POLICY CHANGES FOR ACQUISITION OF OFFENSIVE CYBERSPACE WEAPON SYSTEMS

GRADUATE RESEARCH PROJECT

Brendan K. Casey, Major, USAF

AFIT/ICW/ENG/10-02

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY
AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this report are those of the author and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government.

AFIT/ICW/ENG/10-02

POLICY CHANGES FOR ACQUISITION OF OFFENSIVE CYBERSPACE WEAPON SYSTEMS

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Cyber Warfare

Brendan K. Casey, Major, USAF
AFIT/ICW/ENG/10-02

June 2010

AFIT/ICW/ENG/10-02

POLICY CHANGES FOR ACQUISITION OF OFFENSIVE CYBERSPACE WEAPON SYSTEMS

Brendan K. Casey, MS
Major, USAF

Approved:

______//signed//______________________ __09 June 2010__
Robert F. Mills, PhD (Chairman) Date

______//signed//______________________ __10 June 2010__
John M. Colombi, PhD (Member) Date

AFIT/ICW/ENG/10-02

Abstract

Because the cyberspace environment is changing so quickly, the slow, methodical Department of Defense (DoD) acquisition process may not suffice. By following the evolutionary acquisition method and incorporating five policy caveats, the DoD acquisition process can acquire effective systems quickly.

The purpose of this research is to provide recommended policy changes in the acquisition of offensive cyberspace weapon systems for the Air Force and DoD in general. This paper describes the current DoD acquisition process, explains how cyberspace is different from the other domains, discusses a few innovative acquisition and development approaches, and concludes with the recommended policy changes. A literature search on the cyberspace community along with DoD and Air Force doctrine provided the bulk of the research.

The recommended acquisition policy changes fall into the following categories: expanding the network of development activities, building payloads for specific target sets, security classification, sustainment of cyberspace capabilities and testing throughout the acquisition process.

Table of Contents

List of Figures

Figure

POLICY CHANGES FOR ACQUISITION OF OFFENSIVE CYBERSPACE WEAPON SYSTEMS

I. Introduction

In 1965, Gordon Moore, co-founder of Intel, stated that the complexity of transistors on a chip will increase a factor of two per year (Moore, 1965). This has become known as Moore's Law. Intel has tracked this over the past 40 years and has found it to be valid (Intel, 2010). Because the computer chips are increasing in complexity at such a great speed, the entire cyberspace environment is constantly changing.

The cyberspace environment as a subset of the information environment "is a global environment composed of all individuals, organizations, and systems that collect, process, disseminate, or act on information" (Mullen, 2010). Unlike the environment of air, space, land, or sea, the cyberspace environment is controlled not only by natural laws but also by human-made laws meaning it is also "malleable" (Rattray, 2009). While it is not infinitely malleable, it is changeable such that a cyberspace system's effectiveness can change. As Moore's Law implies, these changes are occurring very fast, a generation of growth capability in at least two years. These changes come about because of hardware being swapped out (CPUs, routers, switches, etc), software implementations changing (newer versions of operating systems, etc) or protocol changes (migrating from Internet Protocol (IP)v4 to IPv6). The adversary's target and environment of use is constantly evolving. Cyberspace operations use cyberspace capabilities "primarily to achieve objectives in or through cyberspace" (Mullen, 2010).

The DoD acquisition process is designed to acquire large scale and large quantity items. These large systems take time. Dunlap predicted adversaries will attempt to get inside the DoD's "acquisition loop … deploy[ing] newer systems before they [the DoD] finished buying already obsolescent ones" (Dunlap, 1996). Because of the quickness the cyberspace environment is changing, the slow, methodical acquisition process may not suffice. By following the evolutionary acquisition method and incorporating new policy caveats, the DoD acquisition process can acquire effective systems quickly. Five policy changes that the DoD acquisition community must embrace are: expanding the network of development activities, building payloads for specific target sets, security classification, sustainment of cyberspace capabilities and testing throughout the acquisition process.

The purpose of this paper is to present a method to best adapt our acquisition processes to provide timely capabilities for cyberspace operations. Its scope is limited to the DoD acquisition process of cyberspace systems, specifically systems that incorporate offensive cyberspace capabilities with a brief discussion of defensive cyberspace capabilities.

This paper begins with a background on the DoD acquisition process. It will summarize the Joint Capabilities Integration and Development System (JCIDS), the Planning, Programming, Budgeting, and Execution (PPBE) system, and the Defense Acquisition System as defined by the DoD Instruction 5000.02. It presents a summary of the evolutionary acquisition method and the purpose of classification. Next this research discusses the definition of the cyberspace domain, cyberspace capabilities, and the components that form an offensive cyberspace weapon system. Three popular commercial platforms are using innovative acquisition and development approaches. This paper addresses who these innovative third-party developers are, how Facebook, Apple's iPhone, and Metasploit use these developers to acquire software capabilities more effectively. The paper concludes with five policy changes that the DoD acquisition community must embrace and how the DoD acquisition community can embrace them.

II. DoD Acquisition Process

> The Defense Acquisition System manages the nation's investments in technologies, programs, and product support to assist the United States armed forces in achieving their objectives. It translates user needs and technological opportunities into producible, deployable products that provide operational capabilities to users. Its primary aim: develop and deploy the solutions to warfighter needs, each with the best value over the system's life cycle, in a timely manner and at a fair and reasonable price. (SAF/USAM, 2006)

Big "A" Acquisition is the term used to describe the three processes in the DoD to deliver a new system to the warfighter. As Figure 1 shows, it is comprised of;

- Joint Capabilities Integration and Development System (JCIDS),
- Planning, Programming, Budgeting, and Execution (PPBE), and
- Defense Acquisition System (DAU, 2009).

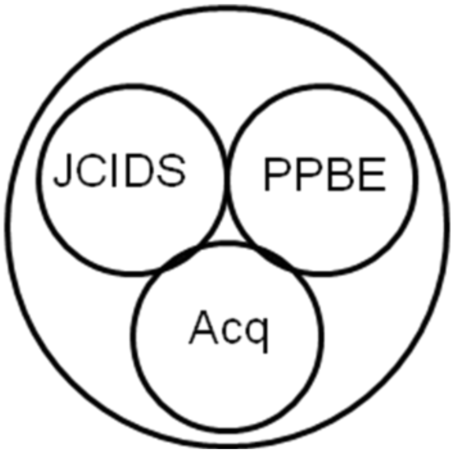

Figure 1: Big "A" Acquisition

Joint Capabilities Integration and Development System (JCIDS)

JCIDS is the first step in this process. The JCIDS process is responsible for identifying shortfalls in warfighting capability (McChrystal, 2009; SAF/USAM, 2006). An analysis is performed comparing the strategic guidance (National Defense Strategy and National Military Strategy) with the capabilities the DoD will need to meet this guidance in an 8-20 year period

(SAF/USAM, 2006). Shortfalls in the DoD capability to meet the guidance are termed needs. The JCIDS process then addresses ways to correct these needs.

An Analysis of Alternatives (AoA) is performed. This analysis looks as different ways to meet the need. The acronym DOTMLPF stands for: Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, or Facilities. DOTMLPF represents alternative ways the DoD can address needs. These must all be considered in the AoA to determine the best fit. For example, to address the need of the importance of cyberspace to the USAF, an organizational change (activating the 24NAF) was deemed necessary to help develop our cyberspace capabilities. Other solutions may require an increase in training at the base level such as annual Information Assurance training while others may require a materiel solution. This research focuses primarily on materiel solutions.

Once a materiel solution route is selected, an Initial Capabilities Document (ICD) must be developed and validated (McChrystal, 2009). This document describes the capabilities of the materiel solution desired to address the mission shortfall (need) as determined by the JCIDS process. The ICD will include Key Performance Parameters (KPP). These parameters differ from the non-key performance parameters in that if the KPPs are not met, the system may be deemed unacceptable for fielding. The KPPs are often the minimum requirements the system must meet to be accepted as addressing the shortfall. The warfighting community may not accept a system that does not meet its KPPs.

Planning, Programming, Budgeting, and Execution (PPBE)

The Programming, Planning, Budgeting, and Execution process is how the DoD funds the acquisition of a materiel solution. This is a continuous process for while a program office is executing this year’s funds, it is budgeting for next year’s funds, and programming for future year’s funds.

