical solution may suffice, “To maintain our competitive edge and military superiority, software-intensive defense systems often include performance requirements and design features demanding the acquisition of unprecedented technologies.”³³ Despite what one may argue is the right thing to do, in these situations there is little incentive for a program manager to admit to high program risks during the acquisition process until absolutely necessary – for fear that reporting issues make programs vulnerable to criticism, jeopardizes funding, and expedites cancellation.³⁴ Similarly, the heavy scrutiny imposed by Service executives, the Office of The Secretary of Defense (OSD), independent audit agencies, and Congress encourage overly optimistic cost, performance, and schedule estimates.³⁵ Not only do realistic cost or schedule estimates serve as a barrier into program entry, but approved budgets are singularly focused and significantly limit a program manager's flexibility to meet dynamic requirements – requirements that evolve and emerge as critical to the warfighter. In told, these problems within the PPBE process are widespread, growing, and detrimental to technology-based acquisitions.

Collaboration

As much as in any other warfare domain, cyber weapons systems development demands extensive collaboration across the Services, national agencies, and industry.³⁶ Despite the necessity to share knowledge of potential cyber threats across the enterprise, however, the entities involved in today's cyber fight remain extremely stove piped. Unfortunately to this day, only a select number of individuals (usually the heads of respective departments or organizations) have a comprehensive understanding of the United States' existing capabilities; requirements; threat assessments; ongoing developments; emerging Research and Development (R&D) and Science and Technology (S&T); schedules; funding; contracts; facilities; best practices; or lessons learned.³⁷ Thus as a nation, we continue to limit our efficiency and effectiveness in meeting warfighter demands by failing to capitalize on the limited resources available – funding, expertise, and access to critical information. Though short operational timelines drive the need to leverage existing tools, emerging technologies, and Commercial or Government Off-the-Shelf (COTS/GOTS) capabilities; cyber operations continue to suffer due to limited partnerships, weak ties, and a non-unified strategy across the cyber community.³⁸

RECOMMENDATIONS

“To succeed in our national security mission, the DoD recognizes the need to maintain a robust and comprehensive effort to continue the development of interagency and DoD policies, doctrine, and requirements. The goal is a conceptual framework for an environment that increases cyber security, develops and acquires robust military capabilities for full spectrum operations in cyberspace, and protects critical infrastructure as well as the Defense Industrial Base.”³⁹

USD AT&L

2011 Draft Strategy for Acquisition and Oversight of DoD Cyber Warfare Capabilities

Model It After JIEDDO

The Joint Improvised Explosive Device Defeat Organization (JIEDDO) was created to lead DoD actions to rapidly provide Counter-Improvised Explosive Device (C-IED) capabilities in support of the CCDR.⁴⁰ It is important to note that the need for JIEDDO arose from two underlying realities: the real-world threat imposed to United States national security stemming from the increasing tactical employment of IEDs in the Middle East, and the necessity to rapidly defeat the adversary’s use of the IED as a weapon of strategic influence.⁴¹ Of equal importance is that within cyberspace, we are already at war. Though a preponderance of doubters and/or uninformed parties still persists, the harsh truism is that as a nation we cannot wait for a “Cyber Pearl Harbor” to occur before taking this domain seriously. As with the C-IED initiative, we must address and invest in this critical area now through an integrated approach to rapid technological innovation.

JIEDDO’s development strategy, and that of this argument, is one of an investment bank.⁴² To expedite innovation, development, and delivery to the warfighter, JIEDDO leverages the concept of off-the-shelf, relatively inexpensive solutions immediately – while high-potential and near-ready technologies are developed and fielded quickly to forces on the ground.⁴³

Additionally, JIEDDO balances risk and expediency through their Joint IED Capability Approval

and Acquisition Management Process (JCAAMP) which creates a steady pipeline of capabilities and initiatives needed for a proactive fight against IEDs (see Figure 3).⁴⁴

