REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 15-07-2010	**2. REPORT TYPE** Research Conference Paper	**3. DATES COVERED** *(From - To)* Oct 2009-Jul 2010

4. TITLE AND SUBTITLE Mission Assurance: Issues and Challenges	**5a. CONTRACT NUMBER** F4FBBA9067J001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Michael R. Grimaila Robert F. Mills Michael Haas Douglas Kelly	**5d. PROJECT NUMBER** AFIT-2010-ENV-297
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) Center for Cyberspace Research 2950 Hobson Way Wright-Patterson AFB, OH 45433	**8. PERFORMING ORGANIZATION REPORT NUMBER** 081025
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Research Laboratory Information Operations and Cyberspace Research Building 248 Wright-Patterson AFB, OH 45433	**10. SPONSOR/MONITOR'S ACRONYM(S)** AFRL/RHX
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

2010 International Conference on Security and Management (SAM10)

14. ABSTRACT

Virtually all organizations have embedded information and communication technologies into their core organizational processes as a means to increase operational efficiency, improve decision making quality, reduce delays, and/or maximize profit. However, this dependence can place the organization's mission at risk when an event causing the loss, corruption, or degradation of, or access to, a critical information resource occurs. The ability to identify, quantify, document, and manage information dependent risk is of paramount importance to reduce uncertainty in the belief that an organization can attain its mission objectives. In this paper, we discuss the concept of mission assurance with respect to information technology dependence and identify issues and challenges to attaining mission assurance. We propose that mission assurance in federated environments is best achieved through a combination of standardized risk management practices and shared situational awareness among entities involved in concurrently executing the mission.

15. SUBJECT TERMS

Mission assurance; situational awareness; cyber damage assessment; mission impact assessment

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Michael R. Grimaila
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	7	**19b. TELEPHONE NUMBER** *(include area code)* 937-255-3636 x4800 (DSN 785)

Mission Assurance: Issues and Challenges

Michael R. Grimaila[1], Robert F. Mills[1], Michael Haas[1,2], and Douglas Kelly[2]
[1]Air Force Institute of Technology, Wright-Patterson AFB, Ohio 45433, USA
[2]Air Force Research Laboratory, Wright-Patterson AFB, Ohio 45433, USA

Abstract – *Virtually all organizations have embedded information and communication technologies into their core organizational processes as a means to increase operational efficiency, improve decision making quality, reduce delays, and/or maximize profit. However, this dependence can place the organization's mission at risk when an event causing the loss, corruption, or degradation of, or access to, a critical information resource occurs. The ability to identify, quantify, document, and manage information dependent risk is of paramount importance to reduce uncertainty in the belief that an organization can attain its mission objectives. In this paper, we discuss the concept of mission assurance with respect to information technology dependence and identify issues and challenges to attaining mission assurance. We propose that mission assurance in federated environments is best achieved through a combination of standardized risk management practices and shared situational awareness among entities involved in concurrently executing the mission.*

Keywords: mission assurance; situational awareness; mission impact assessment

1 Introduction

Modern organizations embed information and communication technologies (ICT) into their core processes as a means to facilitate the collection, storage, processing, and exchange of data to increase operational efficiency, improve decision quality, and reduce costs. Military organizations are especially dependent on ICT, collectively called "cyberspace," as they continue to build and link together complex systems of systems to provide enhanced capabilities in decision support, intelligence, logistics, operations, planning, and situational awareness. Unfortunately, this dependence can place the organizational mission at risk when an information incident (e.g., the loss, corruption, or degradation of a critical information resource or communication link) occurs [1-5]. Despite the fact that the success of virtually every military objective can be impacted by ICT directly or indirectly, little military guidance has been promulgated to guide organizations to develop a formal understanding between the organizational mission and the underlying ICT. The lack of universally accepted standards for understanding mission risk that can be implemented across organizational boundaries create the potential for serious consequences.

In this paper, we explore the concepts of mission and mission assurance as well as identify issues and challenges to attaining mission assurance in large-scale, federated environments. More importantly, we propose that mission assurance is best achieved through a blend of standardized risk management practices, shared situational awareness, and constant collaboration among the different entities involved in concurrently executing the mission.