The output of the PPBE process is an approved Presidential Budget. The Presidential Budget contains Program Elements (PE) which are the basic budget building block. A PE may have a one-to-one relationship with a program if the program is large enough, a program may contain multiple PEs, or a PE may include a number of smaller programs grouped together because of similar mission area. An example of a one-to-one relationship is the PE 0605864f for "Space Test Program" (SAF/USAM, 2006). GPS, because of its large scope, contains multiple PEs (e.g., terminals, ground stations, and space vehicles), while the PE for MILSATCOM Terminals contains multiple programs under one PE (SAF/USAM, 2006).

Seeing as PEs are the basic building blocks of the PPBE process, the Services request funding based on PE instead of requesting funding for individual programs. This allows Congress to designate funds for specific PEs giving Congress insight into how the DoD is spending the appropriated defense money.

The budget process is a biennial process meaning that a budget is approved every two years as opposed to every year (SAF/USAM, 2006). Therefore, for the fiscal year (FY) (1 Oct to the following 30 Sep) of 2011, the budget was approved in the fiscal year 2010 budget. The next budget will be approved for fiscal year 2012. Budgets are approved on the even years.

The budget is actually approved in the Future Years Defense Program (FYDP). As seen in Figure 2, the FYDP is comprised of six years of planning. This includes the current year, next year, and planning for the following four. Because there is not a new budget approved for the next year (off year), the FYDP should be as accurate as possible. For the following four years, the budget may be updated in future FYDPs. For the budget approved in FY10, the FYDP covers the budget for FY10 – FY15.

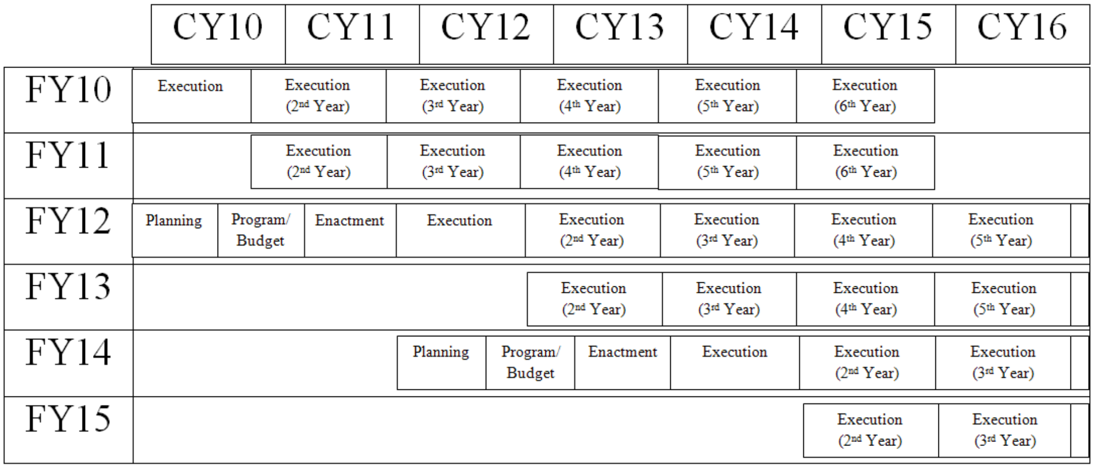

Figure 2: PPBE Process

Because budget approval is a long process, the Services usually start submitting their budgets two years before the first execution year. Therefore, for the FY10 FYDP, the Services began planning in FY08.

To begin the PPBE process, the Major Commands (MAJCOMS), Direct Reporting Units (DRUs), and Field Operating Agencies (FOAs) submit a Program Objective Memorandum (POM) to their Service (SAF/USAM, 2006). The POM contains a budget request for specific PEs. These budget requests fall into one of four categories:

- Initiatives: add funds for new programs or capabilities to existing ones
- Disconnects: add or realign funds to correct shortfalls in current budgeting
- Offsets: reduce, restructure, or cancel programs
- Zero-balance transfers: realign funds between appropriations in an existing program (i.e., switch R&D funds for O&M funds for the same amount)

The MAJCOMS, DRUs, and FOAs prioritize the POMs submitted by their units to achieve one POM for the organization to send to HQ USAF.

The USAF and other Services then prioritize the POM requests from all their units. Each Service submits one POM to the Office of the Secretary of Defense (OSD). With assistance from Joint Staff, OSD prioritizes into one POM request to the President. The President then prioritizes the OSD POM with the other Executive agencies' POMs for Congress who approves the Presidential Budget.

Defense Acquisition System (DoDI 5000.02)

Now that a requirements document (the ICD from the JCIDS process) and funding to begin work (the FYDP from the PPBE process) are approved, the Defense Acquisition System process begins.

DoDI 5000.02 "Operation of the Defense Acquisition System" defines the overall process. It is the process that describes the

> management framework for translating capability needs and technology opportunities, based on approved capability needs, into stable, affordable, and well-managed acquisition programs that include weapon systems, services, and automated information systems (AISs). (USD(AT&L), 2008)

As seen in Figure 3, this process is broken into five phases:

- Materiel Solution Analysis
- Technology Development
- Engineering and Manufacturing Development
- Production and Deployment
- Operations and Support

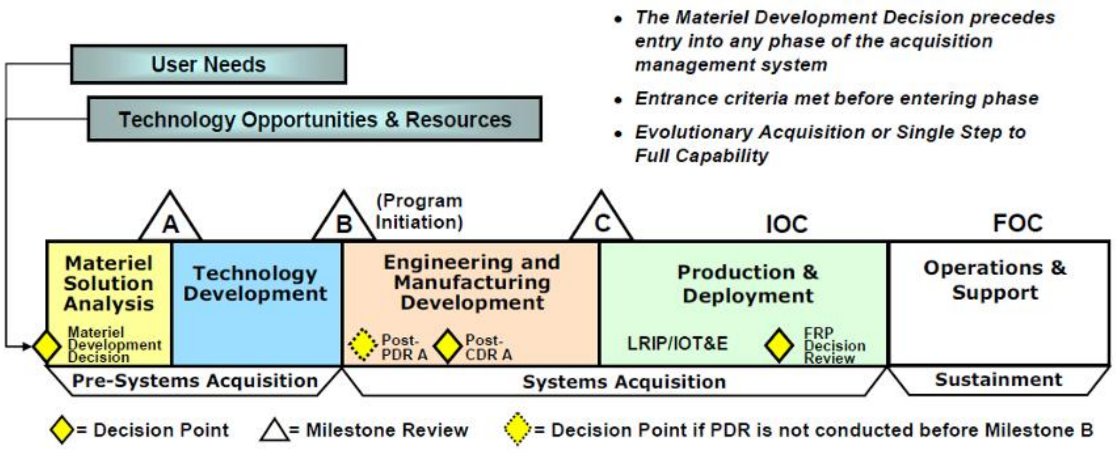
The Materiel Development Decision precedes entry into any phase of the acquisition management system
Entrance criteria met before entering phase
Evolutionary Acquisition or Single Step to Full Capability
User Needs
Technology Opportunities & Resources
A
B
(Program Initiation)
C
IOC
FOC
Materiel Solution Analysis
Materiel Development Decision
Technology Development
Engineering and Manufacturing Development
Post-PDR A
Post-CDR A
Production & Deployment
LRIP/IOT&E
FRP Decision Review
Operations & Support
Pre-Systems Acquisition
Systems Acquisition
Sustainment
= Decision Point
= Milestone Review
= Decision Point if PDR is not conducted before Milestone B

Figure 3: Defense Acquisition Management System (USD(AT&L), 2008)

The first two phases comprise the Pre-System Acquisition process. The Materiel Solution Analysis includes the work done in the JCIDS process. Input to this phase is the user needs defined as warfighting capability shortfalls. An AoA is performed to see which of the DOTMLPF solutions is the best. If it is a materiel solution, continue into the Technology Development Phase. The purpose of this phase is to reduce technological risk before implementing technologies into a new program. This includes funding new technologies or funding new uses of existing technologies in the Science and Technology sector (e.g., DoD laboratories, universities, or R&D corporations). Reducing technological risk means finding a technology that is mature enough to meet the needs of the warfighter and be able to be deployed through refinement and integration in the rest of the acquisition process.

The next two phases comprise the System Acquisition process. After Milestone B, a new program is initiated. This requires specific funding from a PE for the program. No longer can the program fall under General R&D; it must be specifically funded through an approved PE. This is also the phase most people think about when they think acquisition.

