Examining Acquisition Leaders' Readiness to Support Future LandCyber Operations

Matthew Lee

April 15, 2014

PUBLISHED BY
The Defense Acquisition University
Project Advisor: Jeffrey Caton
The Senior Service College Fellowship Program
Aberdeen Proving Ground, MD

Table of Contents

List of Figures

List of Tables

Abstract

The purpose of this research is to help define the necessary foundation for the acquisition leader's readiness for LandCyber operations through the next decade. This research examines potential acquisition leader knowledge and training gaps in cybersecurity that influence the cybersecurity shortfall risk in the weapon systems developed and fielded to the warfighter. The results may facilitate the U.S. Army Acquisition institution's development of curriculums to prepare leaders and improve readiness in support of LandCyber operations. Many works in the literature indicate a need for more cybersecurity training and address the impact of training on the weapon systems that support LandCyber operations. A survey of acquisition leaders is used to collect cybersecurity knowledge, skills, and abilities (KSAs) in determining individual knowledge, awareness level, and training gaps.

Survey data collected from 156 acquisition leaders provide information to determine their readiness level base on the predefined readiness level criteria. Statistical analysis of findings indicates acquisition leaders' readiness is at the level just below average. Further analysis of the data results in the acquisition leaders' readiness at the lowest level. Whether acquisition leaders' level of readiness is just below average or at the lowest, research shows that the level is below what is necessary for acquisition leaders to be able to support LandCyber operations, especially in the constantly changing future. Cybersecurity and resilience can be improved by acquisition leaders who have a clear understanding of what cybersecurity is and by ensuring that acquired weapons systems are secure and risks are managed and mitigated. The findings from survey data show that leaders and the workforce need to understand cybersecurity through increased training and education. This paper makes several recommendations that can improve acquisition leaders' readiness to support LandCyber operations.

Chapter 1 – Introduction

Background

Internet usage has increased exponentially in the past decade (Figure 1; Internet Live Stats, 2014). This increase is expected to continue in the next decade. The Internet is the key enabler of cyberspace, a global domain within the information environment, consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (Joint Staff, 2013). Any devices that connect to the network are considered to be in cyberspace; this includes most weapon systems. According to the Department of Defense (DoD, 2011), DoD must address cyber vulnerabilities. *Joint Publication 3-12 (R)* defines cyberspace operations as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace" (Joint Staff, 2013, p. v). Cybersecurity is part of the defensive aspect of cyberspace operations.

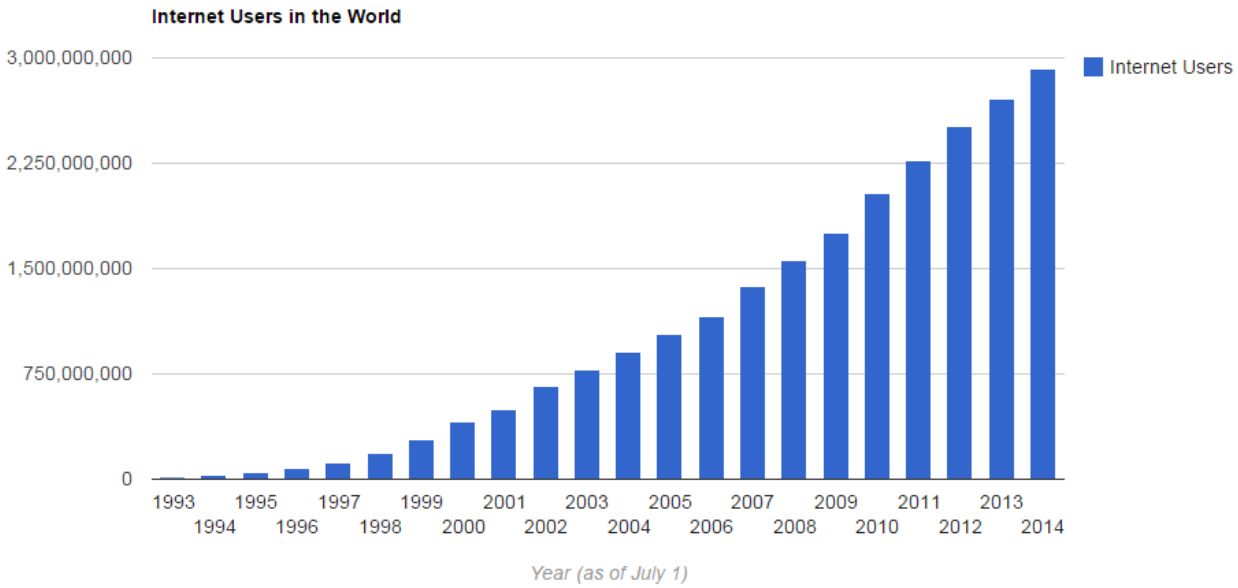
For information dominance and superiority, almost all weapon systems are connected to cyberspace and affect Army operations on the ground, requiring a new framework called LandCyber:

> LandCyber is a unified overarching operational and institutional solution framework to account for cyberspace [in] all aspects of Army operations. It transforms an Army dominant on the ground into an Army able to sustain operations in and among populations active physically on land and virtually in cyberspace. (U.S. Army Cyber Command, 2013, p. iv)

The paradigm shift from Army land operations to LandCyber operations necessitates a change to the education and training of our warfighters and workforces. Appendix A lists some of the emerging cyber doctrine/policy, studies, and latest cyber news and events.

Preliminary evidence from prior research, doctrine, and policies indicates a need to train and educate our acquisition leaders (any employee in a leadership role, including branch chiefs, team leaders, supervisors, and above) on cyberspace and how each can influence LandCyber operations. Acquisition leader cybersecurity readiness affects the development and maintenance of more secure weapon systems. For this study, readiness is defined in five levels.

- Level one = no knowledge of cyberspace.
- Level two = some cybersecurity training completed.
- Level three = previous level plus an understanding of what cyberspace operations are and how they impact land warfare, and an understanding of the current and future theater-level risks and threats.
- Level four = previous level plus an understanding of DoD Information Technology Security Certification and Accreditation Process (DITSCAP), DoD information Assurance Certification and Accreditation Process (DIACAP), and Risk Management Framework (RMF), and of the differences between them.
- Level five = previous level plus achievement of cybersecurity certification.



Source: Reprinted with permission from Internet Live Stats (2014); copyright by internetlivestats.com

Figure 1 – World Internet Users Trend

Significant research has not been conducted to explore acquisition leaders' cybersecurity readiness. The research detailed in this paper assesses the current acquisition leader readiness and the appropriate level of readiness necessary to maximize acquisition support to provide weapon systems with minimum cyber vulnerabilities to our warfighters.

Problem Statement

If acquisition leaders do not understand cybersecurity and the associated threats, leaders will not know what preventive measure to take to address or eliminate cyber vulnerabilities. Cyber vulnerabilities in all phases of the weapon system acquisition life cycle will not be conscientiously mitigated or eliminated if people do not understand the issues. This research paper helps to define the necessary foundation for the acquisition leader's readiness for LandCyber operations through the next decade.

Purpose of This Study

The purpose of this study is to analyze the acquisition leaders' readiness to support future LandCyber operations. The proliferation of cyberspace increases opportunities and vulnerabilities. Based on literature reviews and survey findings, the research will determine whether current acquisition leaders are ready to support future LandCyber operations. The reviews and findings will also help define the possible training gap to prepare acquisition leaders better to support future LandCyber operations.

Significance of This Research

According to a DoD and General Services Administration (GSA) report (2013), acquisition leaders need to understand cyber risk before they become accountable for the cybersecurity risks when developing and fielding the products:

> Identify and modify government acquisition practices that contribute to cyber risk. Integrate security standards into acquisition planning and contract administration. Incorporate cyber risk into enterprise risk management and ensure key decision makers are accountable for managing risks of cybersecurity shortfalls in a fielded solution. (p. 8)

This research examines acquisition leaders' potential knowledge and training gaps in cybersecurity that influence the cybersecurity shortfall risk in the weapon systems. The results may facilitate the U.S. Army Acquisition institution in the development of curriculums to prepare leaders and improve readiness in support of LandCyber operations.

Overview of the Research Methodology

This study uses both quantitative and qualitative design. The research method includes a literature search concerning acquisition leader cybersecurity awareness and training that have impact on the cyber risk of weapon systems.

An online survey via SurveyMonkey was developed and implemented to collect cybersecurity knowledge, skills, and abilities (KSAs) from 1,800 Aberdeen Proving Ground (APG) civilian leaders to determine their readiness level and possible gaps. Two hundred thirty-six APG civilian leaders responded, a response rate of approximately 13%. The survey also collected some qualitative data on training needs from the respondents. The survey allowed respondents to self-assess based on the questions asked to determine individual knowledge, awareness level, and training gaps.

Research Questions

What are acquisition leaders' readiness levels in cybersecurity to support LandCyber operations?

What are the cybersecurity training needs for acquisition leaders to prepare them better in support of LandCyber operations?

Research Hypothesis

Current cybersecurity awareness and training of acquisition leaders is insufficient to support LandCyber operations.

Objectives and Outcomes

The study identifies the cybersecurity readiness level for acquisition leaders through the quantitative survey of the sample of APG acquisition leaders. The survey and qualitative literature review help define necessary training for acquisition leaders in the area of cybersecurity.

This research focuses only on the cybersecurity that is part of the defensive aspect of cyberspace operations. Therefore, it provides a basis for a future in-depth study of the entire

cyberspace operations readiness level for acquisition leaders that can be used to improve future LandCyber operations.

The acquisition leaders' knowledge in cybersecurity is insufficient to support LandCyber operations. DoD, Army Cyber, and acquisition communities need to institutionalize appropriate cybersecurity training and education to prepare our acquisition leaders in order to support LandCyber operations.

Limitations of the Study

Due to the time limitations of this research, the focus is on the cybersecurity that is part of the defensive aspect of cyberspace operations and on acquisition leaders' readiness level as perceived by the survey population.

This study is limited to the survey population of APG, composed of 236 civilian leaders who responded. Because there is no official benchmark for cybersecurity readiness levels, the readiness levels are defined in the background section. The survey population of APG leaders is not a control group and the readiness level is self-assessed based on the survey question responses. Possible cybersecurity training options are suggested based on survey responses and the literature review.

The APG population comprises a mixture of acquisition leaders that is similar to other posts, camps, and stations. Therefore, it provides a good sample that represents the entire United States. Given additional time, it is recommended that this study be expanded to examine the entire cyberspace operations readiness level for all acquisition leaders.

Validity of the Research

Possible threats to validity include the selection of references, extraneous variables, and any biases of the APG acquisition survey respondents. The research gathered survey responses

from 236 leaders within APG, Maryland. Extraneous variables include new doctrines and institutionalized training and cyber components' training strategies. By including these extraneous variables in the research, I can account for the impact of these variables on acquisition leader's cybersecurity readiness assessment and training recommendations. The survey repondents' individual interpretations of cyber definitions could vary based on bias. Several major cyber definitions were given on the survey to help mitigate bias that may be due to imprecise language. Another limitation is the number of survey respondents, which limits the accuracy of the sample.

Reliability of the Responses

Cyberspace and LandCyber operations are rapidly changing, and this study provides a snapshot in time of various situations and scenarios. Within the timeframe of this study, the research can easily be replicated with similar results with a review of doctrines and policy as referenced. In addition, the survey data can be evaluated, but resubmitted survey questionnaires may result in different responses based on changes in the population and changes in surroundings.