The remainder of this paper is structured as follows: In section 2, we define mission and mission assurance. In section 3, we examine the relationship between mission assurance and information technology and review existing guidance for mitigating mission risks. In section 4, we summarize the challenges encountered in attaining mission assurance. Finally, in section 5 we present our conclusions and make recommendations for future works.

2 Mission and Mission Assurance

In all endeavors, it is essential to first clearly define the vocabulary used in order to remove any ambiguity in understanding the meaning of words. This is important because misunderstandings can occur when various communities of interest have different meanings for the same words. This is especially true when discussing "mission" because of the large number of organizational levels, temporal intervals, scales, scopes, and contexts in which it is used.

A typical organization continually reassesses and communicates their "mission" which ideally is a clear and concise written mission statement designed to identify and differentiate their reason for existence. More specifically, the mission statement guides the actions performed and decisions made in the organization, spells out its overall goal, and provides a sense of direction. The mission statement provides "the framework or context within which the company's strategies are formulated" [6]. Note that in this case, the context of the use of the word mission implies an enduring set of objectives at the strategic level (i.e., the long term goals of the organization). However, military units within the organization execute day-to-day activities to accomplish the overall strategic mission. Hence, these units focus more on achieving multiple shorter-term, time-sensitive, more dynamic mission objectives at the operational or tactical level rather than the longer-term and relatively time-insensitive and static strategic objectives.

2.1 Mission

Military missions are inherently complex endeavors involving dynamically changing, time-sensitive, coordinated operations involving multiple organizations. Within the United Stated (US) Department of Defense (DoD), Joint Publication 1-02 "Department of Defense Dictionary of Military and Associated Terms" provides the following definitions for the word mission [7]:

> *1. The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore,*
> *2. In common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task,*
> *3. The dispatching of one or more aircraft to accomplish one particular task.*

Note that the definitions provided are task focused and seem to imply simple, limited duration, tractable complexity, and easily measured and quantified goal attainment. However, more commonly the use of the term mission is broader in scope. For example, Donley [8] analyzed the use of the term mission across multiple DoD documents and identified that more commonly a mission is "considered generally as integrating many activities around a common theme or purpose" [8]. One of the key problems encountered when discussing mission assurance is the lack of a standardized, widely accepted definition for the word "mission." While the term "mission" frequently appears in military publications, rarely is it defined or a reference provided to its meaning which often results in confusion and misunderstanding [9, 10].

Joint Publication 5-0 "Joint Operation Planning" (JP 5-0) provides guidance on conducting joint, interagency, and multinational planning activities across the full range of military operations [11]. Joint operation planning includes all activities that must be accomplished to plan for an operation including the mobilization, deployment, employment, and sustainment of forces. JP 5-0 identifies that missions are linked to tasks through objectives and effects. Three types of tasks are defined: Specified, Implied, and Essential as shown below in Table 1.

Table 1 – Three Types of Tasks [11]

Task Type	**Definition**
Specified	A task that is specifically assigned to an organization by its higher headquarters.
Implied	A task derived during mission analysis that an organization must perform or prepare to perform to accomplish a specified task or the mission, but which is not stated in the higher headquarters order.
Essential	A specified or implied task that an organization must perform to accomplish the mission. An essential task is typically included in the mission statement.

Joint Chiefs of Staff Manual 3500.04C "Universal Joint Task List (UJTL)" provides a common language and reference system for joint force commanders, combat support agencies, operational planners, combat developers, and trainers to communicate mission requirements. It is the basic language for the development of a joint mission essential task list (JMETL) or agency specific mission essential task list (AMETL) that identifies required capabilities for mission success [12]. The relationship between missions, operations (military action), and tasks are shown in Figure 1.

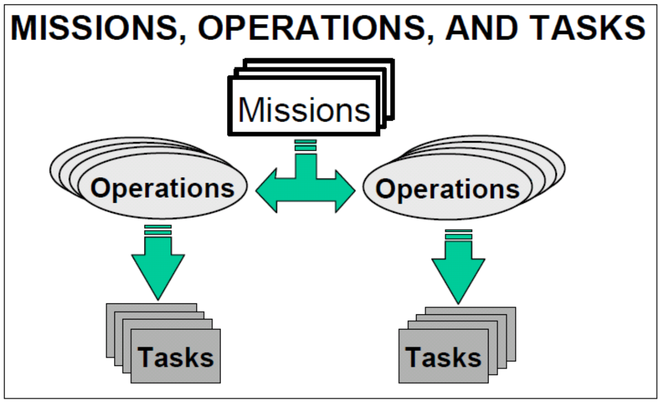

Figure 1 – Relationship between Missions, Operations, and Tasks [12]

In Field Manual 7-0 (FM 7-0) "Training the Force", a Mission Essential Task (MET) is defined as "a collective task in which an organization has to be proficient to accomplish an appropriate portion of its wartime operational mission" [13]. METs are developed based upon the recognition that organizations cannot sustain proficiency on every possible task. As a result, the commander identifies tasks that are essential to accomplishing the mission.