The goals of the Engineering and Manufacturing Development (EMD) phase are to:

- develop a system or an increment of capability;
- complete full system integration (technology risk reduction occurs during Technology Development);
- develop an affordable and executable manufacturing process;
- ensure operational supportability with particular attention to minimizing the logistics footprint;
- implement human systems integration (HSI);
- design for producibility;
- ensure affordability;
- protect CPI by implementing appropriate techniques such as anti-tamper; and
- demonstrate system integration, interoperability, safety, and utility (USD(AT&L), 2008).

In short, the goal is to mature and integrate the technology into a tested, producible, and deployable weapon system while remaining on scheduled and within budget while maintaining performance.

The EMD phase has two major efforts: Integrated System Design and System Capability and Manufacturing Process Demonstration (USD(AT&L), 2008). During the EMD phase, a system program office (SPO) is selected to lead the development effort. The SPO competes the contract and selects a developer.

During the Integrated System Design effort, the SPO, working with the developer and user, will define system functionality, complete hardware and software design, and reduce the system-level risk. The system functionality must meet the needs spelled out in the Capability Development Document (CDD). The CDD was developed under the JCIDS process following the Technology Development phase. It is a maturation of the ICD and specifies "the operational technical performance attributes of the system that will deliver the capability that fills the capability gaps identified in the ICD" (McChrystal, 2009).

The System Capability and Manufacturing Process Demonstration effort focuses on demonstrating that the designed system can be built and will operationally meet all the required capabilities in the CDD. These required capabilities are the KPPs mentioned earlier in the JCIDS section.

During the Production and Deployment phase, the final decision to produce the system in significant quantities is made after a successful operational test. After the system has been designed and tested at a system level, Low-Rate of Initial Production (LRIP) is approved. In LRIP, a small number of systems are manufactured for use during the operational test. This includes moving the system out of the lab, out of the contractor's control, and into testing in an operationally realistic environment using real-world operators on it. Operational testing may also include live-fire testing where a system is destroyed to test survivability. LRIP is not applicable to AIS or software-intensive systems without developmental hardware. Instead, a limited deployment may be applicable for operational testing. If the system completes operational test satisfactorily, it may enter full-rate production and deployment.

The final phase of the acquisition process is the Operations and Support (O&S) phase. Even after a system has been developed and deployed, the O&S must be monitored. This includes executing the Life-Cycle Sustainment Plan to sustain the system in the most cost-effective manner over its total life cycle (USD(AT&L), 2008). Planning for the O&S of the system started in the EMD phase for sustainability must be considered when designing the system else one could end up with a system that functions but cannot be sustained beyond its initial deployment. This phase continues through disposal which should also have been considered in the previous phases. The Total Life-Cycle Cost, a measurement used when selecting a developer and system, includes the research and development costs, the procurement costs, the sustainment costs, and the disposal costs. For most cyberspace systems, the disposal costs are low.

Evolutionary Acquisition

As stated in DoDI 5000.02, "evolutionary acquisition is the preferred DoD strategy for rapid acquisition of mature technology for the user." Evolutionary acquisition is a strategy that implements multiple development phases to deliver capabilities. As seen in Figure 4, each development phase focuses on a limited block of capabilities with each block building on the previous.

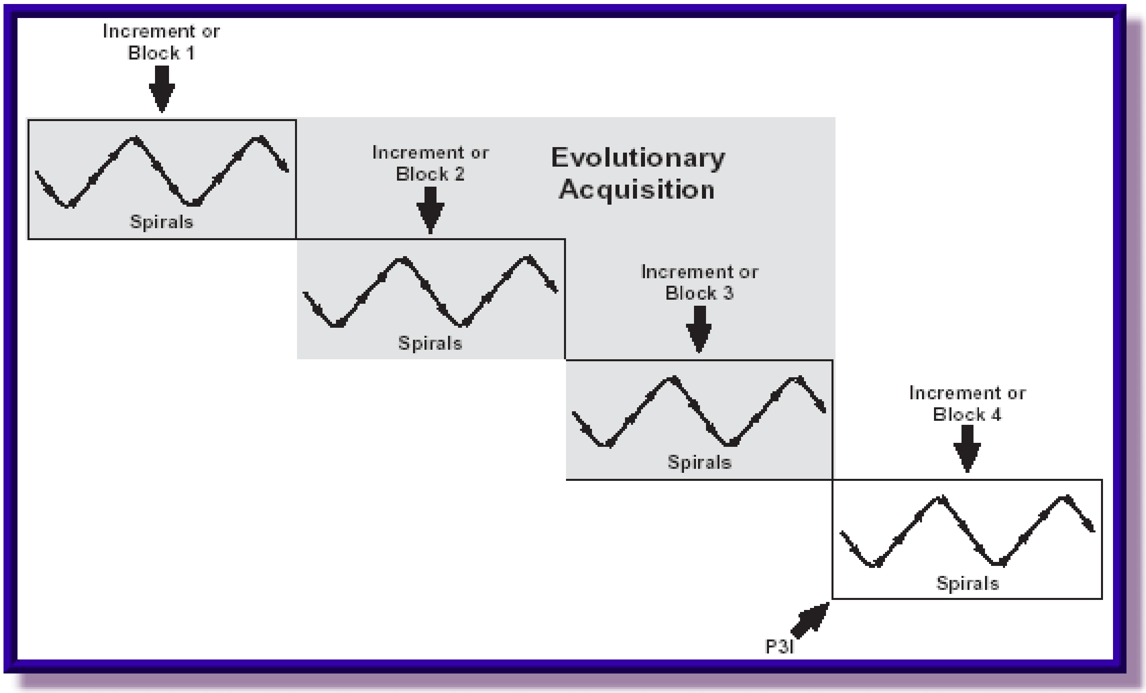

Figure 4: Evolutionary Acquisition (STSC, 2002)

There are two methods for evolutionary acquisition (STSC, 2002). Both are useful for developing cyberspace systems. In incremental development, the final capabilities to be delivered are firmly defined at the outset. Each development phase delivers capabilities that build upon the previous release towards this final product. The second method, spiral development as seen in Figure 5, does not define the final end product but only the capabilities for the first phase (spiral) of development. Instead of building towards a final capability, this method allows for technology maturation to define the final product. Both methods use iterative developments to allow the warfighter to gain some capability quickly with further capability, either expansion or maturation, later (DAU, 2010).

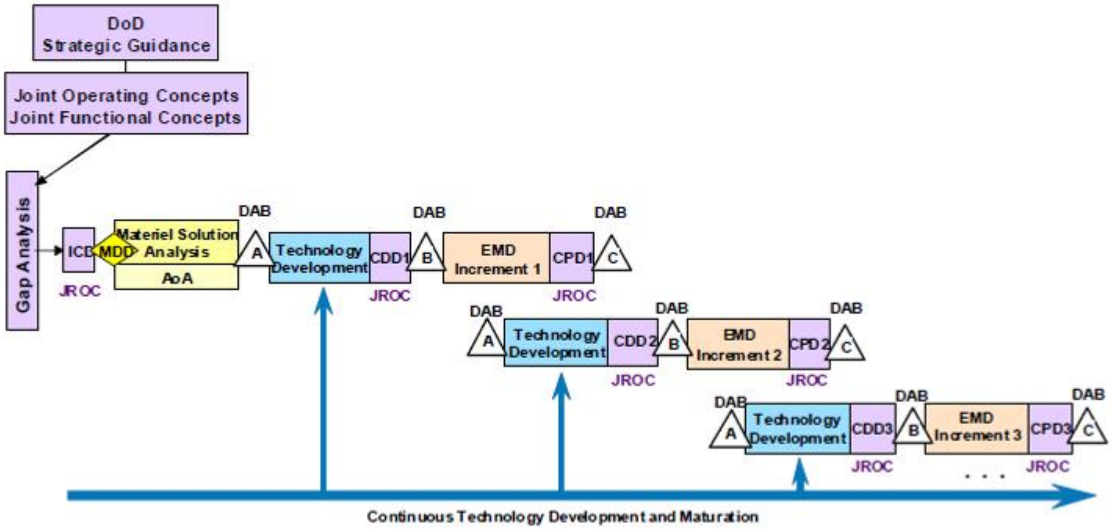

Figure 5: Evolutionary acquisition with spiral/incremental development (USD(AT&L), 2008)

The goal of evolutionary acquisition is to provide some basic capability to the warfighter quickly and build upon that. By limiting the capabilities delivered in each phase, the acquisition community can scope their development to ensure the limited block of capabilities is delivered on time and on budget. Without evolutionary acquisition, the time to complete the "full" system as defined in the ICD may take so long that the technology is outdated by the time the system is delivered to the warfighter.