Chapter 2 – Literature Review

This chapter captures the source information from the literature on the growth of cyberspace usage, the emergence of the cyberspace domain in DoD, the creation of LandCyber in the Army, the need for cybersecurity to protect the cyber vulnerabilities, and leadership understanding of and training in cybersecurity. The proliferation of cyberspace usage creates cyber opportunities and vulnerabilities. The increase in vulnerabilities, threats, and risks creates a demand for new policies, standards, and regulations that will help original equipment manufacturers (OEMs) to build more secure systems, including weapon systems.

With DoD's heavy emphasis in the new cyberspace domain and Army's LandCyber, the Army is in an up-tempo situation in establishing cyber organizational entities to support Army LandCyber and the cyberspace domain. Acquisition plays a major role in preventing cyber vulnerabilities on weapon systems and the DoD information network. Acquisition leaders must first understand the cyberspace operations, cyber vulnerabilities, and cybersecurity standards, policies, and doctrine to ensure that the weapon systems and DoD information networks created meet the cybersecurity standards, and they must continuously monitor the risks through the life cycle of the systems and networks. The information from this literature review is presented in the following four sections:

- The increased usage and impact of cyberspace
- The emergence of the cyberspace domain and the creation of LandCyber
- Cybersecurity and impacts on weapon systems
- Acquisition leaders' need to understand cybersecurity

Increased Usage and Impact of Cyberspace

Acquisition leaders need to understand the basis of cyberspace and how it affects DoD and Army operations. Internet usage is expected to continue to increase in the next decade. The *2014 Quadrennial Defense Review* (QDR; U.S. Department of Defense, 2014) emphasized strategic challenges and opportunities to protect our Nation. It included cyber as one of the key capability areas along with missile defense and nuclear deterrence: "We will invest in new and expanded cyber capabilities and forces to enhance our ability to conduct cyberspace operations and support military operations worldwide, to support Combatant Commanders as they plan and execute military missions" (p. x). Cyberspace has changed peoples' way of life and created many opportunities due to the increase in communication capabilities. However, it also presents security challenges and risks through cyber vulnerabilities.

As more systems enter into cyberspace to take advantage of the opportunities and increase capabilities, the threats and risks grow. Due to the interconnectivities through cyberspace, threats and risks not only occur in the tactical edge but all the way back to the strategic center command at posts, camps, and stations. "As the frequency and complexity of cyber threats grow, we will continue to place high priority on cyber defense and cyber capabilities" (U.S. Department of Defense, 2014, p. 14). DoD will continue to support other Federal Government cybersecurity teams such as those at the Department of Homeland Security, Central Intelligence Agency, and Federal Bureau of Investigation. DoD needs to continue to invest in cybersecurity and ensure that OEMs comply with security standards and keep pace with advances in technology to prevent cyber vulnerabilities. QDR's acknowledgement of cyber criticality includes the following statement: "The Department of Defense will continue to invest

in new and expanded cyber capabilities, building on significant progress made in recent years in recruiting, training, and retaining cyber personnel" (U.S. Department of Defense, 2014, p. 32).

At a recent West Point visit in January 2015, ADM Michael Rogers, commander of United States Cyber Command (USCYBERCOM), said that Cyber Mission Force will have 6,200 people forming 133 teams. This is consistent with the cyber mission force structure identified in the 2014 QDR. USCYBERCOM's achievement of full operational capability in October 2010 constituted establishment of the fifth domain, cyberspace, along with air, land, sea and space.

Emergence of the Cyberspace Domain and the Creation of LandCyber

Cyberspace domain emergence has each of the Services scrambling to integrate cyber into their normal operations. Cyberspace was recognized as a new domain by the Pentagon's cyber strategy after the flash drive incident in the Middle East in addition to other attacks and threats that have emerged (Lynn, 2010). An Army field manual, *FM 3-38*, (Headquarters, Department of the Army, 2014) provides overarching doctrinal guidance and direction on cyber electromagnetic activities, comprising cyberspace operations, electronic warfare, and spectrum management operations. To support the hypothesis of this paper, the concentration will be on cyberspace operations, with less emphasis on electronic warfare and spectrum management operations.

The cyberspace domain is considerably different than the land, air, maritime, and space domains. Cyberspace is an artificial domain consisting of a system-of-systems that exits through the four natural domains. Operations in the four natural domains are confined to the physical place, while cyberspace "greatly expands and complicates the operational framework,

transforming a limited physical battlefield to a global battlefield" (Headquarters, Department of the Army, 2014, pp. 1-5).

The U.S. Army LandCyber White Paper 2018–2030 indicated that the Army must adjust to the convergence of land and cyberspace domains and that failure to adapt surrenders the advantage in cyberspace to future adversaries: "The Army must become one that is organized, trained, and equipped to shape human and machine behavior on land and in cyberspace" (U.S. Army Cyber Command, 2013, p. iv). Given the financial state the Army is facing and the new cyber threats, the Army is supporting the Joint Operations by consolidating the Land operations and Cyberspace operations to form LandCyber Operations. "The convergence of land and cyberspace operations is driving transformational change in Army operations. Land and cyberspace operations will continue to converge creating increased interdependence and, coupled with the momentum of human interaction, create complex operating environments" (U.S. Army Cyber Command, 2013, p. v).

The Army LandCyber White Paper 2018–2030 posited the understanding that, in the near-term, the United States has the technological advantage over the adversaries. The mid-term will be a tie if the United States is leveraging commercial, off-the-shelf, cloud-based technology, which allows adversaries to utilize the threats found in the cloud. Long-term strategy will give the United States the advantage by enabling a cyberspace-educated and trained Armed Forces to use advanced technology such as fiber optic, electromagnetic, and laser to pass information.

The LandCyber commander will have the cyberspace defensive force to provide protection through the use of reconnaissance, surveillance, and counterintelligence from sensors and intrusion detection and prevention capabilities. The LandCyber concept resembles to the Army's older concept of the AirLand battle. The LandCyber framework allows the land

commander a holistic view of the combined operations, including land and cyberspace opportunities, tasks, and vulnerabilities (U.S. Army Cyber Command, 2013).

The current Army forces do not have the cyberspace capabilities to withstand the cyber threats and to mitigate the cyber risks. The Army is continuously building and training the "cyber corps" to complement the ground forces to function in LandCyber operations. The U.S. Army Training and Doctrine Command and West Point are working hard to rapidly expand the cyberspace capabilities.

LTC John Rafferty (2013) questioned the LandCyber strategy in the *White Paper 2018–2030*. In theory, the LandCyber operations construct provides the unified commander with the capability to prevent, shape, and win the Nation's wars. If the LandCyber operations are not implemented carefully and correctly, then vulnerabilities in the cyberspace will overcome the advantage and become a double-edged sword that is self-defeating. Rafferty referred to prevention of future conflict by establishing a credible Armed Forces that deters the adversary. As the Army and DoD build up the Armed Forces, acquisition leaders need to perform their share to complement the cyber forces. These weapon systems and network capabilities support the LandCyber strategy, which enables real-time data access to friendly and enemy forces, providing the commander and warfighter with the competitive advantage over adversaries. Acquisition leaders utilize the advanced technology to improve the capabilities while mitigating vulnerabilities through risk management to support the LandCyber operations. LandCyber operations and advanced technology can be a dream team or a double-edged sword depending on how well the Army manages the cybersecurity risks (Rafferty, 2013).

Cybersecurity and Impacts on Weapon Systems

Another key item that acquisition leaders need to understand is the role that cybersecurity testing plays in preventing cyber vulnerabilities before fielding of weapon systems. Hutchison (2013) discussed the importance of building cyber testing in the requirement to mitigate cyber vulnerabilities and risks to weapon systems. “Given our military dependence on network-enabled capabilities, the lack of a cybersecurity key performance parameter is a major shortcoming with downstream effects in system development and Developmental Test and Evaluation (DT&E), and ultimately places our warfighters at a disadvantage” (Hutchison, p. 35). The office of the Deputy Assistant Secretary of Defense for DT&E and Director, Test Resource Management Center published *Guidelines for Cybersecurity DT&E*. The guidelines help systems in developing and operating vigorous cybersecurity DT&E to increase resilience of military capabilities (Hutchison).

As mentioned by the Combined Arms Center–Capability Development Integration Directorate (2010), cyber vulnerabilities in weapon systems present significant threats to the warfighter. Leaders must not only understand the domain to which they provide acquisition support, but understand the common cyber vulnerabilities and known threats from lessons learned to protect future weapon systems from the same risks. Leaders must manage the risks throughout the life cycle of the systems to include research, development, testing, fielding, and sustainment.

DoD critical operations depend on the Department of Homeland Security (DHS), other Government agencies, and the commercial sector to improve cybersecurity. DoD and DHS signed a memo in 2010 to align and enhance cybersecurity collaboration. DoD works closely with the Defense Industrial Base (DIB) sector. “To increase protection of DIB networks, DoD

launched the DIB Cybersecurity and Information Assurance Program" (Joint Staff, 2013, p. I-8). "Sharing of information between the DoD and the Defense Industrial Base was an important step in addressing widespread cyber-threats. This collaboration could expand to include sharing of DIB cyber personnel with the skills and clearances needed by DoD in a crisis" (U. S. Department of Defense, 2013, p. 15).

Cyber vulnerabilities affect networks and systems rapidly. Leaders and the workforce both need to be well trained to prevent cyber vulnerabilities by using proper cybersecurity practices. "However, the strongest encryption and most secure protocols cannot protect our networks from poorly trained/motivated users who do not employ proper security practices. Commanders should ensure personnel understand and are accountable for their roles in cybersecurity" (Joint Staff, 2013, p. II-12). Even though DoD has increased investments in the cyberspace domain in the recent years, the United States has been making significant investments and efforts in cybersecurity over the past decade. The heavy investment has been in preventive measures rather than reactive efforts to make corrections to cyber vulnerabilities.

Panton, Colombi, Grimaila, and Mills (2014) focused on prevention and minimizing vulnerabilities at the forefront rather than on discovering vulnerabilities after fielding. They suggested using a vulnerability market (VM) to incentivize public and private researchers to exploit and disclose vulnerabilities. The idea has two purposes. One purpose is to discover and eliminate as much vulnerability as possible. The second purpose of the VM concept is to collect enough data to create a meaningful metric that will lead to a measurement technique and method to ensure DoD systems have built-in security (Panton et al., 2014).

The policy, standards, and instructions provide a guide path for acquisition communities to issue safer weapon systems and networks for our warfighters. The acquisition workforce and

specifically the acquisition leaders must understand the policy, standards, and instructions to ensure that the workforce and OEM implement cybersecurity protection accordingly for safer systems with minimum cyber risk to the warfighter. The U.S. Army Chief Information Office (n.d.) has issued a handbook stating that all "commanders, leaders, and managers, are responsible for ensuring that Information Assurance/Cyber Security is part of all Army operations, missions and functions" (p. 2). Leaders have greater responsibility than the workforce in the protection of our national interests. "As a leader, it is your responsibility to ensure that your business and information systems are protected" (U.S. Army Chief Information Office, p. 3).