A Mission Essential Task List (METL) is a list of the tasks that the commander deems essential to mission success. More importantly, the METL explicitly delineates the conditions and performance standards to assure successful mission accomplishment. The benefits of METL development are shown in Table 2.

Table 2 – Benefits of METL Development [13]

Definition
Reduces and prioritizes the number of tasks the organization must train.
Focuses the unit's training on essential tasks.
Provides a forum for professional discussion among commanders concerning the linkage between mission and training.
Enables subordinate commanders and key Non-

Commissioned Officers (NCOs) to crosswalk collective leader and individual tasks to the mission.
Leads to “buy-in” and commitment of unit leaders to the organizations training plan.

Since METs and METLs document the mission essential tasks, they may be used to develop real-time metrics that represent the current capability of the organization to fulfill its mission. By monitoring the appropriate set of METs, one can infer the likelihood the organization can complete its mission.

2.2 Assurance

Assurance is defined in the American Heritage dictionary as follows [14]:

- The act of assuring.
- A statement or indication that inspires confidence; a guarantee or pledge.
- Freedom from doubt; certainty.
- Self-confidence.
- Excessive self-confidence; presumption.
- Chiefly British Insurance, especially life insurance.

In the context of this paper, assurance is focused upon reducing uncertainty in the expected outcome of an activity. The concept of assurance is closely related to the concept of risk. Risk is formally defined as “the effect of uncertainty on objectives” [15]. While “risk” is often thought of as generating a negative impact, it is more proper to view risk as exposure to the consequences of uncertainty which can impact the organization both positively as well as negatively. Risk is often modeled by a probabilistic analysis involving both the likelihood of potential events and their consequences on the organizational objectives. A deficiency in the information, knowledge, or understanding of an event, its consequence, or likelihood is defined as uncertainty in the context of risk [16].

Within the military, risk management is ingrained into the military decision making process. The purpose of risk management is to identify potential variations from the organizational objectives so that these risks can be managed in order to maximize opportunities, minimize losses, and improve decisions, and increase the likelihood of successful outcomes. Risk management involves “coordinated activities to direct and control an organization with regard to risk” [15]. Ideally, organizations implement a risk management process that involves the “systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk” [16].

2.3 Mission Assurance

By combining the definitions “Mission” and “Assurance” discussed above, we gain insight into the concept of “Mission Assurance.” Mission Assurance is about reducing uncertainty in the belief of the organization’s ability to successfully complete its mission. Mission assurance is not a new phenomenon as it has traditionally has been discussed in well established engineering endeavors including:

- High availability systems
- Failure analysis
- Performance engineering
- Quality assurance
- Reliability
- Reliable system design
- Redundancy
- Security engineering
- Hazard identification
- Software engineering
- Systems engineering
- Safety engineering

In these areas, the scope of the “mission” is clearly defined and limited to assure tractable analysis. For example, consider one definition provided by a systems engineering community for mission assurance [17]:

> *“A full life-cycle engineering process to identify and mitigate design, production, test, and field support deficiencies of mission success. It includes the disciplined application of system engineering, risk management, quality and management principles to achieve mission success.”*

In this definition, we see that the formal identification and understanding of the relationship between mission success and underlying variables which can impact mission success is critical to attaining mission assurance. Further, the use of established risk management principles provides a pathway to mitigate identified mission risks.

While the concept of Mission Assurance is deeply embedded in military doctrine and mission planning, it is not formally defined in the DoD Dictionary of Military and Associated Terms [7]. One possible explanation for this omission is that since there is not a universally accepted definition for the term mission, defining mission assurance would not provide further clarity. Despite the omission, other DoD guidance does address mission assurance. For example, consider DoD Instruction 8500.2 “Information Assurance (IA) Implementation” defines the concept of Mission Assurance Category (MAC) [18]:

> *Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals*

> *and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity.*

Given the recognition of the importance of information systems in support of organizational missions, systems are assigned one of three MAC levels as follows [18]:

- Mission Assurance Category I (MAC I). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.

- Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces.

- Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term.

DoD Directive 3020.40, "DoD Policy and Responsibility for Critical Infrastructure" provides the following definition for "mission assurance" [19]:

> *"A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the Department of Defense to carry out the National Military Strategy. It links numerous risk management program activities and security-related functions, such as force protection; antiterrorism; critical infrastructure protection; IA continuity of operations; chemical, biological, radiological, nuclear, and high explosive defense; readiness; and installation preparedness to create the synergy required for the Department of Defense to mobilize, deploy, support, and sustain military operations throughout the continuum of operations."*

While this definition is focused in the area of critical infrastructure protection, it highlights the need for a holistic understanding of risk through established risk management principles. However, this guidance must be translated and implemented within lower levels of the organization in order to be effective.

3 Mission Assurance and ICT Risk

Mission Assurance requires mission risk management. Understanding mission risk requires defining the mission objectives, identifying the factors which impact the objectives, developing an understanding of the environment and context in which the objectives are fulfilled, quantifying the value that each objective contributes to meeting the strategic mission, and considerations for potential events or scenarios which can impact the mission objectives. Understanding the impact that ICT can have on tasks, operations, and the mission is of paramount importance. There is a great need to develop methods to quantify the mission impact resulting from ICT incidents. Only through introspection can an organization understand its true operational risk, take proactive measures to mitigate risk to an acceptable level, and plan for contingencies to improve their operational mission resilience.

Modern organizations are now more dependent upon external organizations to fulfill their mission objectives than ever before. As a consequence, the ability to mitigate mission risk through the application of controls to internally controlled resources is growing smaller while the need to monitor and react to changes in the state of critical dependencies is growing. Figure 2 shows a representation of mission assurance strategy adapted from "Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments" [9]. In this representation, mission assurance is supported by two activities: the left branch represents activities you conduct prior to risk materializing and the right branch represents activities that you take in response to a risk materializing. This highlights the need for a holistic mission assurance approach that addresses risk mitigation through risk management, continuity of operations planning, contingency planning, and situational awareness.

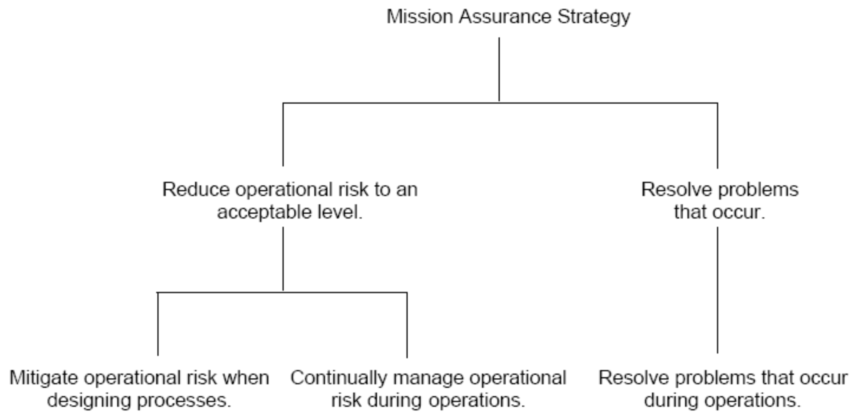
Mission Assurance Strategy
Reduce operational risk to an acceptable level.
Resolve problems that occur.
Mitigate operational risk when designing processes.
Continually manage operational risk during operations.
Resolve problems that occur during operations.