Security Classification

Classification levels aid the DoD in protecting information from unauthorized recipients. The three levels of classification (Top Secret, Secret, and Confidential) are used to define the level of damage the protected information would cause to national security if divulged (Bush, 2003). Protecting information through classification is an expensive process. In 2003, the U.S. government, excluding the CIA, spent $6,531 million ($6.5 billion) on classification measures (OTG, 2004). Protecting information through classification requires physically protecting the information, performing extensive background checks on individuals before allowing access, and building facilities in which to work on the classified material away from non-cleared individuals. Therefore, the DoD must balance the possible damage to national security with the cost of classification when deciding if information should be classified.

Three types of information about a system can be classified: existence of the system, the system's capabilities, or the concept of operations (CONOPS) for the system. Keeping a system's existence classified provides for the most protection but also costs the most to maintain. These costs come not only from the monetary costs of the three factors above but also the lost opportunity of interacting with other systems. Lost opportunities may exist if the system offers synergistic benefits with other systems that are not realized because warfighters do not know of its existence. It is also possible this system could interact negatively with other friendly systems when activated or not even be considered when planning operations.

Protecting the capabilities of a system is very common. While the existence of the F-22 is unclassified, some capabilities about the aircraft may remain classified. For example, the F-22 was designed to be low observable. That is unclassified information. However, its actual radar cross section (i.e. stealthiness) remains classified. The DoD decided not to protect the existence of the weapon system, but specifics about the capabilities of the weapon system are closely guarded.

The CONOPS, often documented in the Tactics, Techniques, and Procedures (TTP), describes how the weapon system will be used in conflict. Again, it is unclassified knowledge that the F-22 will be used in air-to-air and air-to-ground missions. However, the ways in which the F-22 will be employed remain classified. Adversaries know that F-22 exists and that it will be used in specific missions, but they do not know the specifics of how the F-22 will operate to perform those missions.

Throughout the acquisition process, the program office will need to understand what this Critical Program Information (CPI) is and how to best protect it.

> CPI may be classified information or Controlled Unclassified Information about technologies, processes, applications, or end items that if disclosed or compromised, would degrade system combat effectiveness, compromise the program or system capabilities, shorten the expected combat-effective life of the system, significantly alter program direction, or require additional RDT&E resources to counter the impact of the compromise. (DAU, 2010)

The program office must consider whether the existence of the system, specifics about the system's capabilities, or the CONOPS of the system will need to be classified as CPI and how to protect it as such.

Summary

The acquisition process has evolved over time into what exists today. It has been designed as a deliberate process allowing oversight into how the U.S. taxpayers' money is spent. This deliberate process meets the demands of most land, sea, air, and space acquisitions. However, this acquisition process will not work in cyberspace because it is such a different domain.

III. Cyberspace is Different

The DoD acquisition process was designed to acquire systems for the land, sea, air, and space domains. Before this research can discuss acquisition in the cyberspace domain, it must first discuss what the cyberspace domain is, the capabilities are, and the components of an offensive cyberspace system is.

Cyberspace Domain

The cyberspace environment as a subset of the information environment "is a global environment composed of all individuals, organizations, and systems that collect, process, disseminate, or act on information" (Mullen, 2010). It is governed by both natural laws and human-made laws. Like air, sea, land, and space environments, the cyberspace environment is governed by natural laws. These are the laws that humans cannot change. Humans can build tools to exploit these laws to gain access to the domain. The natural laws that govern the cyberspace environment are the electro-magnetic laws that govern the physical layer. These include the sciences of radio frequency for wireless, optics for fiber cables, and power management for memory and timing.

Unlike the other four environments, the cyberspace environment is also governed by human-made laws. Rattray (2009) mentions that "it is created by the connections of physical systems and networks, managed by rules set in software and communication protocols." People had to combine the natural laws with physical systems networking them together to create the environment. The significant portion of Rattray's definition is the inclusion of communication protocols. When the physical computer systems are networked together, the cyberspace environment is not created. It is not until there are the communication protocols allowing each physical system to communicate with one another that an environment is created.

Once the cyberspace environment was created, people needed to learn to exploit it by developing technology which allowed the creation of the cyberspace domain. The Joint Staff defines cyberspace as a domain that "consists of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Mullen, 2010). The cyberspace environment existed but underutilized until people begin to exploit it via tools. Unlike the other environments though, people can only interact with the cyberspace environment through technology.

Technology to interact with the cyberspace environment includes software applications. These are similar to the sea vessels that allow one to travel through the cyberspace environment. While people do not physically travel through the environment, communication in the form of electrical energy does. Applications allow people's communication to be interpreted by the cyberspace environment into electrical energy that will travel through the protocols to other networked computers along physical links to the destination.

For this research, the cyberspace domain is restricted to IP (i.e., internet networks).

Cyberspace Capabilities

Cyberspace capabilities are employed to achieve effects. The Joint Staff calls the employment of these capabilities Computer Network Operations (CNO) in Joint Pub 3-13 (JP 3-13), while the Air Force calls the employment Network Warfare Operations (NWO) in Air Force Doctrine Document 2-5 (AFDD 2-5). Both agree on the definition that is best quoted from the Joint Pub: cyberspace operations "stem from the increasing use of networked computers and supporting IT infrastructure systems by military and civilian organizations" (DoD, 2006). Cyberspace capabilities are limited to causing effects achieved through interactions and operations with cyberspace. As the world moves more toward networking of capabilities (e.g., connecting fighter pilots to one another or with the air operations center on the ground through

Link-16, sharing data between the room of analysts at NSA with the deployed warfighter who can use the intelligence through satellite communication), the operations to protect and attack these capabilities must be analyzed.

Cyberspace capabilities are used for both defensive and offensive purposes. While both types of capabilities reside on the same networks/mediums, they are treated differently because of the goals desired by their use.

Defensive Cyberspace Operations

JP 3-13 calls operations that employ defensive cyberspace capabilities Computer Network Defense (CND). These are the actions "taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks" (DoD, 2006). AFDD 2-5 defines Network Defense (NetD) as "network-based capabilities to defend friendly information resident in or transiting through networks against adversary efforts to destroy, disrupt, corrupt or usurp it" (DAF, 2005). Both doctrines define employment of the same capability but call it something different.

Defensive cyberspace capabilities are used to protect and defend one's own networks from attack. These are the capabilities civilians use when defending their own networks which may include updating patches, monitoring logs, or requiring authentication for access. While the DoD may be targeted differently than their civilian counterparts, the defensive capabilities used in operations are very similar. Also with the civilian sector leading the development in defensive cyberspace capabilities, the DoD often follows the civilian sector's lead in implementing the defense of their networks.

Offensive Cyberspace Operations

JP 3-13 calls the operations to employ offensive cyberspace capabilities Computer Network Attack (CNA). These are actions “taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves” (DoD, 2006). AFDD 2-5 defines Network Attack (NetA) as “network-based capabilities to destroy, disrupt, corrupt, or usurp information resident in or transiting through networks” (DAF, 2005). NetA, like CNA, utilize capabilities to provide the effects of “deny, delay, or degrade information in networks, process dependent on those networks, or the networks themselves” (DAF, 2005). Again, two names for the same employment of capabilities.

Offensive cyberspace capabilities are those capabilities the U.S. uses to punitively affect the adversary’s networks. Because so much of the world is networked today including nation’s militaries, the networks that pass information are a highly valuable target. Unlike the defensive uses, the civilian sector does not participate in offensive cyber. Similar to maintaining an armed force, civilian sector pays taxes to the nation to support a combined armed cyberspace force. The civilian sector is focused on defending themselves and not on attacking others.

Because of this, the systems and methods used to conduct offensive cyberspace are often hidden from the public’s view. It wasn’t until July 2006 that the Air Force reformed the 67th Information Operations Wing as the 67th Network Warfare Wing (NWW) stating publicly that the Air Force has a unit that participates in Network Attack. The mission of the 67th NWW includes the line “to conduct network … attack” (DAF, 2010). While AFDD 2-5 was published in 2005 defining what Network Attack is, it wasn’t until the formation of the 67th NWW that the Air Force publicly had a force that performed it.

Components of an Offensive Cyberspace Weapon System

Cyberspace capabilities are used in operations as part of a cyberspace system. An offensive cyberspace weapon system is comprised of three components: access, core system, and payload. Without any one of the three, an offensive cyberspace weapon system cannot operate.