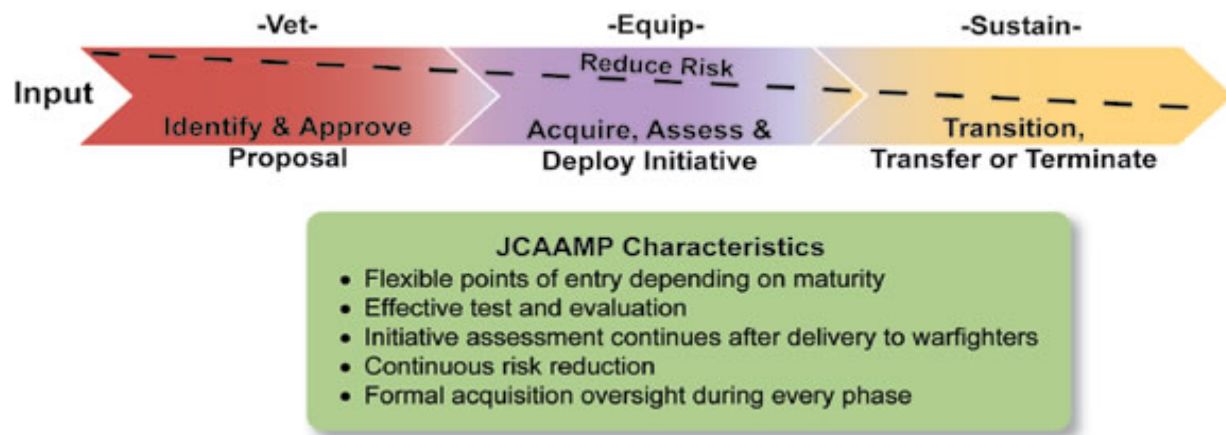


Figure 3 – JCAAMP Process
Reference: JIEDDO Business Opportunities, 6 December 2011

Reorganize To Increase Efficiency

Despite recent policy restructures by the DoD to ensure interconnectedness across the National Security Strategy (NSS), National Military Strategy (NMS), and Cyberspace Operations; the acquisition of cyber capabilities remains cumbersome and disjointed. Currently, United States Cyber Command (USCYBERCOM) is a sub-unified command under United States Strategic Command (USSTRATCOM) – with each of the Service components represented within USCYBERCOM. Using the Air Force component for example – the operational cyber Wings report to the 24th Air Force (24AF), the Numbered Air Force (NAF) which represents Air Force Cyber (AFCYBER); who subsequently reports to Air Force Space Command (AFSPACE). AFSPACE then reports through Air Force channels to USCYBERCOM for all things cyber. Though they all eventually report to USCYBERCOM, in this construct the Service components and external agencies remain stove piped – meaning that requirements, funding, and prioritization have disparate origins. JIEDDO however, has overcome these obstacles through

consolidation. Understanding that individually, these entities are not conducive to rapidly countering the threat, JIEDDO is structured in the unique position of having all three DoD decision-making systems – requirements identification (JCIDS), acquisition (Defense Acquisition System), and financial management (PPBE) within one organization.⁴⁵ This affords the consolidation of the three processes to enable effective streamlining, clear alignment of responsibility, authority and accountability.⁴⁶ Thus the first recommendation for cyber is to align AFCYBER [24AF] directly beneath USCYBERCOM – and likewise for the execution arms of each of the Service components. To the maximum extent possible, each of the Service components should be aligned under a Joint ICD (JICD), and under the same Joint Concept for Cyberspace Operations.⁴⁷ Further, cyber should adopt the concept of the JIEDDO Chief of Staff and the JIEDDO Operational Requirements and Assessment Board. Under USCYBERCOM, the Chief of Staff would develop and maintain an enterprise management system capturing all ongoing cyber initiatives and capabilities across the DoD and other agencies, while the Operational Requirements and Assessment Board validates new requirements; prioritizes existing requirements; and identifies the appropriate sponsor (Service component or agency) to address emerging capability gaps.⁴⁸ This will not only remove several layers of potentially unnecessary bureaucracy within the respective Services, but it will also consolidate requirements; focus cyber development to more effectively meet urgent CCDR needs; increase communication and collaboration; and expedite timelines at the operational and tactical levels.