Figure 2 – Mission Assurance Strategy [9]

4 Mission Assurance Challenges

There are numerous challenges to attaining mission assurance. Five such challenges researchers must address that we have identified include (1) complexity due to large size of the federated environment, (2) lack of a standard mission assurance approach across all organizational levels, (3) gaps in the current DoD approach to assuring the mission and managing risk, (4) different use and definitions of what a system is, and (5) growing dependence on external information resources to achieve mission assurance. While the concept seems to be well understood by multiple communities, a standardized mission assurance approach that provides detailed guidance at the strategic, operational, and tactical levels is missing. Risk management is critical to attain mission assurance, but in practice it is difficult to apply in large scale, federated environments. For example, across the DoD there are more than 7 million computers and 15,000 networks which makes risk identification and quantification difficult [20]. The sheer scale and complexity of cyberspace makes data collection and formal modeling of the cyber domain cost prohibitive. A key question is “How can risk management strategies designed to be applied within a single organization be effectively and economically applied across a federated enterprise with diverse stakeholders?” What is needed is a standardized approach that can be applied and integrated across all levels within an organization and among different organizational units. Unfortunately, traditional approaches to risk management may be impractical because the nature of the underlying risks is systemic and resistant to traditional cost ‑ benefit analysis [21]. Some of the more relevant questions include “How much should an organization spend to understand its risk?,” “Who should encumber the cost of protecting a resource that supports multiple organizational missions?,” and “How do you prioritize competing organizations objectives?”

Within the DoD, the approach of assigning MAC levels to individual systems and national security classifications to sources of information, used as a proxy for mission assurance management, is insufficient to develop a formal understanding of ICT related mission risk. A key limitation is that it assigns the mission criticality value to the system instead of explicitly formalizing the relationship between the mission and the information contained on the system. This assignment is made at the time the system is placed into operation and may change over time. Further, it assumes that the owner of the system who obtains the authority to operate the system is fully aware of all those who are dependent upon the system. What is needed is a more dynamic, automated approach that fuses information available from the ICT to the missions it supports. For example, Goodall et al. have demonstrated the ability to automate the correlation between cyber users, missions, and assets [22, 23].

Another issue is in defining the “system”. The “system” may be defined differently within different organizations. For some, the system may be equivalent to a single platform, for others, the system may be a group of communicating platforms, and for still others, the system may be a dynamically-defined construct that changes significant characteristics from day-to-day. This has implications for the acquisition community, among others, and its ability to equip the Air Force as well as the Air Force’s ability to present capability to combatant commanders that is resilient to cyber attack while operating in a contested environment.

As an organization’s mission becomes more dependent on external resources, the ability to rapidly respond to risks beyond their control that occur becomes extremely important. This requires capturing, maintaining, and refining an understanding of the mission critical information dependencies so that these dependencies can be monitored in real time in support of situational awareness. The ability to rapidly communicate mission impact is important to inform decision making to assure the mission outcome. Multiple efforts are underway to formalize the relationship between the mission and their dependencies so that they can be rapidly communicated to decision makers in support of risk management, continuity of operations, contingency planning, and situational awareness [24-27].

5 Conclusions

Mission assurance is a simple concept to understand, but is difficult to practice in large, federated environments. The need to identify, quantify, document, and manage ICT dependent risk is of paramount importance to reduce uncertainty in the belief that the organization can attain its mission objectives. In this paper, we presented the concept of mission assurance, identified issues and challenges to attaining mission assurance, and proposed that mission assurance in federated environments is best achieved through a mix of standardized risk management, shared situational awareness, and close collaboration among the entities involved in mission execution.

6 Acknowledgements

This work was supported by a research grant from the Air Force Research Laboratory (F4FBBA9067J001).

7 Disclaimer

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

8 References

[1] Grimaila, M.R. and Fortson, L.W., "Towards an Information Asset-Based Defensive Cyber Damage Assessment Process," Proc. of the 2007 IEEE Computational Intelligence for Security and Defense Applications (CISDA 2007); Honolulu, HI; April 1-5, 2007, pp. 206-212.

[2] Grimaila, M.R., Mills, R.F., and Fortson, L.W., "An Automated Information Asset Tracking Methodology to Enable Timely Cyber Incident Mission Impact Assessment," Proc. of the 2008 International Command and Control Research and Technology Symposium (ICCRTS 2008), Bellevue, WA, 17-19 June 2008.

[3] Grimaila, M.R., Fortson, L.W., Sutton, J.L, and Mills, R.F., "Developing Methods for Timely and Relevant Mission Impact Estimation," Proc. of the 2009 SPIE Defense, Security and Sensing Conference (SPIE DSS 2009), Orlando, Florida, April 13-17, 2009.

[4] Grimaila, M.R., Schechtman, G., and Mills, R.F., "Improving Cyber Incident Notification in Military Operations," Proc. of the 2009 Institute of Industrial Engineers Annual Conference, Miami, FL, May 30, 2009 - June 3, 2009.