Phister et al wrote about a CyberCraft that is a combination of the core system and payload in one system (Phister, 2005). The CyberCraft concept incorporates many capabilities into one system including command and control of itself, “information assurance, intelligence gathering, information dissemination, deception, and electronic warfare” (Phister, 2005). The system will also “sift through and process massive amounts of data in real-time with little or no apriori knowledge to determine the intelligence value of the target and thereby be able to invoke the proper attack” (Phister, 2005). The technology to perform all this in one system and be able to maintain that system’s technological edge does not exist. The DoD must break each capability into a manageable block as recommended in evolutionary acquisition. By breaking the offensive cyberspace weapon system into components as seen in Figure 6, the DoD acquisition can better manage each block of capability. Each component is designed to provide specific capabilities. As components age, new versions can be employed to maintain the effectiveness of the overall system.

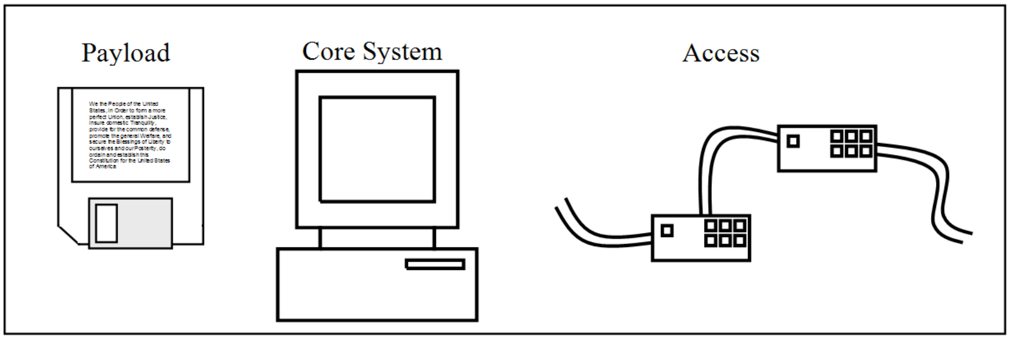
Payload
We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America
Core System
Access

Figure 6: Components of Offensive Cyberspace Weapon System

Access

The access component is necessary because it allows the delivery of the payload to reach the intended target. For airpower, this is analogous to the ingress route the F-22 flies through to get to the target. The ingress route is defined by the departure point of the F-22, the target location, and any opposition in between. Opposition can include air defenses or overflight restrictions. The cyberspace system may need to connect to the target from a CONUS location using the internet. It must consider any firewalls or other anti-intrusion detection systems the payload must pass through on its way to the target. Often this information will be provided to the warfighter through Computer Network Exploitation (CNE) by the Intelligence Community (IC). This is equivalent to airpower's Joint Intelligence Preparation of the Operational Environment (JIPOE) (DoD, 2009). The IC maps out the target's environment through multiple intelligence means to provide the warfighter the best means to survive ingressing to the target.

Core System

The second component of an offensive cyberspace weapon system is the core system itself. This comprises the software, hardware, and CONOPS for detailing how an operation will commence. The core system connects the warfighter to the access point to ingress to the target. The core system may use a GUI to present all the payloads in its inventory to the warfighter. The warfighter, who has been trained on this core system, will be able to select payloads and connect them to the targets. The core system, similar to the F-22 aircraft, is the means to launch the offensive capability. The core system itself is not causing the effect; it is simply the means to cause the effect. The core system should be designed for sustainability through maintenance or upgrades for an extended life.

Payload

The payload is analogous to the missiles on the F-22 that cause the effect to the target. The payload is launched by the warfighter at the core system through the access points to the target. These payloads are the capabilities that exploit vulnerabilities on the target system. The payloads may range from zero-day (useful only a few times) to persistent capabilities whose effect withstands patches and upgrades.

The access component is outside the scope of this research. The core system is a stable system similar to currently managed AIS systems in the DoDI 5000.02. Acquiring payloads will be the focus of the rest of this paper.

IV. Innovative Acquisition Approaches by Others

As the U.S. attempts to incorporate procuring cyberspace systems into the acquisition process, what can the commercial market teach about incorporating third-party capabilities? Third-party developers are those developers who are not involved directly in the action. They are not in house developers, i.e., the DoD or commercial entity themselves (first-party), nor are they contracted directly by the DoD to provide a capability (second-party). When looking at how to incorporate third-party software into DoD systems, one may analyze how Facebook, the Apple iPhone, and Metasploit accomplish this very same thing. All three are systems that exploit the cyberspace domain. Facebook is a social media website that allows third parties to develop software applications for its users within the cyberspace domain. The Apple iPhone is a piece of hardware that allows third party developers to create software applications that run on its unique hardware for its customers which connects the users to the cyberspace domain. Metasploit is a penetration testing system that incorporates additional functionality donated by third party software developers for use in and testing of the cyberspace domain. First, a discussion of who these third-party developers are follows.

Third-Party Developers are Useful

A large open source community exists that specifically develops offensive cyberspace capabilities or takes network administration capabilities and adapts them into offensive cyberspace capabilities. This manipulation may be done by adding specific functions or by developing new concept of operations for the capabilities, e.g., using the capabilities in a new way.

Third-party developers have migrated from kids in their basement to a robust, distributed industry. The DoD should look beyond the historically standard developers and consider online developers as well. The hacker community and the open source community are making great strides in developing useful, credible applications.

The stereotype of the hacker community is “an antisocial, pimply faced, teenage boy” (Beaver, 2010). However as Conti assesses, this community is comprised of highly intense and talented individuals (Conti, 2006). By developing cyberspace systems within the hacker community, a better review of these systems is performed. Conti states the hacker community has a more advantageous peer review process, and “you get a more intense and intellectually honest review than you would from your local research group members or academic peers” (Conti, 2005). He mentions this because with local research groups and academic peers, there is a familiarity between the reviewers and the authors. In the hacker community, anonymity allows all reviewers to be more brutally honest. Plus, it allows reviewers from a much wider background to attempt to find fault in one’s work. One’s work is immediately published publically on the internet for the review process. When errors are found, they are also published very publically.

In a similar vein, Mr. Conti mentions that “hacking is more about innovation” and that “hackers are less constrained by conventional thinking” (Conti, 2006). This community is not restrained by the definitions of how to develop cyberspace systems. They are free to innovate and develop new ways to accomplish tasks. These may replace old methods or be new tasks in themselves.

All in all, the DoD should not turn its back on the open source hacking community. They sometimes develop capabilities that do not fit the DoD’s needs, but they also are the ones who developed essential capabilities used by system administrators everywhere such as “Nmap port scanner, the NetCat network utility, and the OllyDbg debugger” (Cross, 2006). All three were developed in the open source community. All three are used extensively in industry and academia.

Facebook

Facebook is a social media site that allows third parties to develop applications users may use for interaction. The basic Facebook site allows users to post pictures, communicate with other users through private or public communication, and post information about themselves. The goal of applications is to make the user's Facebook experience more unique. This includes games, quizzes, or cause statements. Facebook take no responsibilities for these applications. Under their "About Facebook Platform" document, they state "We do not own or run the applications and websites that you interact with through Facebook Platform, and while we try to enforce standards to protect your information, we cannot guarantee that they will follow our rules. You are responsible for evaluating whether you want to use an application or website and whether you want to share information with it." (Facebook, 2009) They are stating that they try to protect the user by issuing standards developers must follow; however, these standards are not binding. Examples of some standards are found in the Statement of Rights and Responsibilities (Facebook, 2010). Section 9 is titled Special Provisions Applicable to Developers/Operators of Applications and Websites. Below are the first few:

> Your access to and use of data you receive from Facebook, will be limited as follows:
>
> 1. You will only request data you need to operate your application.
> 2. You will only use the data you receive for your application, and will only use it in connection with Facebook.
> 3. You will have a privacy policy or otherwise make it clear to users what user data you are going to use and how you will use, display, or share that data.
> 4. You will not use, display, or share a user's data in a manner inconsistent with the user's privacy settings. (Facebook, 2010)

Facebook puts out standards the developers must follow. Facebook then tells the users it is their (the users') responsibility to allow the application access to their information. Facebook is taking no responsibility. In fact, Facebook does not even test the integration of the applications with their Platform. Instead, they have developed a Developer's Wiki (http://wiki.developers.facebook.com/index.php/Main_Page) and a simple Get Started site (http://developers.facebook.com/get_started.php) that walks the developer through attaching their application to the Facebook Platform. Once the developer attaches the application, they are free to advertise it to all the users of Facebook. Facebook does not take any action when new applications are developed or pushed to their users.

iPhone

Apple has created an Apps Store to house Apple's and third-party applications for the iPhone. These applications are only licensed to the user and not sold. Under the Apps Store Terms and Conditions, Apple states that "[t]he Application Provider of each Third Party Product is solely responsible for that Third Party Product" (Apple *Terms*, 2010). Apple takes no responsibilities for the third-party applications in the Apps Store.