> If mission analyses indicate that currently assigned DoD cyber personnel are insufficient for crisis or surge requirements, the Department could leverage existing DoD civilian staff. The Department can identify requirements for developing a DoD Civilian cyber-surge capability to identify qualified staff available from the broader DoD civilian workforce to address cyber-crises. (U. S. Department of Defense, 2013, p. 15)

Acquisition Leaders Need to Understand Cybersecurity

A working group from DoD and GSA published a report to address Executive Order 13636 by making recommendations on incorporating security standards into acquisition and contracts:

> When the government purchases products or services with inadequate in-built cybersecurity, the risks persist throughout the lifespan of the item purchased. The lasting effect of inadequate cybersecurity in acquired items is part of what makes acquisition reform so important to achieving cybersecurity and resiliency. Purchasing products and services that have appropriate cybersecurity designed and built in may have a higher up-front cost in some cases, but doing so reduces total cost of ownership by providing risk

> mitigation and reducing the need to fix vulnerabilities in fielded solutions. (DoD & GSA, 2014, p. 12)

DoD and GSA found that cybersecurity is just one of several conflicting and competing priorities that the acquisition workforce faced during system acquisition. The report noted that cyber risk management and acquisition processes must be connected. Including cybersecurity as a requirement may be more costly up-front, but this initial investment reduces total ownership cost and results in more secure systems. Corporate and government leaders have been worrying about the resilience to cyber risks. "DoD and GSA view the ultimate goal of the recommendations as strengthening the cyber resilience of the Federal government by improving management of the people, processes, and technology affected by the Federal Acquisition System" (DoD & GSA, 2014, p. 6).

The DoD-GSA report provided the following recommendations to address cybersecurity:

1) *Institute Baseline Cybersecurity Requirements as a Condition of Contract Award for Appropriate Acquisitions.* Government should only work with companies that meet the cybersecurity baseline requirements in their operation as well as products and services to government.
2) *Address Cybersecurity in Relevant Training.* Need to train the relevant workforces by first institute acquisition cybersecurity into training curricula.
3) *Develop Common Cybersecurity Definitions for Federal Acquisitions.* Clearly define key cybersecurity terms in government acquisitions increases efficiency and effectiveness.

4) *Institute a Federal Acquisition Cyber Risk Management Strategy.* Identify a list of cyber risk criteria to support acquisitions with correspondent to the types of acquisition.
5) *Include a Requirement to Purchase from Original Equipment Manufacturers, Their Authorized Resellers, or Other "Trusted" Sources, Whenever Available, in Appropriate Acquisitions.* Acquisition requirement to acquire for OEM or trusted sources.
6) *Increase Government Accountability for Cyber Risk Management.* Institute security standards in acquisition planning and "ensure key decision makers are accountable for managing risks of cybersecurity shortfalls in a fielded solution" (DoD & GSA, 2014, p. 8).

Acquiring commercial products saves costs by increasing access to fast-changing technology. Vulnerabilities, however, can come from every entry point in the supply chain. "To achieve cyber resiliency; the Federal government must ensure it is capable of mitigating the risks of emerging threats" (DoD & GSA, 2014, p. 11). "Increasing the knowledge of the people responsible for doing the work will facilitate appropriate cyber risk management and help avoid over-specifying cybersecurity requirements (which leads to higher costs) or under-specifying cybersecurity requirements (which leads to greater risks)" (DoD & GSA, 2014, p. 11).

According to Waddell, Smith, Shufelt, and Caton (2011), cyberspace operations are what senior leaders need to know about cyberspace, with an emphasis on the creation of a workshop to examine how academia supports senior leaders for emerging cyberspace challenges. Their article acknowledged the need for educational training as a forum where cyberspace concerns can be discussed by senior leaders. While their article focused on senior leaders' cyber development,

this cyberspace training and curriculum can be extended to educate leaders at all levels. All levels of leadership have roles and responsibilities in the security of weapon systems and networks in support of cyberspace operations, particularly for the Army in LandCyber operations. “The threat is real and growing; cyberspace is a battlespace; the United States is vulnerable and the vulnerability is increasing; U.S. participants in the cyberspace security effort must establish ‘unity of effort’ and work together” (Waddell et al., p. 8).

Many DoD senior leaders recognize the need to develop Army capabilities to include training and educating leaders and soldiers.

> Fully operationalizing cyberspace throughout the Army requires developing leaders and soldiers who are able to operate in land and cyberspace. Education, training and leader development are critical. We're engaging Army leaders and elements to institutionally increase understanding of cyberspace and challenging the notion that cyberspace operations merely involve information technology and are only about defending networks. (Hernandez, 2012, p. 208)

The Army and DoD have heavily invested in developing Army capabilities for soldiers. The Army cyber/electromagnetic study indicates that Army leaders lack an understanding of cyber (Combined Arms Center–Capability Development Integration Directorate, 2010). Leaders must understand the holistic picture of cyber operations to prevent cyber vulnerabilities and threats to weapon systems and networks. Rafferty (2013) pointed out that “understanding the Army’s cyberspace potential in operational terms is essential to grasping the LandCyber strategy” (p. 6).

> Cyberspace operations training and leader development support the cognitive component that links capabilities to the operations process and results in the delivery of cyberspace

> operations services and effects. Achieving the Army's vision for cyberspace operations requires the Army to participate actively in defining and developing needed cyberspace capabilities. (U.S. Army Cyber Command, 2013, p. 22)

DoD, Army Cyber Command, academia, and industry have been collaborating in educating and developing the cyber workforce to protect our national interests better. According to Brickey and Tallo (2014), LTG Edward Cardon, commander of U.S. Army Cyber Command, delivered the opening remarks at the Cyber Workforce Development, Education and Training Workshop, hosted by National Defense University (NDU), to promote the cyber workforce and leadership. The workshop provided the venue for NDU's Information Resources Management College, the Army Cyber Institute, the private sector, DoD, and academia to discuss cyber leader development, training, and education (Brickey & Tallo). Consistently, Army Cyber Command Strategy also focuses on educating and developing the workforce to meet the cyber mission demand better:

> Army Cyber Command and Second Army are partnered with select government, industry, academia, and partners and Allies to create a collaborative network to best meet mission requirements. The Army has policies that helps recruit, develop, manage, and retain the talent for its professional, innovative, imaginative, and collaborative workforce. (U.S. Army Cyber Command, 2014, p. 3)

Summary

This paper studies the acquisition leader's readiness to support future LandCyber operations. We conducted an examination of what cyberspace is and why it is a problem that acquisition leaders need to be prepared to deal with. It is expected that Internet usage will continue to increase in the next decade. DoD needs to continue to invest in cybersecurity and

ensure that OEMs comply with security standards and keep pace with advances in technology to prevent cyber vulnerabilities. This study reviews how cyberspace operations emerged into the cyberspace domain. U.S. Army Cyber Command (2013) indicated that the Army must adjust to the convergence of land and cyberspace domains because failure to adapt will surrender the advantage in cyberspace to future adversaries.

This literature review identified what cyberspace operations are and how the Army combines cyberspace operations and land operations into LandCyber operations. Leaders must manage the risks throughout the life cycle of the information networks and weapon systems, including research, development, testing, fielding, and sustainment. The acquisition workforce and specifically the acquisition leaders must understand the policy, standards, and instructions to ensure the workforce and OEM implement cybersecurity protection accordingly for safer systems with minimum cyber risk to the warfighter. Including cybersecurity as a requirement may be more costly at first, but this initial investment reduces total ownership cost and results in more secure systems. Leaders must understand the holistic picture of the cyber operations to prevent cyber vulnerabilities and threats to weapon systems and networks. Much of the literature consistently identifies cyber training and education as a necessity for acquisition leaders and the workforce to support future LandCyber operations.

Chapter 3 – Research Methodology

Research Hypothesis

Current cybersecurity awareness and training of acquisition leaders is insufficient to support LandCyber operations.

Research Process

The research used both quantitative and qualitative design. This research method included a literature search on acquisition leader cybersecurity awareness and training that have impact on the cyber risk of weapon systems. The literature reviewed included peer-reviewed articles and publications, DoD and Army doctrines, policies, studies, instructions, reports, and publications. An online survey conducted via SurveyMonkey was developed and implemented to collect cybersecurity KSAs from Army civilian acquisition leaders to determine their readiness to support LandCyber operations. The survey also collected some qualitative data on training needs from the respondents. The survey allowed respondents to self-assess to determine individual knowledge, awareness level, and training gaps. The survey sample was limited to APG civilian leaders at the grade level of General Schedule (GS) 14 and 15 or their equivalents in broad band pay schedules. A total population of approximately 1,800 senior Government civilians was targeted for the survey. The total number of respondents was 236, which is 13% of the surveyed population. Within this population 156, or 66%, identified themselves as part of the acquisition field.

Data Collection

The online survey includes 19 questions. The questions are both quantitative and qualitative. Here is the rationale for each question:

- Question 1 was the survey consent agreement.

- Question 2 distinguished whether the respondent was in acquisition field.
- Questions 3 & 4 identified the respondent's role and organization.
- Question 5 determined the respondent's level of involvement in the cyber related field.
- Questions 6, 7, 8, and 9 assessed the level of understanding on cybersecurity, level of training, and certification possessed by the respondent.
- Question 10 identified the respondent's assessment of cyberspace operations impact on land warfare.
- Question 11 assessed the understanding of how to improve future LandCyber operations.
- Question 12 surveyed the understanding of current and future cyber risks and threats to LandCyber operations.
- Question 13 identified the respondent's assessment of future trends of cybersecurity demand.
- Question 14 assessed the understanding of cyberspace and cybersecurity policies and doctrines.
- Question 15 assessed the level of agreement of the cybersecurity training necessity.
- Questions 16 & 17 were used to determine whether the respondent's organization has cybersecurity training plans in place and the level of their effectiveness.
- Question 18 & 19 allowed free-text comments and suggestions on both the survey and cyber training.

As stated previously in chapter 1, there was potential individual bias based on the individual interpretations of cyber definitions. Another limitation was the number of

respondents, only 13% of the surveyed population, which may reduce the accuracy of the sample. Data gathered through the survey were exported to Microsoft Excel to perform statistical analysis and display charts that are portrayed in chapter 4.

The analysis determined the readiness level based on the gathered data and compared this against the pre-established definitions of the cybersecurity readiness levels. Both the statistical and analytical analysis provided conclusive evidence to prove the hypothesis. The resulting conclusion and recommendations are presented in chapter 5.

Chapter 4 – Findings

Population & Sample Size

The survey responses were anonymous and limited to the survey population of APG, MD composed of GS-14/15 Army civilian acquisition leaders. The survey data reported in this research include responses of 156 acquisition civilians in APG, MD in the grades GS-14 or GS-15 or pay band equivalent. There were a total of 236 respondents to the survey. Eighty respondents indicated that they were non-acquisition Army civilians. Because this research is intended to capture information about the Army acquisition community, respondents outside of the Army acquisition community were omitted from the analysis.

Collected Survey Data

The survey data reported in this research include responses to 19 questions. Survey questions included demographic questions and technical qualitative and quantitative questions. Question 3 identifies their leader roles. Questions 4 through 18 data are discussed in detail in this chapter. The complete survey instrument developed through SurveyMonkey is included as Appendix B. The focus of this survey is on civilian acquisition leaders.

The total number of respondents (Figure 2) was 236, of which 156 identified themselves as acquisition civilians. One hundred forty acquisition civilians responded up to question 7. Questions 8 and 9 were used to test the cybersecurity process knowledge of the respondents. One hundred thirteen acquisition civilians responded up to question 12. The next couple questions assess respondents understanding on cybersecurity demand and cyber policies and doctrines. The possible rationale for respondents to stop at questions 7 and 12 was the lack of understanding. Only 106 acquisition civilians actually completed the entire survey.