Budget (PPBE) Flexibility and Culture Change

The second recommendation serves to overcome the rigidity within the existing financial process. If not the most important recommendation, improving the budget flexibility is a close second to reorganization. As was discussed earlier, within the current PPBE and Program

Objective Memorandum (POM) processes, Service components are required to plan and program cost estimates to meet requirements thresholds. Thus, budgets approved by Service executives, OSD, and Congress are meant to be spent in accordance with pre-defined guidelines – significantly reducing a program manager’s ability to be responsive to dynamic threats, situations, and warfighter requirements. Hereto, cyber should adopt JIEDDO best practices. The Director, JIEDDO has the authority to approve initiatives valued up to \$25 million (total life-cycle costs), to include incremental funding; and to recommend via the Senior Resources Steering Group, approval to the Deputy Secretary of Defense for those initiatives greater than \$25 million.⁴⁹ Not only does the Director maintain the authority to pursue such initiatives, but the Director also has the ability to reprioritize, terminate, transition, or transfer an ongoing initiative at any point.⁵⁰ This is exactly what cyber needs. Under this construct, the Service components could still POM through normal Service channels, however, USCYBERCOM would receive an annual allotment to spend consistent with emerging CCCR requirements. Being that requirements would now all stem from the same source, USCYBERCOM, the Service components would have a comprehensive understanding of what needs to comprise their POM inputs. This also ensures USCYBERCOM has sufficient funds to disperse throughout a given fiscal year to meet the urgent operational needs of the CCCR. Further, the current culture of “Yes, a requirement exists, but who told you to spend Air Force (substitute any Service component or agency) funds to meet that requirement,” would change immediately. Because requirements and prioritization would both originate within USCYBERCOM, with direct ties to the NSS, the NMS, a JICD, and CCCR needs; the Service components and agencies would become the execution arms of a unified strategy to fly, fight, and win in cyberspace.

Implement an Evolutionary Approach to Increase Fielding Speed

In conjunction with a reorganized, more efficient command structure and a more flexible PPBE process, the third recommendation is to demand that the DoD applies an evolutionary approach to its weapons systems acquisitions. To achieve “rapid acquisition,” JIEDDO efficiently and effectively leverages available funding, balanced operational and programmatic risk, and responsive contracting support to design, develop, and produce quality systems.⁵¹ To ensure delivery of time sensitive operational capability, JIEDDO operates under the construct of schedule, not cost, as the independent variable.⁵² Moreover, JIEDDO employs parallel development and procurement processes, and multiple technology paths, to achieve an 80 percent solution to deploy capabilities to the warfighter as early as practical.⁵³ Though the DoD recognizes a similar approach, evolutionary acquisition, it is frequently underutilized. According to USD AT&L, evolutionary acquisition focuses on time-phased delivery of capability based on technologies demonstrated in relative environments – followed by subsequent increments of capabilities over time to accommodate improved technology.⁵⁴ Where the DoD often misses the mark, however, is by identifying cost as the independent variable, and by failing to concretely identify incremental thresholds. Like JIEDDO, the DoD must obtain a trained workforce and an assessment methodology to ensure the right decisions are made, at the right times, to provide an acceptable level of capability at stated time sensitive needs.⁵⁵ Otherwise, warfighters will continue to search for alternate methods of procuring cyber capabilities while avoiding the use of the DoD acquisition workforce and processes.