However, they do perform some assistance to the third-party developer. Similar to Facebook, Apple has a list of terms the developers must follow under section 3.3 Program Requirements for Developers (Apple *iPhone*, 2010). However, unlike Facebook, which focused very much on the privacy of users' data, Apple focuses on ensuring developers use the Apple API appropriately. The only time Apple takes an active role in third-party applications is in section 6 Application Submission and Selection (Apple *iPhone*, 2010). Once the third-party is confident in the development and testing of the application, it may be submitted to Apple. Apple will then review the application with the associated documentation and decide to either "reject Your Application for distribution for any reason, …; or … select and digitally sign Your Application for distribution via the App Store" (Apple *iPhone*, 2010).

Metasploit

The Metasploit Project is a collection of capabilities for penetration testing (The Metasploit Project, 2010). From their website, the purpose of Metasploit is to "provide information on exploit techniques and to create a functional knowledgebase for exploit developers and security professionals" (The Metasploit Project, 2010). The Metasploit system comprises of a graphical user interface (GUI) which allows users to select a target to attack using capabilities exploiting known vulnerabilities. In this manner, exploit developers may be able to develop exploits against specific vulnerabilities and test them out.

This is a very interesting system for the DoD's offensive cyberspace use. There is the core GUI system which does not have any offensive cyberspace capability itself. The added exploit capabilities submitted on a daily basis are integrated into the core system to provide the additional capability. The core system is similar to having an F-22. The F-22 alone may not be an offensive system, but AIM-120's or AIM-9X's are added to give it an offensive air-to-air capability. Also, new air-to-air missiles can be developed independent of F-22 development for integration as long as they are developed to meet the interface requirements of the F-22. The exploits added to the Metasploit system are similar to the missiles. They must interoperate with the host system but beyond that, are able to develop and be upgraded without changing the host (core) system.

Developers are invited to contribute to the Metasploit Project as testers, tech writers, artists, or module or core developers. The users themselves, as part of the open source community, are invited to take an active role in producing and maintaining a better product.

Once an exploit is developed, "someone on the core team tests third-party submissions when possible" (Moore, 29 Mar 2010). Volunteers that have been accepted into the core team are responsible for testing the new third-part exploits for functionality. However, this is not always accomplished as the Metasploit team is constantly trying to push new exploits and may not have the time. There is a "judgment call about how well the exploit was written" made by the core team (Moore, 29 Mar 2010).

For non-exploits, "all external patches and features are reviewed" by someone on the core team before they are included (Moore, 24 Mar 2010). If the patch causes an error, it is that core team member's responsibility to roll it back.

Metasploit utilizes a volunteer group of core team members to review and test submitted code following a checklist-based testing methodology. New exploits are not always reviewed because of their daily additions, but patches to the core system are. Because this is a volunteer organization and they "generally don't know who uses a piece of code until we break it", the Metasploit team does "not guarantee the usability of the development codebase" (Moore, 29 Mar 2010; 24 Mar 2010).

Summary

None of these models are useful for the DoD to implement when using third-party developers. All three rely on the user to accept the risk. This is not an acceptable model for a program office to follow in that the program office would be forcing the warfighter to accept the risk while the program office accepts none. While risk is never completely removed from a cyberspace capability, the program office needs to understand the risks of the system fully and be able to communicate these risks to the warfighter. While these three examples do limit the risk by forcing developers to conform to a standard interface, it is not enough for DoD applications.

However, this does show that all three successful commercial platforms (Facebook, Apple's iPhone, and Metasploit) are increasingly relying upon third-party developers for software capabilities. They are opening the doors to non-standard developers such as the open source community and hackers. These communities can develop effective capabilities quickly and adapt to constantly changing cyberspace environment. The DoD must consider these developers when acquiring cyberspace systems.

V. Recommended Policy Changes

The DoD acquisition process is not broken. Evolutionary Acquisition is an appropriate method for procuring cyberspace systems that undergo fast technology changes. Offensive cyberspace systems are comprised of three components. One is provided by the IC (the access), the second is similar to most AIS systems (core system), but the third requires additional caveats (payloads). Five caveats follow for procuring effective payloads for offensive cyberspace systems:

- Expanding the network of development activities,
- Building payloads for specific targets,
- May need to keep systems classified,
- Understand what type of sustainment is needed for cyberspace capabilities, and
- Testing throughout the acquisition process.

Expanding the Network of Development Activities

Similar to the three commercial companies previously discussed, the DoD should not ignore the third-party market on the internet. There exist many open source capabilities that have demonstrated their effectiveness in the commercial market already. Other capabilities have been used by the hacker community to perform limited offensive cyberspace attacks. The DoD should consider all these capabilities, however, they should be acquired in such a way that they are trusted and timely.

As the hacking community currently demonstrates, a cyberspace capability developed for one purpose (e.g., system administration) may be used for another (e.g., unauthorized remote system control). Many of the current successful hacking systems such as Metasploit, Nessus, and Nmap began as system administrator systems for either discovering vulnerabilities on their systems or monitoring the connections of their networks (Skoudis, 2006). During the AoA for the cyberspace system, the program office should consider the open-source hacking and system administrator capabilities. These capabilities have demonstrated their effectiveness and can aid in the technology maturation as full fledged capabilities, capabilities or systems that require some modification, or a starting point for developers. This will require the program office to be more active in selecting a development path. It requires the program office to actively research what is available instead of passively waiting for developers to respond to a request for proposals.

Code Review

If the program office acquires a capability used by the commercial sector that is freely distributed on the web, the capability may contain malicious software hidden within it. One way developers attempt to combat people inserting malicious logic and redistributing the code is by advertising the hash of the original capability. This is not enough for the DoD. The DoD must perform code review to ensure the original developer did not insert malicious logic. To perform a credible code review, the program office must have a reviewer familiar with the programming language to understand completely what the system is doing. Computer languages, be they object oriented or scripting, have unique characteristics that operate differently from one another. Only someone who is familiar enough with the language will be able to discover them. This may require the program office to hire an outside consultant. This consultant must be independent from the developer of the capability, an expert in the language, and trusted. Independence gives the program office credibility. Someone funded by the program office objectively is reviewing the code allowing a better chance of discovering errors or malicious logic. Expertise is required as stated before because developers can hide malicious logic within the code. The reviewer must be trusted to provide honest feedback as the reviewer may be the only expert opinion used for fielding an offensive cyberspace weapon system, a DoD weapon system.

Code Recompile

As stated previously, cyberspace systems downloaded from the web may not always be clean, i.e. they may contain malicious logic in them that is not documented. Therefore, the code should be recompiled from the program offices-approved source code. This is the only way to guarantee that the cyberspace system is performing what and only what it was designed and understood to perform.

Specific systems may exist that are the best buy to meet a specific capability gap that the DoD can only acquire the executable and not the source code. For these instances, the program office must articulate the risk of the possibility of malicious logic in the executable to the warfighter making the decision on fielding. The program office may mitigate this risk through extensive research for what others have discovered, but they must also do their own testing to confirm.

Building Payloads for Specific Target Sets

As the Defense Acquisition Reform Panel stated "challenges with the requirements process are a major factor in poor acquisition outcomes" (Andrews, 2010). It continues to say one of the biggest problems is "requirements creep" (Andrews, 2010). Requirements creep is when the required capabilities the delivered system should provide continue to change throughout the acquisition process. Even though the requirements for the overall system is documented in the ICD, CDD, or Capability Production Document (CPD), each block in the evolutionary acquisition must limit which requirements (capabilities) will be delivered in that block.

For payloads addressing the requirements for an offensive cyberspace weapon system, very specific requirements should be addressed and not changed to ensure the payload is delivered timely to be effective. Instead of developing an overall offensive cyberspace weapon system that can address multiple targets, payloads should be developed instead that target a specific vulnerability on a specific type of system. Instead of developing a system that targets Internet Protocol (IP)-based systems, develop instead myriad payloads that target specific vulnerabilities of an IP-based system. The myriad payloads will be integrated into one overall system though integration with the core system. By focusing each development effort on specific vulnerabilities, the payloads should be developed quicker and delivered in a timely manner. Payloads should not only target one vulnerability but also one type of target. Payloads should be developed that target Linux systems while another payload will target Windows systems. Depending upon the vulnerabilities, a payload might be needed for each instance (e.g., Windows XP, Windows 7, or Windows 2000) of the Windows target system. This has the drawback of the warfighter being responsible for many more payloads in their arsenal than before. The core system should be developed to handle this configuration management issue. The payloads should integrate with the core system such that the warfighter, when describing a target, is only presented those payloads that are effective against it. Therefore, even if the core system currently contains 100 payloads, only 50 may target Windows and of those 50 only 20 target Windows XP. These 20 would be displayed to the warfighter to select when planning the mission against a target running Windows XP.

