A Systematic Comprehensive Computational Model for Stake Estimation in Mission Assurance

Applying Cyber Security Econometrics System (CSES) to Mission Assurance Analysis Protocol (MAAP)

Robert K. Abercrombie, *Senior Member, IEEE*
Frederick T. Sheldon, *Senior Member, IEEE*
Cyberspace Sciences and Information Intelligence Group
Computational Sciences and Engineering Department
Oak Ridge National Laboratory (ORNL)
Oak Ridge, TN 377831 USA
abercrombier@ornl.gov, sheldonft@ornl.gov

Michael R. Grimaila, *Senior Member, IEEE*
Dept. of Systems Engineering and Management
Center for Cyberspace Research
Air Force Institute of Technology (AFIT)
Wright-Patterson Air Force Base, Ohio 45433 USA
Michael.Grimaila@afit.edu

***Abstract*—In earlier works, we presented a computational infrastructure that allows an analyst to estimate the security of a system in terms of the loss that each stakeholder stands to sustain as a result of security breakdowns. In this paper, we discuss how this infrastructure can be used in the subject domain of mission assurance as defined as the full life-cycle engineering process to identify and mitigate design, production, test, and field support deficiencies of mission success. We address the opportunity to apply the Cyberspace Security Econometrics System (CSES) to Carnegie Mellon University and Software Engineering Institute's Mission Assurance Analysis Protocol (MAAP) in this context.**

Keywords—Cybersecurity Metrics, Risk Management, Stakeholder Value, Information Assurance Controls and Mitigation Costs

I. INTRODUCTION

In earlier works, we presented a computational infrastructure that allows an analyst to estimate the security of a system in terms of the loss that each stakeholder stands to sustain as a result of security breakdowns [1-3]. Here, we discuss how this infrastructure can be used in the subject domain of mission assurance.

Mission Assurance is a full life-cycle engineering process to identify and mitigate design, production, test, and field support deficiencies of mission success [4]. Businesses and government agencies do not differ significantly in their mission assurance needs: They all need an information environment that's reliable, available, survivable and secure enough to get the job done [5, 6] . However, it can be argued that military operations do indeed differ from non-military operations in many ways, but especially due to their dynamic nature and the criticality of consequences resulting from degraded decision making [7, 8]. Despite this difference, we can borrow from the methods used in securing non-military organizations to improve our abilities to provide accurate and timely damage assessment [8, 9]. Organizations typically use a risk management process to identify and mitigate risks to assure their organizational mission [10]. Risk management provides a documented, structured, and transparent process to identify critical resources, estimate threats and vulnerabilities that may intersect to cause harm (risks) to those resources. Moreover, the process estimates the likelihood of risk occurrence and evaluates tradeoffs among control measures used to mitigate the risks, and periodically revisits the analyses as needed. However, the value of the analysis is a strong function of the accuracy of the inputs to the process.

Mission assurance enables agencies (or enterprises) to integrate security with continuity and risk management practices to develop a day-to-day operational model that focuses on safeguarding employees and managing business risk. The ultimate goal of mission assurance is to create a state of resilience that supports the continuation of an enterprise's critical business processes and protects its employees, assets, services and functions. Mission assurance provides a basis to address risks in a uniform and systematic manner across the enterprise. The objective is to have the business processes and the infrastructure support the delivery of assured services [11].

II. DOD MISSION ASSURANCE CATEGORIES

All DoD information systems require an assigned *mission assurance category* (MAC) that is directly associated with the importance of the information they contain relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission [12]. Specific requirements for availability and integrity are associated with the MAC, while requirements for confidentiality are associated with the information classification or sensitivity and need-to-know. Both sets are primarily expressed in the form of Information Assurance (IA) controls and are satisfied by: a) employing the tenets of defense-in-depth for layering IA solutions within/among IT asset(s), and b) ensuring appropriate robustness of the solution, as determined by the relative strength of the countermeasure and the confidence that it is

The submitted manuscript has been authored by a contractor of the U.S. Government under contract DE-AC05-00OR22725. Accordingly, the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes.

978-0-7695-4211-9 2010
U.S. Government Work Not Protected by U.S. Copyright
DOI 10.1109/SocialCom.2010.171

implemented and will perform as intended (e.g., authentication and non-repudiation).

MACs are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

1. E2.1.38.1. Mission Assurance Category I
2. E2.1.38.2. Mission Assurance Category II
3. E2.1.38.3. Mission Assurance Category III

Ideally, the assignment of the MAC category would be based upon an analytical framework that documents and justifies the category based upon all stakeholder inputs. Unfortunately, this task often is delegated to an individual who has limited understanding of the mission value of the resource [13]. For this reason there is a great need for a value analysis methodology that provides transparency in the process.

III. Cyber Security Econometrics System (CSES) Foundations

CSES provides many advantages over other known measurement or analysis systems or methodologies such as: (1) it reflects variances existing between different users or stakeholders of the system [1]. Different stakeholders may attach different stakes to the same requirement or service (e.g., a service may be provided by an information technology system, cyber, enterprise or process control system, etc.). (2) For a given stakeholder, CSES can highlight variances that may exist among the stakes attached to satisfying each requirement. For example, a stakeholder may attach or identify different stakes to satisfying different requirements within the overall system. (3) For a given compound specification (e.g., combination(s) of commercial off the shelf software and/or hardware), CSES can identify variances that may exist amongst the levels of verification and validation that are performed on components of the system (or specification). The verification activity may produce higher levels of assurance in satisfying some components of the specification more than others.