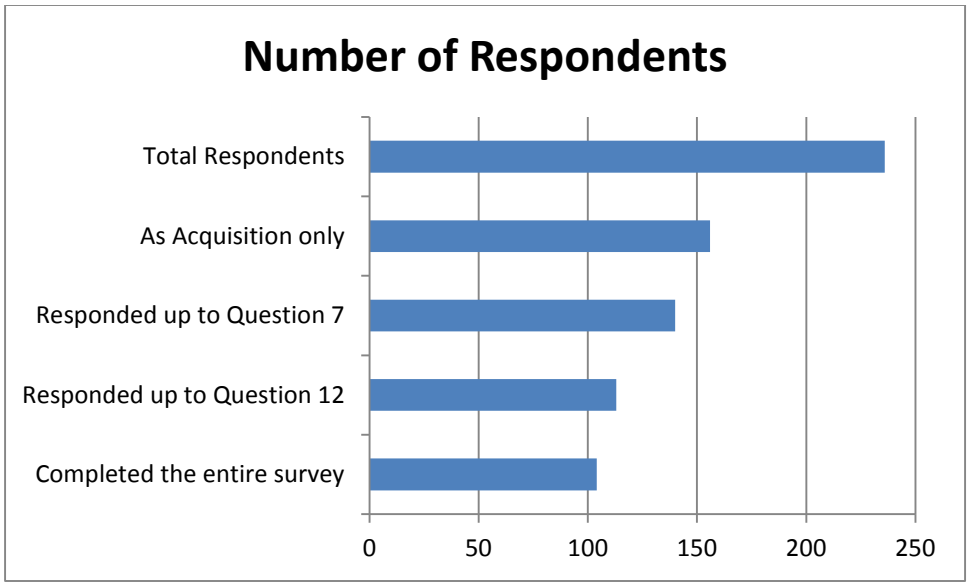


Figure 2 – Number of Respondents

Figure 3 shows the survey results that identify the major organizations respondents represented. The figure indicates that most major organizations in the acquisition community across APG, MD were represented in this survey. The organization with the most respondents was Research, Development, and Engineering Command. The least represented organization was Program Executive Office Intelligence Electronic Warfare & Sensors. of the distribution of respondents show in Figure 3 resembles the proportional sizes of the organizations at APG.

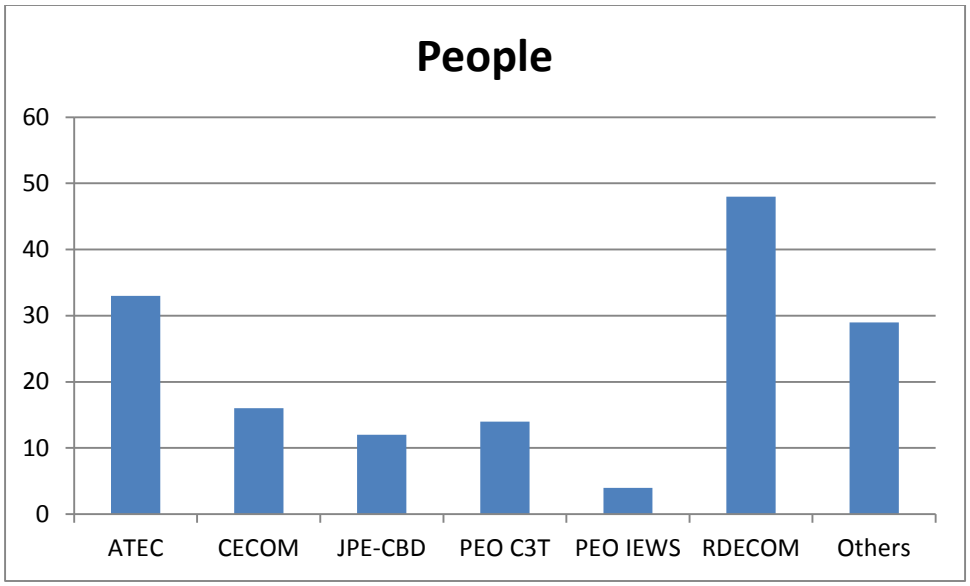


Figure 3 – Question 4: Major Organization Respondents

Nineteen percent of the respondents indicated that their job either involved or highly involved association with cyberspace or a related field. Fifty-five percent of the respondents indicated that they are minimally involved or not involved with cyberspace. Sixteen percent provided a neutral response. Figure 4 shows that more than half of the respondents' work is minimally involved or not involved with cyberspace or related fields.

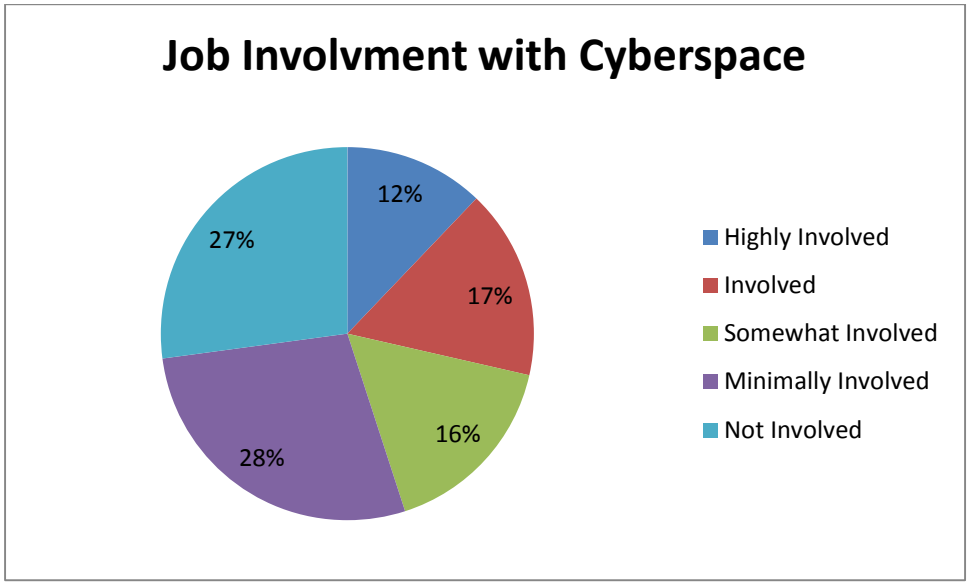


Figure 4 – Question 5: Job Involvement with Cyberspace

Only one respondent has two cybersecurity certifications. Only 12% of the respondents, or 17 people, indicated having one cybersecurity certification. The majority of the respondents do not have any cybersecurity certification, which accounts for 87%, as indicated in Figure 5.

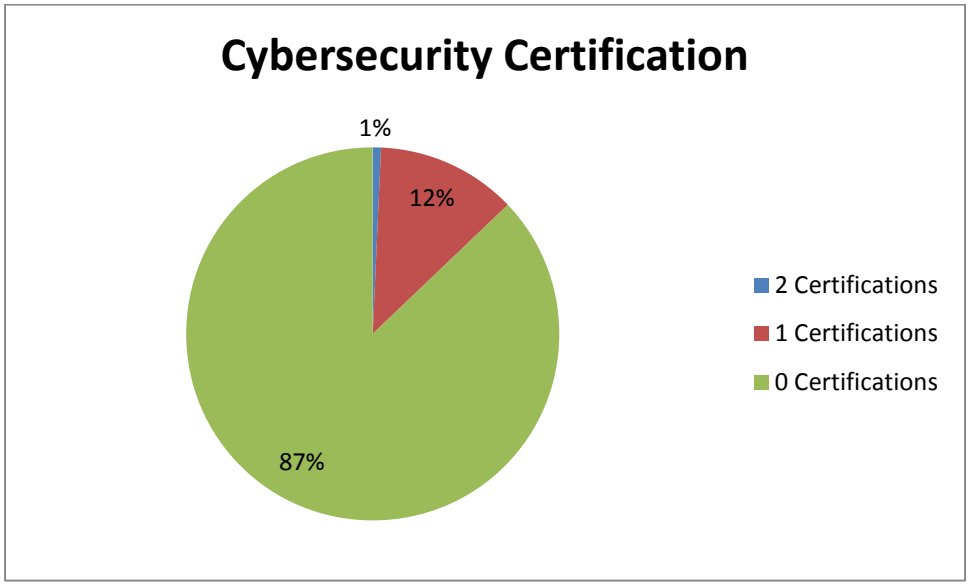


Figure 5 – Question 6: Cybersecurity Certification

Question 7 surveyed the population based on their level of cyberspace operations and/or cybersecurity training to support their jobs. Forty-seven percent indicated having the appropriate amount of training to accomplish their jobs. Forty-seven percent indicated that they had either minimum or insufficient training to accomplish their job, as portrayed in the Figure 6.

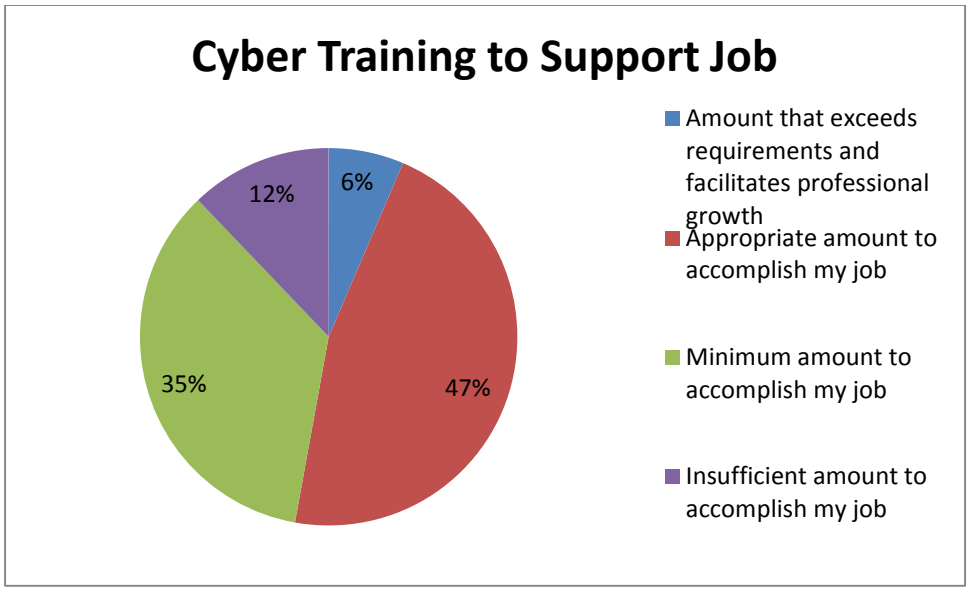


Figure 6 – Question 7: Cyber Training to Support Job.

Question 8 assessed the respondents' knowledge of cybersecurity processes, RMF, DIACAP, and DITSCAP. Thirty-one percent of the responses were correct. Sixty-one percent of the respondents did not answer any knowledge questions correctly (Figure 7).