An example is Metasploit, a system that already performs this configuration management. Once the target is selected, a list of vulnerabilities is displayed to exploit that type of target. These vulnerabilities next present a list of exploits that may be used against the target system. As explained earlier, new exploits are added to the core Metasploit system. These new exploits are the equivalent to the payloads the DoD would be developing.

Security Classification

Determining the CPIs of cyberspace systems and how to protect them through classification is essential to success. As stated previously, three types of information about a system can be classified: existences, capabilities, or CONOPS. Each system will require analysis for unique classification requirements, but the following is a guide.

Because the DoD relies on the civilian sector for much of their defensive cyberspace capabilities, the existence of these capabilities does not need to be protected. These are the same or derivatives of products available to the commercial market. Along with the existence, the DoD does not need to classify the capabilities of these systems. Especially for commercially produced products, there is no reason to hide the capabilities for they are available to all. For non-commercial-off-the-shelf products, the DoD may wish to keep some parts of active defensive capabilities protected. These would be capabilities that are not available on the commercial market and cannot easily be studied.

The CONOPS of the defensive cyberspace capabilities should be protected. Not all the CONOPS, such as patching or requiring authentication, because these are similar to the civilian sector, but specifics of how the patches arrive from the vendor (if unique) or how the DoD reacts to contain a cyberspace attack. These actions may be unique for the DoD based on research, testing, and experience that validates the best method. While the defensive capabilities themselves are in the public domain and can be studied by the adversaries, that information (CONOPS or capabilities) developed uniquely for the DoD should be deemed CPI and protected through classification.

Unlike the defensive capabilities, the offensive capabilities are unique to the DoD. While civilian sector capabilities may be used for offensive purposes similar to computer hackers using network administrator systems, the specifics must remain classified. If the DoD does select a commercially available system to turn into an offensive cyberspace capability, the existence of using this system should be protected. If the adversary was to learn the exact commercially available system the DoD used to target them, the adversary would be able to acquire the same system, study it, and develop defenses against it.

General capabilities may be articulated such as capability to take down an adversary's power grid, but the capabilities used, the vulnerabilities exploited, and the CONOPS to succeed must all remain classified. The vulnerabilities exploited can often be easily patched if the adversary is aware, but because networks are so large and interconnected, one vulnerable system may be missed. By exploiting the one vulnerable system, the system will function as designed. The CONOPS explain how the warfighter will use these capabilities against a vulnerability to cause an effect. If any of these three are discovered by the adversary, a patch will often nullify the effectiveness of the offensive cyberspace weapon system.

The U.S. Government has started this effort. Just this past March, the White House has declassified an outline of a "major government effort to protect its computer networks" (Nakashima, 2010). This effort as part of the Comprehensive National Cybersecurity Initiative (CNCI) addresses the protection of private sector computer systems. Portions that dealt with the National Security Administration's (NSA) role in cyberspace security were declassified while the government's offensive cyberspace capabilities remained classified.

Understand Sustainment of Cyberspace Capabilities

The Life-Cycle Sustainment Plan (LCSP) started in the Technology Development phase and continually updated throughout the acquisition process should include information about the sustainment of the system (DAU, 2010). The metrics developed by the program office for choosing the appropriate sustainment plan need to be rethought when it comes to payloads. While most acquisition processes focus on developing systems for long life expectancy in the Operations and Support phase because this often provides the best buy, not all cyberspace capabilities should be developed for such a long life. The offensive cyberspace core system should be developed with a sustainment plan to keep the system effective for a long duration, but many payloads that focus on specific vulnerabilities should be designed to only live for the period that those vulnerabilities exist. These vulnerabilities may change as the adversary patches their target systems through normal operations or perform a tech refresh on the systems replacing the entire network. For example, a payload that relies on a zero-day exploit should not have a life expectancy beyond a few months after initial use. While the payload is not expected to become ineffective immediately, its effectiveness will decrease as adversaries who witnessed the initial attack begin to patch their exploited vulnerability.

This is significant for the operations and support phase of some programs "account for about 60 to 70 percent of a system's total life-cycle costs" (GAO, 2000). They far outweigh the cost of the development and procurement. However, for the cyberspace capabilities that do not require long sustainment because their effectiveness will lessen as target systems are patched or replaced, the DoD must redistribute the money from these phases. Program offices should not force a long term sustainment plan onto a system that is not expected to live a long time. Instead the program office should ensure the sustainment of the system is appropriate.

Testing Throughout the Acquisition Process

While Developmental Testing (DT) occurs throughout the development process, Operational Testing (OT) is performed during the Production and Deployment phase. All of these testing events add time and effort to the development of the system. Because the DoD development community is small for these efforts, the same people helping with the development will also aid in the testing. These people's workload is interrupted because of all these test events. By consolidating and focusing the testing events on what is most needed, the system can be delivered more quickly to the warfighter.

The purpose of Test and Evaluation (T&E) as presented in Air Force Instruction 99-103 is to “mature system designs, manage risks, identify and help resolve deficiencies as early as possible, and ensure systems are operationally mission capable” (DAF, 2009). DoDI 5000.02 states the purpose is “to provide knowledge to assist in managing the risks involved in developing, producing, operating, and sustaining systems and capabilities” (USD(AT&L), 2008) One of the general T&E principles is tailoring: “T&E strategies and plans must be flexible to fit the needs of the acquisition program” (DAF, 2009). For payloads, integrated testing provides a tailoring method that saves time to field the system.

Integrated testing combines the DT team with the OT team and any other testers into one. This Combined Test Force (CTF) performs planning and testing as one unit. This allows both the DT and OT to use the same testing events to gain their required data. The advantage is a savings of testing events.

For payloads derived from third-party/commercially available capabilities, only integrated testing by the CTF is needed. Most integrated testing is still divided between the DT-led events and the OT-led events. For these payloads, only the OT-led events are necessary.

DoDI 5000.02 states that the “materiel developer” conducts DT (USD(AT&L), 2008). For a commercially developed capability, the material developer has already performed testing before releasing the final product to the commercial market. For open source developed capabilities, there is no specific materiel developer to task with testing. The open source community as a whole performs parts of the testing. The “technical capabilities and limitations” and the “design technical risks” can all be discovered under a CTF (USD(AT&L), 2008). Except for integration with the core system which is new code, the OT-led events will be enough.

OT is designed to “determine the operational effectiveness and suitability of a system” (USD(AT&L), 2008). The environment a payload operates in is not significantly different from the development environment. For many DoD acquired systems, the two environments are significantly different. For example, an F-22 being flown by a professional test pilot and being maintained by the engineers who developed the aircraft is significantly different than the operational F-22 flown by a fighter pilot newly trained on the aircraft and maintained by an overworked shop of maintainers with varying levels of expertise. Payloads from commercial sources have already demonstrated their functionality; that is why they were selected in the first place. All that needs to be tested is to ensure payloads meet the warfighter’s need.

While some may say the integration of the payload with the core system can be performed as part of Force Development Evaluation (FDE), calling it part of the operation and sustainment of the core system, this is incorrect. The core system, even though it is under operational management of the warfighter, still must follow the program office’s sustainment plan. That sustainment plan includes ensuring the system is effective. Integrating new payloads into the core system ensures the effectiveness of the system. Therefore, DT-led CTF events must test the integration.

VI. Conclusion and Future Research

Even with the speed of development for cyberspace capabilities, the DoD acquisition process is still appropriate. Five aspects of the DoD acquisition process must be adapted by the program office when acquiring cyberspace systems. First, all developers of cyberspace capabilities should be considered including the open source community. Secondly, offensive cyberspace weapon systems must be developed to go against specific targets. Building more capability into a cyberspace system slows the development such that the system may be outdated and ineffective before fielding. The scope of capabilities should be very narrow for payloads. Thirdly, for offensive cyberspace weapons, the commercially acquired capability may be classified as critical program information and protected through classification. Fourth, most payloads should be developed with very little sustainment. While all systems must consider disposal, payloads should be thought of as throw-away capabilities because the vulnerabilities they exploit can quickly change. Their disposal happens sooner. Finally, very little if any developmental testing needs to be conducted for those systems acquired from the open source community. Instead, the combined test force should focus on operational testing to characterize the system.