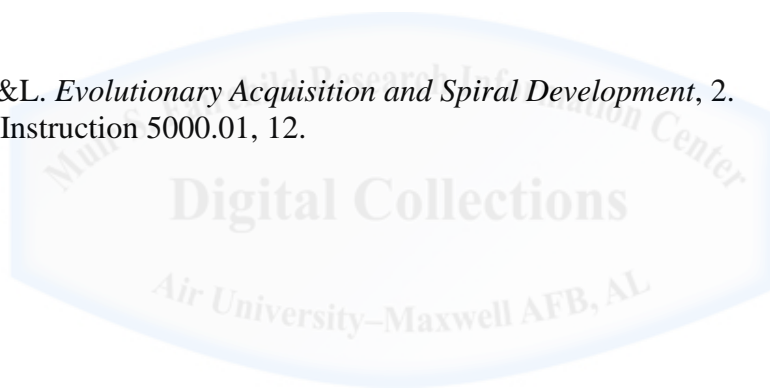
CONCLUSION

Within cyberspace, we are already at war – a war for information and technology superiority to ensure global reach and global power. The harsh truism is that as a nation we cannot wait for a “Cyber Pearl Harbor” to occur before taking cyberspace seriously. As with JIEDDO and the C-IED initiative, we must posture and invest in this critical area now through an integrated approach to rapid technological innovation. To placate the endless chase of advancing software, and the progression of adversary’s offensive and defensive tactics and techniques, the DoD must overcome systems complexity, budget rigidity, limited partnerships, weak ties, and a non-unified strategy across the cyber community. As it stands now, the existing DoD acquisition process is quickly becoming irrelevant with regards to cyberspace. Cyber war-fighters are searching at all cost to avoid the bureaucracy and lengthy timetables associated with today’s Defense Acquisition System. To overcome these impediments, the DoD must focus on reorganization for efficiency; budget flexibility; and the rapid fielding of capabilities to our warfighters. If not, the status quo of yesterday’s technology, delivered tomorrow will ultimately render the DoD Defense Acquisition System irrelevant in the cyber fight.

ENDNOTES

1. Joint Vision 2010, 11.
2. Kopp, Carlo. *Surviving the Modern Integrated Air Defense System*, 1.
3. Ibid., 1.
4. Ibid., 1.
5. Ibid., 1.
6. Charette, Robert N. *What's Wrong With Weapons Acquisitions*, 2.
7. Ibid., 1.
8. Jabbour, Kamal. *Cyber Vision and Cyber Force Development*, 63.
9. Kurzweil, Ray. *The Law of Accelerating Returns*, 1.
10. Ibid., 1.
11. Joint Publication (JP) 3-13, GL-6.
12. Ibid., GL-5.
13. Leighton, Cedric. *Pull the Cyber War Trigger, If We Have To*, 1.
14. Ibid., 1.
15. Charette, Robert N. *The Weapons Acquisition Process: An Intellectual Disconnect*, 2.
16. Defense Acquisition Portal, 1.
17. Schwarz, Moshe. *Defense Acquisitions: How DoD Acquires Weapon Systems and Recent Efforts to Reform the Process*, 1.
18. Defense Acquisition Portal, 1.
19. Schwarz, Moshe. *Defense Acquisitions: How DoD Acquires Weapon Systems and Recent Efforts to Reform the Process*, 4.
20. Ibid., 8.
21. Ibid., 8.
22. Ibid., 16.
23. Charette, Robert N. *What's Wrong With Weapons Acquisitions*, 4.
24. Ward, Dan, *Acquisition Lessons from a Galaxy Far, Far Away*, 67.
25. Ibid., 70.
26. Ibid., 70.
27. USD AT&L. *Draft Strategy for Acquisition and Oversight of DoD Cyber Warfare Capabilities*, 4.
28. Charette, Robert N. *What's Wrong With Weapons Acquisitions*, 1.
29. Ibid., 1.
30. GSAM. *Software Victory – Exception or Rule*, 2-21.
31. Ibid., 2-21.
32. Schwarz, Moshe. *Defense Acquisitions: How DoD Acquires Weapon Systems and Recent Efforts to Reform the Process*, 16.
33. GSAM. *Software Victory – Exception or Rule*, 2-16.
34. Ibid., 2-11.
35. Ibid., 2-11.

36. USD AT&L. *Draft Strategy for Acquisition and Oversight of DoD Cyber Warfare Capabilities*, 11.
37. Ibid., 12.
38. Ibid., 12.
39. Ibid., 3.
40. JIEDDO Official Website, 1.
41. Ibid., 1.
42. JIEDDO – BAA/BIDS. *How to do Business with JIEDDO*, 1.
43. Ibid., 1.
44. Ibid., 1.
45. JIEDDO Instruction 5000.01, 2.
46. Ibid., 2.
47. USD AT&L. *Draft Strategy for Acquisition and Oversight of DoD Cyber Warfare Capabilities*, 7.
48. JIEDDO Instruction 5000.01, 7 and 32.
49. Ibid., 4.
50. Ibid., 4.
51. Ibid., 12.
52. Ibid., 12.
53. Ibid., 12.
54. USD AT&L. *Evolutionary Acquisition and Spiral Development*, 2.
55. JIEDDO Instruction 5000.01, 12.