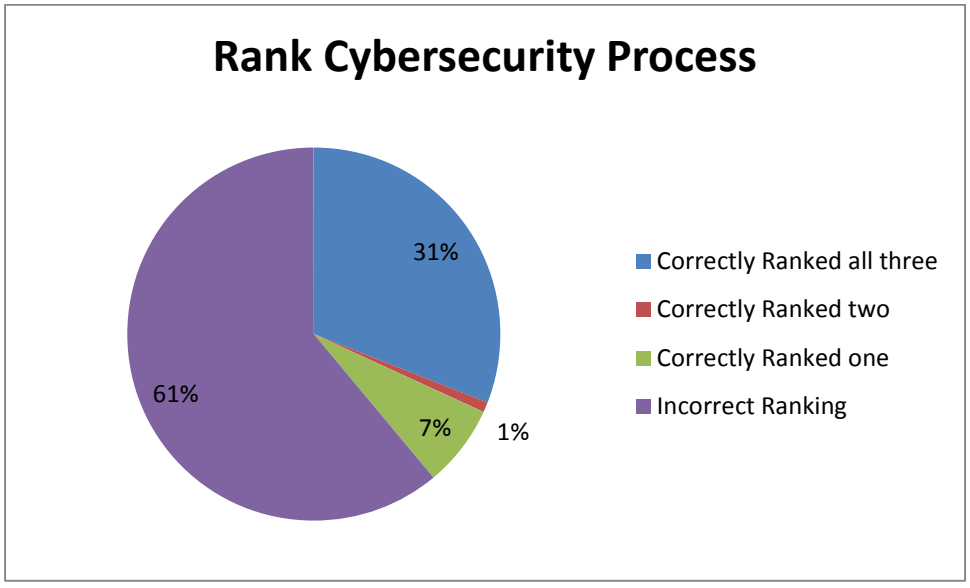


Figure 7 – Question 8: Cybersecurity Process Knowledge

Question 9 was used to determine the respondents' knowledge of cybersecurity processes, RMF, DIACAP, and DITSCAP. Twenty-two percent matched all three processes correctly. Thirty-one percent matched one or more correctly. Sixty-nine percent did not match any cybersecurity knowledge content correctly. Figure 8 indicates that the majority of acquisition leaders do not understand the cybersecurity processes and their approaches. Question 6, 7, 8, and 9 were used to determine the acquisition leaders' level of understanding of cybersecurity, level of training, and certification possessed.

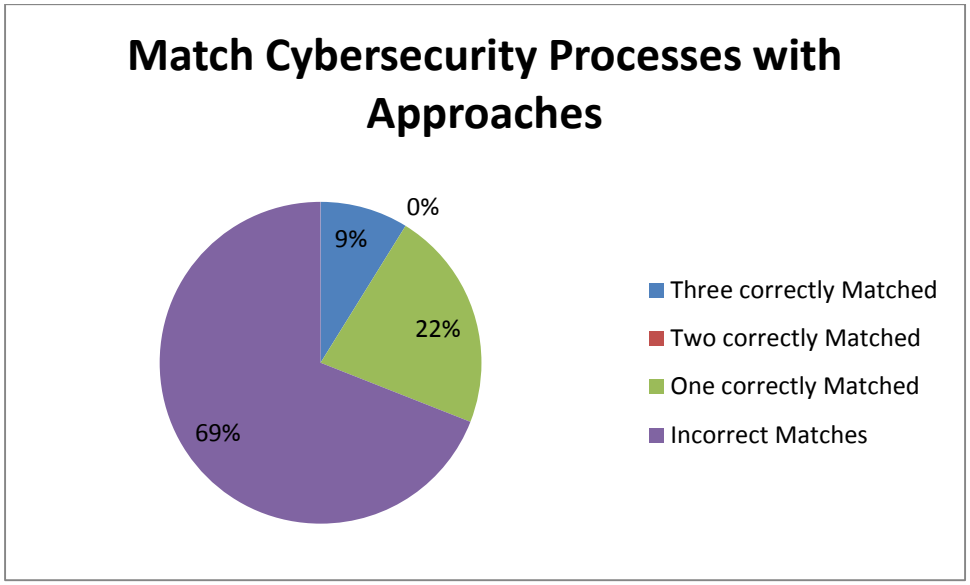


Figure 8 – Question 9: Match Cybersecurity Processes with Approaches

Figure 9 identifies acquisition leaders' assessment of the extent that cyberspace operations affect land warfare. Twenty-five respondents indicated the extent is an 85–100% impact. Thirty respondents specified that the impact is 60–85%. Twenty-eight respondents stated that there was a 40–60% impact. The majority of the respondents indicated cyberspace operations affects land warfare.

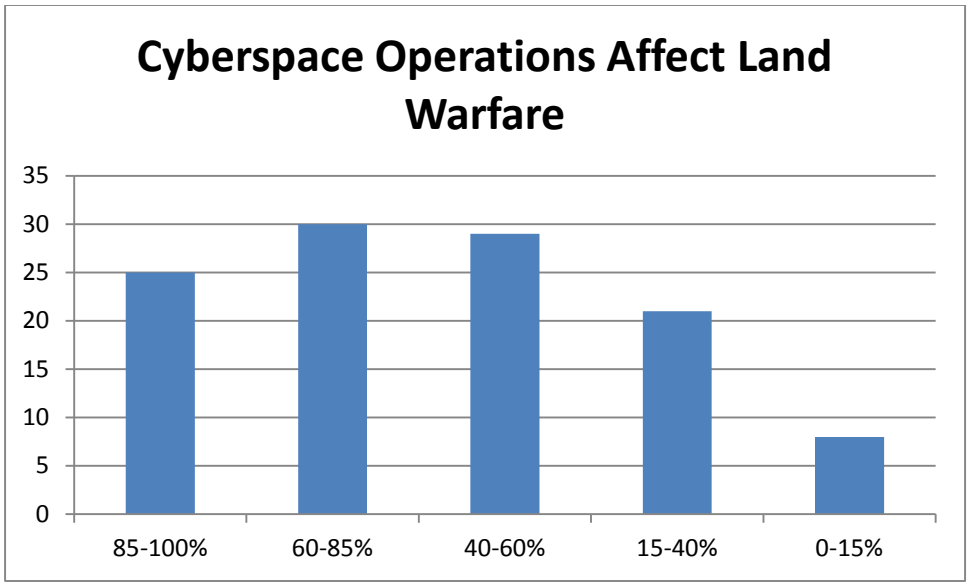


Figure 9 – Question 10: Percentage of Cyberspace Operations that Affect Land Warfare?

Figure 10 depicts whether the respondent in their current situation, as an acquisition leader, believes he or she can improve future LandCyber operations. Half of the respondents said yes, while the other half said no.

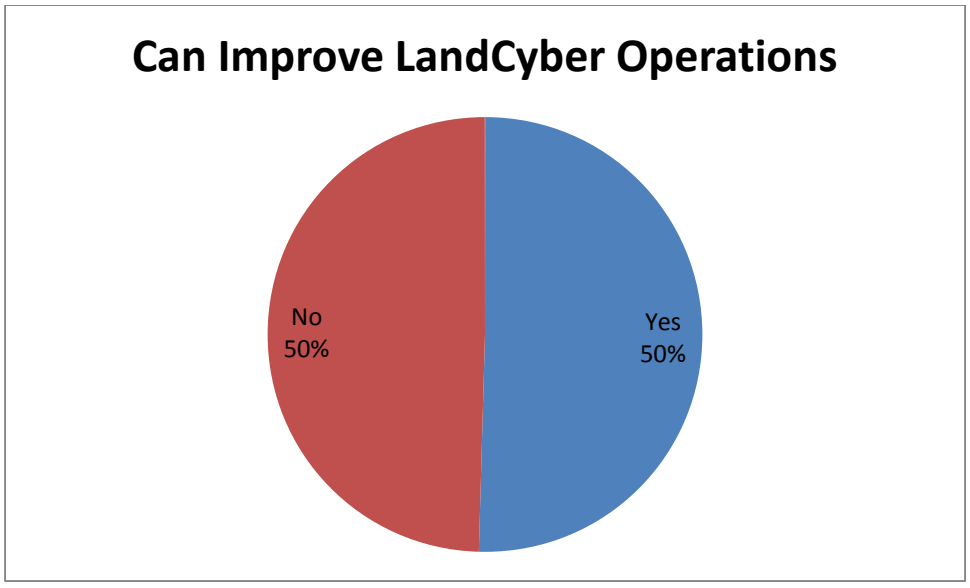


Figure 10 – Question 11: Can You Improve LandCyber operations?

Figure 11 combines the assessment of both the current and future theater-level cyber risks and threats to LandCyber Operations. The chart indicates that acquisition leaders do not know or understand the current and future theater-level cyber risks and threats to LandCyber Operations, with 45% and 50% in the 0–15% range. In between the 0–40% range, data show 72% and 68% respectively.

Figure 12 depicts the assessment of future cybersecurity demands on the acquisition workforce and leaders. The respondents' sense is that there will be a significant increase in demand for both acquisition workforce and leaders.

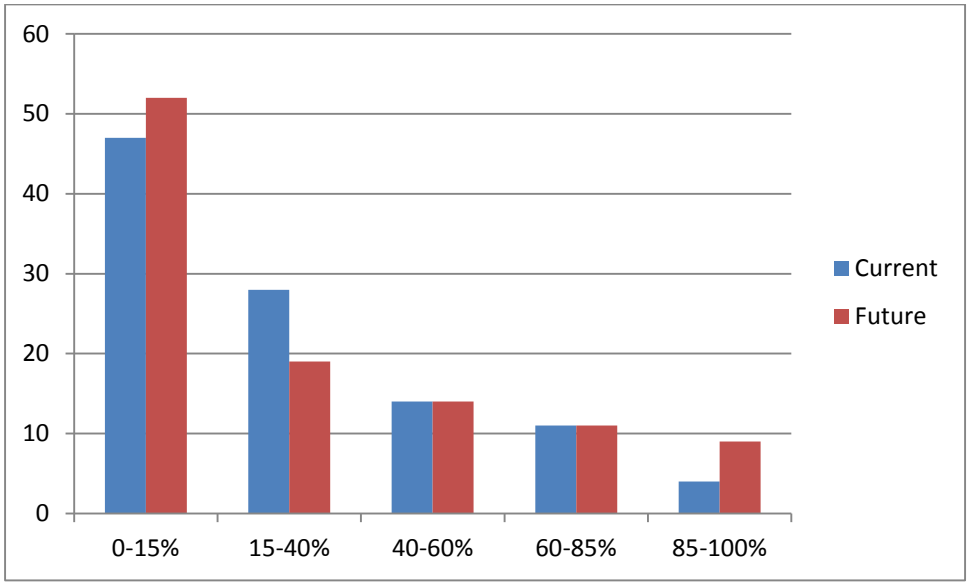


Figure 11 – Question 12: Assessment of Theater-level Cyber Risks and Threats to LandCyber Operations

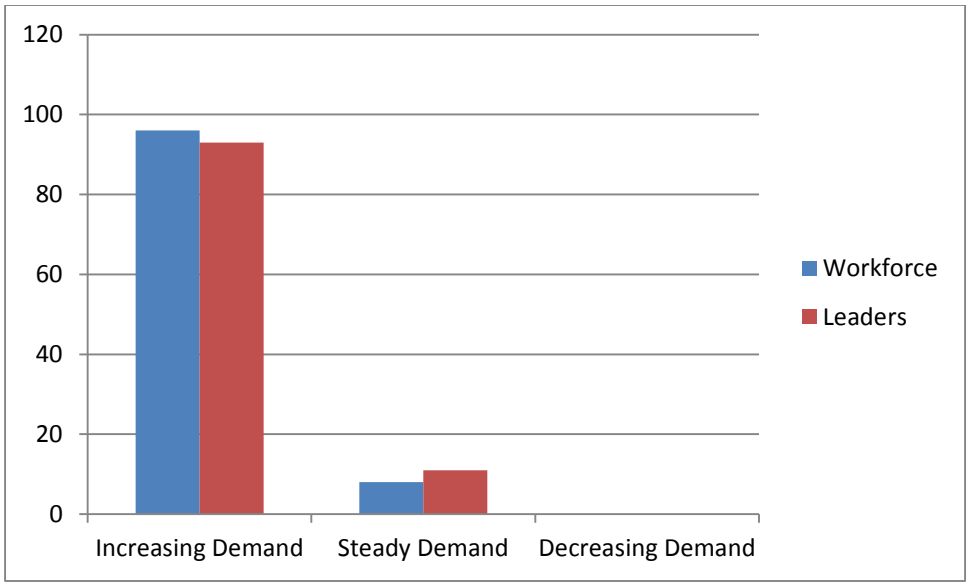


Figure 12 – Question 13: Assessment of Future Cybersecurity Demand

Figure 13 and Figure 14 represent respondents' understanding of cyberspace operations and cybersecurity policies and doctrine. Figure 13 shows the number of people who answered this survey question who understand particular policies or doctrines. Department of Defense Instruction (DoDI) 8510.01 and DoDI 8500.01 are the most understood documents. Figure 14 shows the number of acquisition leaders who responded to this survey question who understand the combination of policies and doctrines. Seventy-one percent of acquisition leaders understand no more than one cyberspace operations or cybersecurity policy or doctrine.