Future research in the field of offensive cyberspace weapon systems should focus on how to characterize the reliability of the systems. The cyberspace systems' effectiveness relies not only on the capability itself but like all weapon systems on the environment. The cyberspace environment being malleable can be adjusted by the adversary. Therefore, the effectiveness of the system depends upon the adversary's cyberspace environment.

Commanders and targeteers use the Joint Munitions Effectiveness Manual (JMEM) when selecting the appropriate weapon for a mission. The offensive cyberspace force must develop a manual that can characterize the effectiveness of all their capabilities. To do this, a credible characterization of cyberspace systems must be developed and accepted by the warfighting community.

While this research proposed policy changes to aid in the acquisition of offensive cyberspace weapon systems, this is assuming that the acquisition process is appropriate for these systems. Further research should analyze if our current method of acquisition is appropriate at all for acquiring and developing cyberspace capabilities. It may be that the program offices are not structured for this quick acquisition. Instead the warfighter may treat the acquisition of payloads as operations and maintenance of the core systems.

Bibliography

Andrews, Rob. *Defense Acquisition Reform Panel Chairman Rob Andrews Expert Perspectives on Managing the Defense Acquisition System and The Defense Acquisition Workforce*. Washington: House Armed Services Committee, 25 February 2010.

Apple. "Terms and Conditions." Website. http://www.apple.com/legal/itunes/appstore/ca/terms.html. 1 April 2010. Retrieved 18 May 2010.

Apple. *iPhone Developer Program License Agreement*. Apple, 22 January 2010.

Beaver, Kevin. *Hacking for Dummies 3rd edition*. Hoboken, NJ: Wiley Publishing Inc., 2010.

Bush, George W. *Executive Order 13292 – Further Amendment to Executive Order 12958, as Amended, Classified National Security Information*. Washington: Federal Register Vol 68, No 60, 25 March 2003.

Conti, Gregory. "Hacking and Innovation," *Communications of the ACM*, 34-35 (June 2006).

Conti, Gregory. "Why Computer Scientists Should Attend Hacker Conferences," *Communications of the ACM*, Vol. 48, No. 3: 23 – 24 (March 2005).

Cross, T. "Academic Freedom and the Hacker Ethic." *Communications of the ACM*. 37 – 38. (June 2006).

Defense Acquisition University (DAU). "Defense Acquisition Guidebook." Website. https://dag.dau.mil/Pages/Default.aspx. 5 May 2010.

Defense Acquisition University (DAU). *PMT 352B Seminar Book – "Big A" Acquisition*. Washington: Defense Acquisition University, January 2009.

Department of Defense (DoD). *Joint Doctrine for Information Operations.* JP 3-13. Washington: Joint Chiefs of Staff, 13 February 2006.

Department of Defense (DoD). *Joint Intelligence Preparation of the Operational Environment*. JP 2-01.3. Washington: Joint Chiefs of Staff, 16 June 2009.

Department of the Air Force (DAF). *Information Operations*. AFDD 2-5. Washington: HQ USAF, 11 January 2005.

Department of the Air Force (DAF). *Capabilities-Based Test and Evaluation*. AFI 99-103. Washington: SECAF, 20 March 2009.

Department of the Air Force (DAF), "24th Air Force – 67th Network Warfare Wing." Website. http://www.24af.af.mil/units/67nww.asp. Retrieved on 17 May 2010.

Dunlap, Charles J. "How We Lost the High-Tech War of 2007." *The Weekly Standard*, Vol. 001, Issue 19 (29 January 1996).

Facebook. "Developers About." Website, http://developers.facebook.com/about. 28 August 2009. Retrieved on 17 May 2010.

Facebook. "Statement of Rights and Responsibilities." Website. http://www.facebook.com/terms.php. 22 April 2010. Retrieved on 17 May 2010.

General Accountability Office (GAO). *Defense Acquisitions: Higher Priority Needed for Army Operating and Support Cost Reduction Efforts.* Washington: GAO. September 2000.

Intel. "Moore's Law: Made real by Intel innovation." Website. http://www.intel.com/technology/mooreslaw/index.htm. Retrieved 18 May 2010.

The Metasploit Project. "Metasploit." Website. http://www.metasploit.com. 12 March 2010.

Moore, Gordon E. *Cramming more components onto integrated circuits.* Electronics, Vol 38, No 8. (19 April 1965).

Moore, HD. "Testing Question." Electronic Message. 1518EST, 24 March 2010.

Moore, HD. "Re: Testing Question." Electronic Message. 0232EST, 29 March 2010.

McChrystal, Stanley A. *Joint Capabilities Integration and Development System*. CJCSI 3170.01G. Washington: Joint Staff, 1 March 2009.

Mullen, M.G. *Joint Operations*. Joint Publication 3-0. Washington: Joint Staff, 22 March 2010.

Nakashima, Ellen. "White House declassified outline of cybersecurity program." *The Washington Post*. 3 March 2010.

OpenTheGovernment.org (OTG). "Secrecy Report Card: Quantitative Indicators of Secrecy in the Federal Government." Report. http://www.openthegovernment.org/otg/secrecy_reportcard.pdf. 26 August 2004. Retrieved 24 May 2010.

Phister, Paul W. and others. "CyberCraft: Concept Linking NCW Principles with the Cyber Domain in an Urban Operational Environment," Rome, NY: Air Force Research Lab, 2005.

Rattray, Gregory J. "An Environmental Approach to Understanding Cyberpower." *Cyberpower and National Security*. ed Franklin D. Kramer, et al. Dulles, VA: National Defense University and Potomac Books, 2009.

SAF/USAM. *Air Force Acquisition Action Officer 101*. Washington: SAF/US, July 2006.

Skoudis, Ed, and Tom Liston. *Counter Hack Reloaded.* Upper Saddle River, NJ: Prentice Hall, 2006.

Software Technology Support Center (STSC) CrossTalk: The Journal of Defense Software Engineering. "STSC CrossTalk – Evolutionary Acquisition and Spiral Development." Website. http://www.stsc.hill.af.mil/CrossTalk/2002/08/easd.html. August 2002. Retrieved on 17 May 2010.

Under Secretary of Defense for Acquisitions, Technology and Logistics (USD(AT&L)). *Operation of the Defense Acquisition System*. DoDI 5000.02. Washington: DoD, 8 December, 2008.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

1. REPORT DATE *(DD-MM-YYYY)* 02-06-2010	**2. REPORT TYPE** Graduate Research Paper	**3. DATES COVERED** *(From – To)* Jun 2009 – Jun 2010

4. TITLE AND SUBTITLE Policy Changes for Acquisition of Offensive Cyber Systems	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Casey, Brendan K., Maj, USAF	**5d. PROJECT NUMBER** N/A
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765	**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT/ICW/ENG 10-02
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) 350th Electronic Systems Wing OL-AA 950 ELSG/NWC Attn: Maj Mark Saeger San Antonio, TX (210) 925-6679 (mark.saeger@us.af.mil)	**10. SPONSOR/MONITOR'S ACRONYM(S)** OL-AA 950 ELSG/NWC
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Because the cyberspace environment is changing so quickly, the slow, methodical Department of Defense (DoD) acquisition process may not suffice. By following the evolutionary acquisition method and incorporating five policy caveats, the DoD acquisition process can acquire effective systems quickly.

The purpose of this research is to provide recommended policy changes in the acquisition of offensive cyberspace weapon systems for the Air Force and DoD in general. This paper describes the current DoD acquisition process, explains how cyberspace is different from the other domains, discusses a few innovative acquisition and development approaches, and concludes with the recommended policy changes. A literature search on the cyberspace community along with DoD and Air Force doctrine provided the bulk of the research.

The recommended acquisition policy changes fall into the following categories: expanding the network of development activities, building payloads for specific target sets, security classification, sustainment of cyberspace capabilities and testing throughout the acquisition process.

15. SUBJECT TERMS
Cyberspace; Acquisition; Offensive Cyberspace; Components of Offensive Cyberspace Weapon System

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Robert F. Mills, PhD (ENG)
REPORT **U**	**ABSTRACT** **U**	**c. THIS PAGE** **U**	UU	50	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, x4527 (robert.mills@afit.edu)