[5] Grimaila, M.R., Fortson, L.W., and Sutton, J.L, "Design Considerations for a Cyber Incident Mission Impact Assessment (CIMIA) Process," Proc. of the 2009 International Conference on Security and Management (SAM09), Las Vegas, Nevada, July 13-16, 2009.

[6] Hill, Ch., Jones, G. Strategic Management. Houghton Mifflin Company: New York, 2008.

[7] JP1-02, "Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms," October 2009.

[8] Donley, M.B., "Problems of Defense Organization and Management," Joint Forces Quarterly (JFQ), Summer 1995.

[9] Alberts, C.J. & Dorofee, A.J., "Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments," Carnegie Mellon University Networked Systems Survivability Program Report, 2005.

[10] Hale, B., "Mission Assurance: A Review of Continuity of Operations Guidance for Application to Cyber Incident Mission Impact Assessment (CIMIA)," Master's Thesis, Department of Systems Engineering and Management, Air Force Institute of Technology, June 2010.

[11] JP 5-0, "Joint Operation Planning. JP 5-0," Washington: US DoD, Joint Chiefs of Staff, 2006.

[12] CJCSM 3500.04C, "Universal Joint Task List (UJTL). CJCSM 3500.04C," Washington: US DoD, 1 July 2002.

[13] FM 7-0, "Army Field Manual 7-0: Training the Force," Headquarters Department of the Army, October 2002.

[14] American Heritage Dictionary, 4th Edition, http://www.houghtonmifflinbooks.com/ahd/.

[15] ISO 73 (2009) ISO GUIDE 73: Risk Management — Vocabulary. Intl. Organisation for Standardisation), 1st Ed.

[16] ISO 31000 (2009) ISO 31000:2009: Risk management -- Principles and guidelines. ISO, 1st Ed. 2009.

[17] Hefner, R., et al. (November 2004) "Mission Assurance and CMMI", CMMI Technology Conference & User Group, Northrop Grumman Corporation.

[18] DoDI 8500.2, "Information Assurance (IA) Implementation," DoDI 8500.2. Washington: United States Department of Defense, 6 February 2003.

[19] DoDD 3020.40, "DoD Policy and Responsibilities for Critical Infrastructure," DoDD 3020.40. Washington: United States Department of Defense, 14 January 2010.

[20] Daniel, L., "Officials warn of 'phishing' scams targeting troops," USAF News, 10 May 2010, http://www.af.mil/news/story.asp?storyID=123203895

[21] Rosenzweig, P., “National Security Threats in Cyberspace – Post Workshop Report,” 2009, http://www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf

[22] Goodall, J.R., D’Amico, A, and Kopylec, J.K, “CAMUS: Automatically Mapping Cyber Assets to Missions and Users,” Proc. of the 2010 Military Communications Conference (MILCOM 2009), 2009.

[23] D’Amico, A., Buchanan, L., Goodall, J., and Walczak, P., “Mission Impact of Cyber Events: Scenarios and Ontology to Express the Relationships Between Cyber Assets, Missions and Users,” Proc. of the 2010 International Conference on Information Warfare and Security (ICIW 2010), WPAFB, OH, April 8-9, 2010.

[24] Anderson, E., Choobineh, J., Fazen, M., and Grimaila, M.R., “Mission Impact: Role of Protection of Information Systems,” Proc. of the 2010 Intl. Conf. on Information Warfare and Security (ICIW 2010), WPAFB, OH, April 8-9, 2010.

[25] Hale, B. Grimaila, M.R., Mills, R.F., Haas, M., and Maynard, P., “Communicating Potential Mission Impact using Shared Mission Representations,” Proc. of the 2010 International Conference on Information Warfare and Security (ICIW 2010), WPAFB, OH, April 8-9, 2010.

[26] Hellesen, D., and Grimaila, M.R., “Information Asset Value Quantification Expanded,” Proc. of the 2010 International Conference on Information Warfare and Security (ICIW 2010), WPAFB, OH, April 8-9, 2010.

[27] Haigh, T., Harp, S., and Payne, C., “AIMFIRST: Planning for Mission Assurance,” Proc. of the 2010 International Conference on Information Warfare and Security (ICIW 2010), WPAFB, OH, April 8-9, 2010.