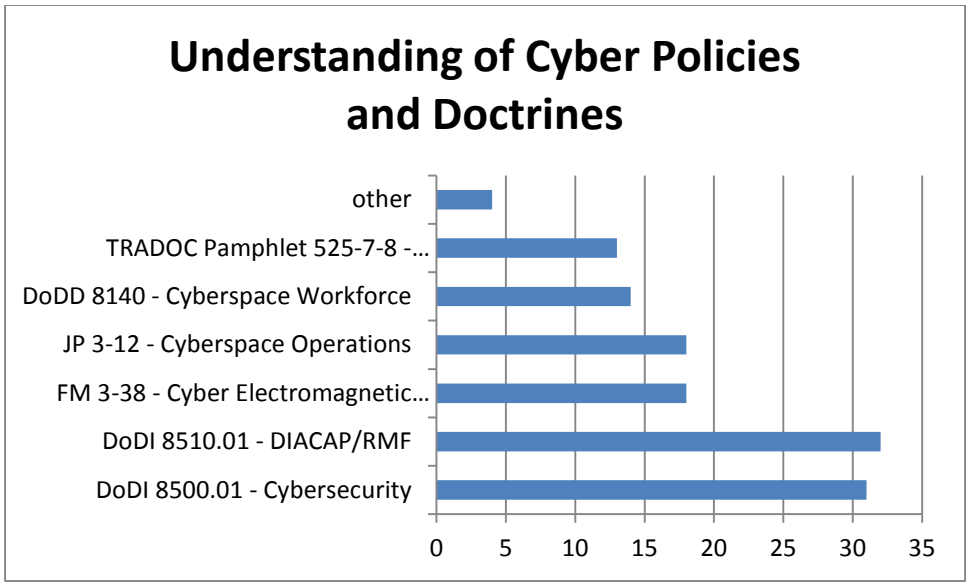


Figure 13 – Question 14: Understanding of Cyber Policies and Doctrines

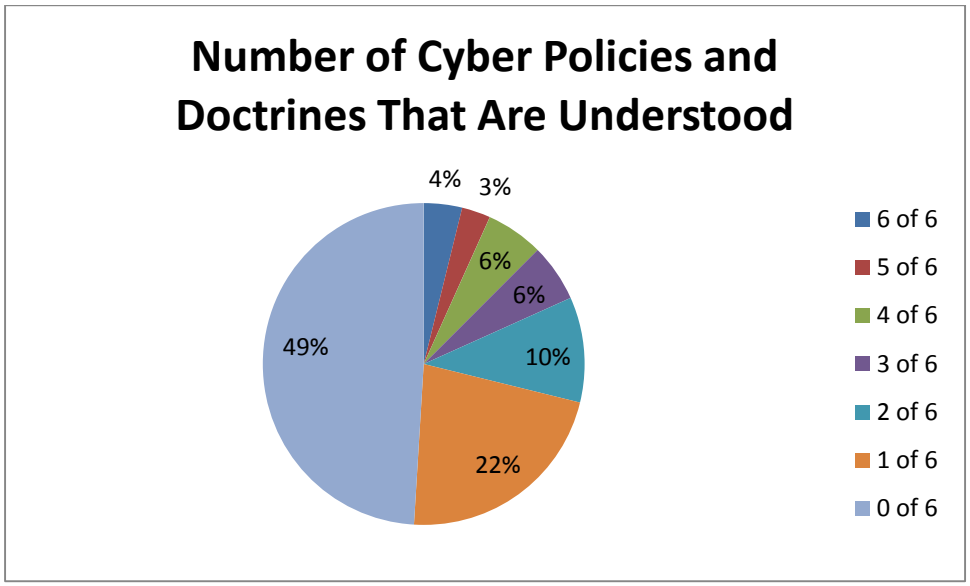


Figure 14 – Question 14: Number of Cyber Policies and Doctrines That Are Understood

Question 15 is an assessment of acquisition leaders' necessity for cyber training to support their job. Over 66% of the respondents either agree or strongly agree that they need cyber training to support their jobs (Figure 15).

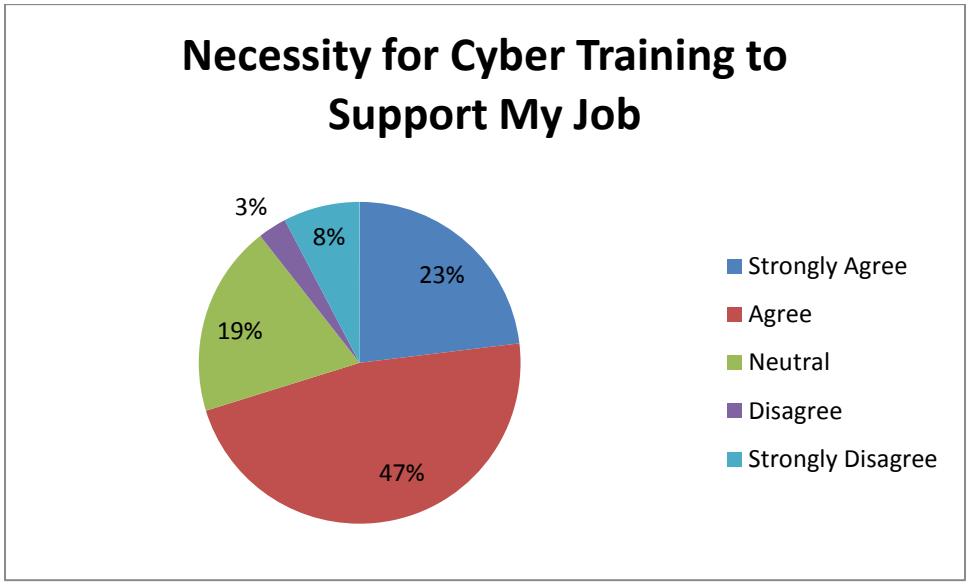


Figure 15 – Question 15: Necessity for Cyber Training to Support My Job

Figure 16 shows that 52% of represented organizations have established cybersecurity training plans. This result may represent individual interpretation of the definition of "cybersecurity training," due to imprecise language on question 16. Respondents may have interpreted cybersecurity training to mean annual basic cybersecurity awareness training. The intent of question 16 was to provide a more in-depth assessment of cybersecurity training, such as certification and how cybersecurity affects the warfighters that we support.

Figure 16 – Question 16: Organization Has Cybersecurity Training Plan

For those organizations that have cybersecurity training plans, question 17 asked respondents to rate the effectiveness of the plans. Figure 17 shows that the majority responded with "somewhat effective" (45%) followed by "effective" (36%). Again, the result may be due to individual differences in interpretation of "cybersecurity training," as in question 16.

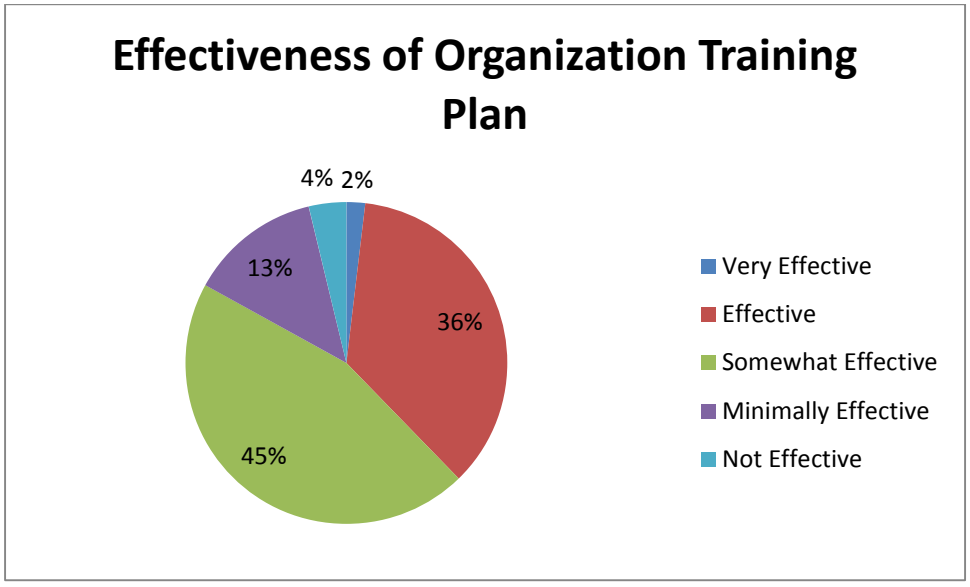


Figure 17 – Question 17: Effectiveness of Organization Training Plan

Question 18 is an open-ended request for recommendations from respondents on cyber training to assist acquisition leaders in support of future land warfare. All responses were manually classified into six broad categories (Table 1). There were total of 28 responses. The first category is the recommendation to establish initiatives in university and institutional training, recruitment, and cybersecurity certification. The second category is the recommendation for a robust, specific, and conceptual cybersecurity training that applies to the line of work. The third category is the recommendation to implement Defense Acquisition University (DAU) and other classroom training on cyberspace and cybersecurity. The fourth category is the recommendation to train on the process of policy and doctrine development and include incorporation of cyber reviews into the systems engineering process to mitigate potential threats and risks. The fifth category is the recommendation to develop on-the-job training with real-world experience, as well as a lessons-learned briefing and database. The last category is grouped with the recommendation to create the categorized cyber field (Cyber Task Force equivalent) training similar to the Space Cadre for space professionals.

Table 1 – Question 18: Recommendations for Cyber Training

Cyber Training for Acquisition Leaders	
University and institutional training, recruitment, and cybersecurity certification	29%
Complete, robust, specific, and conceptual training that applies to the job	25%
DAU and other classroom trainings	21%
Policy and doctrine development and incorporation of cyber reviews into systems engineering process to mitigate potential threats and risks	11%
On-the-job real-world experience and lessons learned	7%
Categorize cyber field (Cyber Task Force) and training, such as Space Cadre for Space professionals	7%
Total	100%

Summary

Findings from the literature review and survey data all indicated that Army leaders lack the necessary training and education on cybersecurity to support current and future LandCyber operations. Such operations require network and weapon systems to have few or no cyber vulnerabilities that create risks and threats that can cause the loss of decisive advantage over the adversaries. In order to minimize cyber vulnerabilities on network and weapon systems, leaders who are involved with developing, fielding, and sustaining systems must first understand cybersecurity threats and risks and their causes.