BIBLIOGRAPHY

- Chairman of the Joint Chiefs of Staff Instruction 3170. Joint Capabilities Integration and Development System. 17 Mar 2011.
- Charette, Robert N. Nov 2008. *The Weapons Acquisition Process: An Intellectual Disconnect*. <http://spectrum.ieee.org/aerospace/military/the-weapons-acquisition-process-an-intellectual-disconnect> (accessed 25 October 2011).
- Charette, Robert N. Nov 2008. *What's Wrong With Weapons Acquisitions*. <http://spectrum.ieee.org/aerospace/military/whats-wrong-with-weapons-acquisitions> (accessed 25 October 2011).
- Defense Acquisition Portal. <https://dap.dau.mil/aphome/das/Pages/Default.aspx> (accessed 18 November 2011).
- DoD Instruction 5000.02. *Operation of the Defense Acquisition System*. 8 December 2008.
- Gates: May 2008. *Next War Itis plagues military – US news – Military – msnbc.com*. http://www.msnbc.msn.com/id/24600218/ns/us_news-military/t/military-must-focus-current-wars-gates-says/ (accessed 18 November 2011).
- Guidelines for Successful Acquisition and Management of Software-Intensive Systems: Version 3.0. *Software Victory – Exception or Rule?* May 2000.
- Homeland Security. Feb 2003. http://www.dhs.gov/files/publications/editorial_0329.shtm (accessed 25 October 2011).
- Jabbour, Kamal. *Cyber Vision and Cyber Force Development*. Strategic Studies Quarterly, Spring 2010. <http://www.au.af.mil/au/ssq/2010/spring/jabbour.pdf> (accessed 25 October 2011).
- JIEDDO. <https://www.jieddo.DoD.mil/> (accessed 18 November 2011).
- JIEDDO Instruction 5000.01. *JIEDD Capability Approval and Acquisition Management Process*. 22 Dec 2010.
- JIEDDO – BAA/BIDS. <https://www.jieddo.DoD.mil/bizops.aspx> (accessed 18 November 2011).
- Joint Publication (JP) 3-13. *Information Operations*. 13 Feb 2006.
- Joint Vision 2010. <http://www.dtic.mil/jv2010/jv2010.pdf> (accessed 25 October 2011).
- Kopp, Carlo. Feb 2009 *Surviving the Modern Integrated Air Defence System*. <http://www.ausairpower.net/APA-2009-02.html> (accessed 25 October 2011).

Kurzweil, Ray. Mar 2001. *The Law of Accelerating Returns*.
<http://www.kurzweilai.net/the-law-of-accelerating-returns> (accessed 25 October 2011).

Leighton, Cedric. *Pull the Cyber War Trigger, If We Have To*.
<http://defense.aol.com/2011/11/11/pull-the-cyber-war-trigger-if-we-have-to/?icid=related2>
(accessed 21 November 2011).

Schwarz, Moshe. *Defense Acquisitions: How DoD Acquires Weapon Systems and Recent Efforts to Reform the Process*. 23 Apr 2010.

USD AT&L. *DRAFT Strategy for Acquisition and Oversight of Department of Defense Cyber Warfare Capabilities*. 17 Aug 11.

USD AT&L. *Evolutionary Acquisition and Spiral Development*,
<https://acquisition.navy.mil/content/download/863/.../041202acq.pdf> (accessed 9 December 2011).

US Government Accountability Office. *DEFENSE ACQUISITIONS: Charting a Course for Lasting Reform*, GAO- 09-663T, 30 Apr 2009.

Ward, Dan, Lt Col, USAF. *Don't Come to the Dark Side: Acquisition Lessons from a Galaxy Far, Far Away*. Defense AT&L. Sep-Oct 2011.