The findings from the literature review and data collected from the survey questions are used to statistically and analytically analyze conclusions and provide recommendations in chapter 5. The collected survey data have been analyzed to categorize the readiness of the acquisition leaders based on the predefined level of readiness in chapter 1.

Chapter 5 – Conclusions and Recommendations

The objective of this research was to analyze the acquisition leaders' readiness to support future LandCyber operations. The proliferation of cyberspace increases opportunities as well as vulnerabilities. Based on the literature review and survey findings, the research determined that current acquisition leaders have various levels of readiness to support future LandCyber operations. The literature review did not provide enough information to identify the readiness level of acquisition leaders. It did indicate the need to educate and train leaders to prepare them better in support of LandCyber operations: "As with any change to practice or policy, there is a concurrent need to train the relevant workforces to adapt to the changes. Incorporate acquisition cybersecurity into required training curricula for appropriate workforces" (DoD & GSA, 2014, p. 7).

The findings from survey data painted a picture that leaders and the workforce need to understand cybersecurity through training and education. Table 2 depicts the five readiness levels and criteria defined in chapter 1, as well as the associated responses from the survey questions. Each readiness level criteria is cross-checked to see whether the acquisition leader actually demonstrated proficiency based upon his or her responses from the survey questions. The Response Data cells show the percentage of the responses that either met or did not meet the level criterion. If more than 50% of the collected responses met the level criterion, then Y was assigned. Otherwise, the N was assigned. Level one is the lowest readiness level, representing no training nor understanding of cybersecurity. The dark green color represents meeting the level. Light green represents meeting the requirements based on the raw data response. Yellow indicates meeting half or one of the two requirements. Red represents not meeting the requirement.

Table 2 – Readiness Level

Readiness	Criteria	Response Data
Level 1	No training nor understanding of cybersecurity	Y=100% N=0%
Level 2	Cyberspace operations & cybersecurity training (Figure 6 – Question 7)	Y = 53% N = 47%
Level 3	Cyberspace operations affect LandCyber (Figure 9 – Question 10)	Y = 67% N = 33%
	Theater-level risks and threats (Figure 11 – Question 12)	Y = 32% N = 68%
Level 4	DITSCAP, DIACAP, RMF (Figure 7 & 8 – Question 8 & 9)	Y = 9% N = 91%
Level 5	Cybersecurity certification (Figure 5 – Question 6)	Y = 13% N = 87%

Figure 6 shows 53% of the respondents have appropriate or an above average level of cyber training to support their job. However, Figure 4 shows that the level of cyberspace involvement in their jobs is low at 29%. Therefore, the data shown in Figure 6 for cyber training does not substantiate the belief that acquisition leaders are well trained in cyber security since involvement is low, with minimal cyber training. This may be an anomaly caused by imprecise terminology in question 7. Additionally, evidence from data collected in questions 8, 9, and 14 indicate that acquisition leaders do not understand cybersecurity, cyber policies, and doctrine. Questions 8 & 9 test respondents' knowledge on cybersecurity processes of DITSCAP, DIACAP, and RMF; and question 14 examines respondents' understanding of cyberspace operations and cybersecurity policies and doctrine. The established conditions for meeting a level requirement is 50% or greater. Since 53% of respondents are having cyber training, this meets level two readiness criteria.

There are two criteria for achieving readiness level three. The response data for questions 10 and 12, depicted in Figures 9 and 11, are used to address level three. Question 10 assesses

acquisition leaders' knowledge on cyberspace operations that affect land warfare. Figure 9 shows that 67% of acquisition leaders believed that over 50% of cyberspace operations affect land warfare. Question 12 assesses acquisition leaders' knowledge and understanding of current and future cyber risks and threat to LandCyber operations. Figure 11 shows acquisition leaders lack a good understanding of current and future theater-level cyber risks and threats to LandCyber operations. Both Figures 9 and 11 depict data that support the acquisition leaders' readiness level three criteria. Because one criterion was met and one was not, Table 2 rated acquisition leaders' readiness level three as half met.

Readiness level four has additional requirements for understanding DITSCAP, DIACAP, and RMF. Questions 8 and 9 assess acquisition leaders' knowledge and understanding of cybersecurity processes. Based on the responses to these two questions, 9% of the respondents correctly answered questions 8 and 9, but 91% answered incorrectly. However, 30% of the respondents did answer at least one question correctly. Table 2 shows that most acquisition leaders do not meet readiness level four.

The additional criterion for achieving readiness level five is to have cybersecurity certification. Question 6 gathered cybersecurity certification data. Figure 5 shows that 87% have no certificates, while only 13% have one or more. This data, reflected in Table 2, shows that acquisition leaders do not achieve readiness level five even if they achieved the previous levels. According to the statistical and analytical analysis and assumptions, the data shown in Table 2 shows the average readiness level of acquisition leaders to be 2.5. That means meeting the criteria for level two, and half of three. Further analysis based on data gathered from question 8, 9, and 14 deduced that acquisition leaders' possess minimal cyberspace operations and cybersecurity training. The claimed training from question 7 may refer to annual cybersecurity

awareness training. This annual refresher training is completed within 60 minutes and is intended for the broad Federal workforce. All Federal employees with network access are required to complete this basic cybersecurity awareness training on an annual basis. This leads to the conclusion that the average readiness level of acquisition leaders is closer to level one.

Whether acquisition leaders' level of readiness is 1 or 2.5, either is still too low for them to be able to support LandCyber operations, especially in the constantly changing future. This result informs a recommendation for United States Army Acquisition to institutionalize training and education for better preparation of Army acquisition leaders on cybersecurity and beyond to support Army LandCyber operations.

Cyberspace has tremendous impacts on our life, both personally at home and professionally at work. Cyberspace threats and risks must be closely managed and mitigated to ensure weapon systems and information are not available to our adversaries. In the battlefield where lives are at stake, cyber vulnerabilities raise the threat and risk level several fold. The acquisition workforce and acquisition leaders must protect our warfighter by protecting the weapon systems that we field to ensure cyber vulnerabilities are kept to a minimum. That will not happen until acquisition leaders understand cyberspace operations, the cyberspace domain, and cybersecurity. Cybersecurity and resilience can be improved by acquisition leaders gaining a clear understanding of what cybersecurity is and by ensuring acquired weapons systems are secure and risks are managed.

The acquisition workforce, and especially acquisition leaders, needs to understand that cybersecurity should be part of the requirement that is built into each system acquisition to minimize the risks. Training and education of the acquisition workforce and acquisition leaders who are held accountable for the procurement of products such as weapon systems will facilitate

the process for ensuring that cybersecurity requirements are built into the acquisition process to reduce costs and risks.

Additionally, for more senior acquisition leaders, education and training remain the top priority. Cyberspace operations, including cybersecurity, need to involve leadership in the curriculum. One way to achieve this is through senior service colleges. Developing cyber capabilities is a national urgency and necessity, and it should involve all DoD military, civilians, and contractors. Cyber education has been institutionalized throughout national universities and colleges. Information can be found at National Initiative for Cybersecurity Careers and Studies (U.S. Department of Homeland Security, n.d.), Cyber Security Education Consortium (Cyber Security Education Consortium, 2014), and Maryland Cybersecurity Center (Maryland Cybersecurity Center–UMD, 2015). Acquisition leaders have the obligation to be part of cyber capabilities and support the recruitment, training, and retention of cyber-capable personnel.

Several training and education categories recommended by the respondents in the open-ended question 18 are listed in Figure 18. These were discussed in chapter 4. The Army and DoD have been working on implementation of these categories of education and training for the "Cyber Task Force." Among the categories that have begun to be addressed are the DAU cyber session embedded in some of the Defense Acquisition Workforce Improvement Act certification courses.

There are two recommendations for further study on this topic. The first recommendation is to redistribute the survey in its entirety with the modification of question 7 and question 10. The modification to question 7 is to clearly state that cyber training excludes annual cybersecurity and Information Assurance awareness training. Question 10 should be modified into a knowledge test question to truly assess respondents' understanding of the impact of

cyberspace operations on land warfare. These two changes will provide more accurate results. Replicating this research would strengthen the reliability and validity of the results.

The second recommendation for an advanced study is to expand the research to cover the entire cyberspace (offensive, defensive, and network operations) readiness level for acquisition leaders. This will increase the scope of the study and result in a more comprehensive understanding of acquisition leaders' readiness of the entire cyberspace that supports LandCyber operations.

References

Brickey, J., & Tallo, D. D. (2014). *Cyber beacon 2014: Cyber workforce development, education and training workshop.* Washington, DC: National Defense University.

Combined Arms Center–Capability Development Integration Directorate. (2010). *Army cyber/electromagnetic contest capabilities based assessment.* Ft. Leavenworth, KS: Author.

Cyber Security Education Consortium. (2014). *Home page*. Retrieved from http://cseconline.net/2014/

Department of Defense & General Services Administration. (2013). *Improving cybersecurity and resilience through acquisition.* Washington, DC: U.S. Department of Defense.

Headquarters, Department of the Army. (2014). *FM 3-38: Cyber electromagnetic activities.* Washington, DC: Author.

Hernandez, R. A. (2012, October). U.S. Army Cyber Command: Cyberspace for America's force of decisive action. *Army*, *62*(10), pp. 205–208.

Hutchison, S. J. (2013). Cybersecurity: Defending the new battlefield. *Defense AT&L*, *42*(6), 34–39.

Internet Live Stats. (2014). *Internet users*. Retrieved from http://www.internetlivestats.com/internet-users

Joint Staff. (2013). *Joint publication 3-12 (R): Cyberspace operations.* Washington, DC: Author.

Lynn, W. J. III. (2010, September/October). *Defending a new domain: The Pentagon's cyberstrategy*. Retrieved from http://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

Maier, M. R. (2014). *Cyberspace and the Army soldier after 2020.* Aberdeen Proving Ground, MD: Defense Acquisition University.

Maryland Cybersecurity Center. (2015). *Cybersecurity education at UMD*. Retrieved from http://www.cyber.umd.edu/education

Panton, B. C., Colombi, J. M., Grimaila, M. R., & Mills, R. F. (2014). Strengthening DoD cyber security with the vulnerability market. *Defense Acquisition Research Journal, 21*(1), 466-484.

Rafferty, J. L. Jr. (2013). *LandCyber operations: A double edged sword or a dream team?* Carlisle, PA: U.S. Army War College.

U.S. Army Chief Information Office. (n.d.). *Leader's information assurance/Cybersecurity handbook*. Washington, DC: Author.

U.S. Army Cyber Command. (2013). *The U.S. Army LandCyber white paper 2018–2030.* Fort Meade, MD: Author.

U.S. Army Cyber Command. (2014). *United States Army Cyber Command and Second Army strategy leading the nation's Army in cyberspace.* Fort Belvoir, VA: Author.

U.S. Army Training and Doctrine Command. (2010). *Cyberspace operations concept capability plan 2016–2028.* Fort Monroe, VA: Author.

U.S. Department of Defense. (2011). *Department of Defense strategy for operating in cyberspace*. Washington, DC: Author.

U. S. Department of Defense. (2013). *Department of Defense cyberspace workforce strategy.* Washington, DC: Author.

U.S. Department of Defense. (2014). *2014 Quadrennial Defense Review*. Washington, DC: Author.

U.S. Department of Homeland Security. (n.d.). *Education—Futhering in cybersecurity & STEM*. Retrieved from http://niccs.us-cert.gov/education/education-home

Waddell, W., Smith, D., Shufelt, J., & Caton, J. (2011). *Cyberspace operations: What senior leaders need to know about cyberspace.* Carlisle, PA: U.S. Army War College.

Glossary of Acronyms and Terms

APG.....Aberdeen Proving Ground

ATEC .....Army Test and Evaluation Command

CECOM .....Communication and Electronic Command

DAU.....Defense Acquisition University

DHS.....Department of Homeland Security

DIB.....Defense Industrial Base

DITSCAP.....Department of Defense Information Technology Security Certification and Accreditation Process

DIACAP.....Department of Defense Information Assurance Certification and Accreditation Process

DoD.....Department of Defense

DoDD.....Department of Defense Directive

DoDI .....Department of Defense Instruction

DT&E.....Developmental Test and Evaluation

FM.....Field Manual

GAO.....General Accounting Office (now known as the Government Accountability Office)

GS .....General Schedule

GSA.....General Services Administration

JPEO-CBD.....Joint Program Executive Office for Chemical and Biological Defense

KSA.....knowledge, skills, and abilities

NDU.....National Defense University

OEM.....Original Equipment Manufacturer

PEO C3T.....Program Executive Office Command Control Communications - Tactical

QDR.....Quadrennial Defense Review

RMF.....Risk Management Framework

USCYBERCOM.....United States Cyber Command

VM… .....vulnerability market

Appendix A – Emerging Army Cyber Doctrine/Policy, Organization and Studies

The Army is preparing for cyberspace by updating and adding many Army policies, standards, and doctrine (Table A1).

Table A1 – Emerging Army Doctine/Policy

Emerging Army Doctrine/Policy
• 2010: U.S. Army Training and Doctrine Command Pamphlet 525-7-8 Cyberspace Operations Concept Capability Plan published
• 2012: Army Doctrine Publication (ADP)/Army Doctrine Reference Publication (ADRP) 3-0 Unified Land Operations updated to include cyberspace technologies in the Army operational environment
• 2012: LandCyber White Paper published
• 2013: Joint Publication (JP) 3-12 Joint Cyberspace Operations approved
• 2013: Army Field Manual (FM) 3-12 Cyberspace Operations draft developed
• 2014: Army FM 3-38, Cyber Electromagnetic Activities (CEMA) approved
• 2014: QDR 2014, cyber is major part

The Army is reorganizing and establishing new cyber organizations to support the cyberspace effort (Table A2).

Table A2 – Evolving Army Organizations

Evolving Army Organizations
• 2010: U.S. Army Cyber Command/2nd Army, Ft. Belvoir, VA
• 2010: U.S. Cyber Command, Ft. Meade, MD
• 2011: 780th Military Intelligence Brigade/First Cyber Brigade, Ft. Meade, MD
• 2012: U.S. Army Training and Doctrine Command Integrated Capabilities Development Team (ICDT) for cyberspace established
• 2013: Cyber Center of Excellence announced, to be located in Ft. Gordon, GA
• 2014: Army Cyber Institute, West Point, NY
• 2014: NETCOM is direct report unit to 2nd Army
• 2014: Stood up Military Occupational Specialty branch for Cyber

Many completed and ongoing studies support these new cyber initiatives (Table A3).

Table A3 – Completed and Ongoing Cyberspace Studies

Completed and Ongoing Cyberspace Studies
• 2013: ARCYBER Cyber Capabilities Based Assessment (CBA) completed and Functional Solutions Analysis (FSA) final report approved
• 2013: Cyber Leader Development, Education, and Training Assessment and Implementation Strategy completed
• 2013: Land Cyber Map Exercise (MAPEX) conducted
• 2014: Cyberspace DOTMLPF-P Integrated Capabilities Recommendation (DICR) ongoing
• 2014: Cyberspace Integrated Capabilities Document (ICD) in development
• 2014: Cyber Material Development Strategy
• 2014: Cyber Material Development Acquisition Strategy, 2014–2018

Note: Some of the above information in Tables A1, A2, and A3 comes from Maier (2014, pp. 6–7).

Table A4 provides a list of the latest cyber news and activities.

Table A4 – Latest Cyber News/Events

Latest Cyber New/Events
• Office of Personnel Management hacked, with information on 4 million Federal employees stolen
• Cyber security legislation: Cyber Threat-Sharing Bill—Finalizing before vote
• President Obama signed executive order for program to allow sanction to overseas hackers.
• White House unclassified computer system hacked by Russian from compromised State Department computers.
• Tewksbury Police Department paid ransom to cyberterrorists who used CryptoLocker ransomware virus.
• List of companies hacked: Anthem Inc, J.P. Morgan Chase, Home Depot, Google, Apple iCloud, eBay, Target

Appendix B – Survey Instrument

Examining Acquisition Leaders' Readiness to Support LandCyber Operation

Thank you for participating in this survey.

***1. INFORMED CONSENT AGREEMENT**

As an adult 18 years of age or older, I agree to participate in this research about Examining Today's Acquisition Leaders' Readiness to Support Future Landcyber Operation. This survey is being conducted to support research efforts being performed by Matthew Lee, a student of the Senior Service College Fellowship Program of the Defense Acquisition University.

I understand that my participation is entirely voluntary; I can withdraw my consent at any time. By agreeing to participate in this study, I indicate that I understand the following:

1. The purpose of the research is to help define the necessary foundation for the acquisition leader's readiness for landcyber operations through the next decade. Should I choose to participate in the survey, I am aware that my feedback will be consolidated with other participants and the outcome will be briefed to Army leadership allowing them to understand todays' acquisition leaders training gap in cyberspace operation and cybersecurity.

2. If I choose to participate in this research, I will be asked to complete an online questionnaire. The questionnaire will include items relating to Acquisition Leaders' Readiness to Support Future Landcyber Operation. The questionnaire will take approximately 10 minutes to complete.

3. There is no incentive for participation.

4. All items in the questionnaire are important for analysis and my data input will be more meaningful if all questions are answered. However, I do not have to answer any that I prefer not to answer. I can discontinue my participation at any time without penalty by exiting out of the survey.

5. This research will not expose me to any discomfort or stress beyond that which might normally occur during a typical day. There are no right or wrong answers; thus, I need not be stressed about finding a correct answer.

6. There are no known risks associated with my participating in this study.

Page 1

Examining Acquisition Leaders' Readiness to Support LandCyber Operation

7. Data collected will be handled in a confidential manner. The data collected will remain anonymous.

8. The purpose of this research has been explained and my participation is entirely voluntary.

9. I understand that the research entails no known risks and by completing this survey, I am agreeing to participate in this research.

END OF INFORMED CONSENT

I have read the Informed Consent Agreement and will participate voluntarily.

- ◯ Yes
- ◯ No

***2. I am currently a member of the acquisition workforce.**

- ◯ Yes
- ◯ No

***3. What is your leadership role?**

	Branch Chief	Division Chief	Director or Deputy Director	Project Manager (PM) or Deputy PM	Product Manager (PdM) or Deputy PdM; Product Director (PdD) or Deputy PdD	Team Lead	Other
Selection	◯	◯	◯	◯	◯	◯	◯

Other (please specify)

Examining Acquisition Leaders' Readiness to Support LandCyber Operation

***4. Which major organization you are under?**

	CECOM	RDECOM	ATEC	PEO C3T	PEO IEWS	PEO EIS	JPEO-CBD	Other
Selection	◯	◯	◯	◯	◯	◯	◯	◯

Other (please specify)

These definitions apply to the rest of the questions (5-18):

Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers and their operators.

Cybersecurity is part of the defensive aspect of cyberspace operations.

LandCyber is a unified overarching operational and institutional solution framework to account for cyberspace to all aspects of Army operations.

***5. The following best describes the level of involvement that my job has with cyberspace operations, cybersecurity, or related fields.**

	Highly Involved	Involved	Somewhat Involved	Minimally Involved	Not Involved
Selection	◯	◯	◯	◯	◯

***6. I personally have cybersecurity certification through a National Initiative for Cybersecurity Education approved organization; select all that apply.**

- ☐ Global Industrial Cyber Security Professional (GICSP) from GIAC
- ☐ Certified Information Systems Security Professional from (ISC)2
- ☐ Graduate Certificates in Cyber Security from UNUC
- ☐ Cybersecurity Specialist from CISCO
- ☐ Cybersecurity Nexus from ISACA
- ☐ Risk Management from DRI International
- ☐ Secure+ from CompTIA
- ☐ Insider Threat from SEI CERT
- ☐ Cybersecurity Certification from McAfee
- ☐ Other (please specify)

Examining Acquisition Leaders' Readiness to Support LandCyber Operation

***7. The following best describes my level of cyberspace operations and/or cybersecurity training to support my job.**

- ◯ Amount that exceeds requirements and facilitates certification of expertise
- ◯ Amount that exceeds requirements and facilitates professional growth
- ◯ Appropriate amount to accomplish my job
- ◯ Minimum amount to accomplish my job
- ◯ Insufficient amount to accomplish my job

***8. Order these cybersecurity processes in order from the year they first introduce 1st, 2nd, 3rd:**

☐	RMF	☐ Don't Know
☐	DIACAP	☐ Don't Know
☐	DITSCAP	☐ Don't Know

***9. Match the cybersecurity processes to the underlining approaches:**

	RMF	DIACAP	DITSCAP	Don't Know
System Level Approach	◯	◯	◯	◯
Joint Task Force Transformation Initiative	◯	◯	◯	◯
Enterprise Level Approach	◯	◯	◯	◯

***10. What is your assessment in percentage of cyberspace operations that impacts land warfare?**

	0-15%	15-40%	40-60%	60-85%	85-100%
Selection	◯	◯	◯	◯	◯

***11. In your current situation, can you, as an acquisition leader, improve future LandCyber operation?**

- ◯ Yes
- ◯ No

Examining Acquisition Leaders' Readiness to Support LandCyber Operation

***12. What is your knowledge and understanding of current and future Theater level cyber risks and threats to LandCyber Operations (in term of percentage)?**

	0-15%	15-40%	40-60%	60-85%	85-100%
Current	◯	◯	◯	◯	◯
Future	◯	◯	◯	◯	◯

***13. What are your assessments of the future cybersecurity demand trends on acquisition staff?**

	Increasing Demand	Steady Demand	Decreasing Demand
Acquisition Workforce	◯	◯	◯
Acquisition Leaders	◯	◯	◯

***14. I understand the cyberspace operations and cybersecurity policies and doctrine. Select all that applies.**

- ☐ DoDI 8500.01 - Cybersecurity
- ☐ DoDI 8510.01 - DIACAP/RMF
- ☐ FM 3-38 - Cyber Electromagnetic Activities
- ☐ JP 3-12 - Cyberspace Operations
- ☐ DoDD 8140 - Cyberspace Workforce
- ☐ TRADOC Pamphlet 525-7-8 - Cyberspace Operations Concept Capability Plan 2016-2028
- ☐ Other (please specify)

***15. I understand the necessity for cybersecurity training to support my job.**

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Selection	◯	◯	◯	◯	◯

***16. My organization has an established cybersecurity training plan.**

- ◯ Yes
- ◯ No

Examining Acquisition Leaders' Readiness to Support LandCyber Operation

17. How effective does your organizational cybersecurity training plan in supporting your job?

	Selection
Not Effective	◯
Minimally Effective	◯
Somewhat Effective	◯
Effective	◯
Very Effective	◯

18. Do you have any recommendation for cyber training to better assist acquisition leaders in support of future land warfare?

19. Provide other comments you may have relate to this survey.

Thank you for completing this survey.

Page 6