The CSES follows a defined process [1, 2, 14, 15]. The initial inputs (1) organizational mission (and components thereof), (2) value of its objectives and assets if uninterrupted, and (3) the components of the enterprise system that support each mission component, are determined by stakeholders.

The stakeholders, with assistance from SMEs, define the criteria of a quantitative value of an asset. For example, the criteria may include:

- Financial basis (e.g., operational cost of downtime per unit of time defined by hardware/software costs, facilities and staffing versus profit); which is the quantitative measurement to be used within the CSES.
- Federal Information Security Management Act (FISMA) of 2002, stakeholder derived value of assets per NIST 800-60, and/or FIPS 199/200 (February 2004, Standards for Security Categorization of Federal Information and Information Systems) dictated requirements.
- Stakeholder defined requirements; acceptable and unacceptable impact levels against the value related to IA tenets of confidentiality, availability and integrity may also be examined.

The CSES process proceeds in three steps (generation of stakes matrix, dependency matrix, and threat matrix) to derive the mitigation costs matrix[1]. CSES accounts for failure costs and verification (i.e., mitigation costs). CSES provides a:

- Framework for measuring the appropriate attributes that support the decisions necessary to (1) design security countermeasures, (2) choose between alternative security architectures, (3) respond to events such as intrusions or attacks and (4) improve security (including reliability and safety) during both design and operational phases.
- Comprehensive basis for choosing courses of action that have the highest risk reduction return on investment, i.e., reduce the most risks for the lowest cost.

The basis of CSES stems from and is consistent with the spirit of Value Based Software Engineering.

CSES comprehends the different organizational mission needs for all stakeholders, including reliability and safety. CSES identifies information assurance controls and mitigation costs as an investment toward assuring mission success.

IV. CSES - A Cascade of Linear Models

In this section, we present the composition of the CSES model and motivate its application.

A. The Stakes Matrix

We consider a system S and we let H_1, H_2, H_3, … H_k be stakeholders of the system, i.e., parties that has a stake in its operation. We let R_1, R_2, R_3, … R_n, be security requirements that we wish to impose on the system, and we let $ST_{i,j}$, for $1 \le i \le k$ and $1 \le i \le n$ be the stake that stakeholder H_i has in meeting requirement R_j. We let PR_j, for $1 \le j \le n$, be the probability that the system fails to meet security requirement R_j, and we let MFC_i, (Mean Failure Cost), for $1 \le i \le k$, be the random variable that represents the cost to stakeholder H_i that may result from a security failure.

We quantify this random variable in terms of financial loss per unit of operation time (e.g. $/hour); it represents the loss of service that the stakeholder may experience as a result of a security failure. Under some assumptions of statistical independence, we find that the Mean Failure Cost for stakeholder T_i can be written as:

$$MFC_i = \sum_{1 \le j \le n} ST_{i,j} \times PR_j .$$

If we let MFC be the column-vector of size k that represents mean failure costs, let ST be the k×n matrix that represents stakes, and let PR be the column-vector of size n that represents probabilities of failing security requirements, then this can be written using the matrix product (∘):

$$MFC = ST \circ PR.$$

The Stakes matrix is filled, row-by-row, by the corresponding stakeholders. As for PR, we discuss below how to generate it.

B. The Dependency Matrix

We consider the architecture of system S, and let C_1, C_2, C_3,… C_h, be the components of system S. Whether a particular security requirement is met or not may conceivably depend on which component of the system architecture is operational. Lets we assume that no more than one component of the architecture may fail at any time. We define the following events:

- E_i, $1 \le i \le h$, is the event: the operation of component C_i is affected due to a security breakdown.
- E_{h+1}: No component is affected.

Given a set of complementary events E_1, E_2, E_3, … E_h, E_{h+1}, we know that the probability of an event F can be written in terms of conditional probabilities as:

$$P(F) = \sum_{k=1}^{h+1} P(F \mid E_k) \times P(E_k).$$

We instantiate this formula with F being the event: the system fails with respect to some security requirement. To this effect, we let F_j denote the event that the system fails with respect to requirement R_j and we write (given that the probability of failure with respect to R_j is denoted by PR_j):

$$PR_j = \sum_{k=1}^{h+1} P(F_j \mid E_k) \times P(E_k).$$

If

- we introduce the DP (Dependency) matrix, which has n rows and h+1 columns, and where the entry at row j and column k is the probability that the system fails with respect to security requirement j given that component k has failed (or, for k=h+1, that no component has failed),
- we introduce vector PE of size h+1, such that PE_k is the probability of event E_k, then we can write

$$PR = DP \circ PE.$$

Matrix DP can be derived by the system's architect, in light of the role that each component of the architecture plays to achieve each security goal. As for deriving vector PE, we discuss this matter in the next section.

C. The Impact Matrix

Components of the architecture may fails to operate properly as a result of security breakdowns brought about by malicious activity. In order to continue the analysis, we must specify the catalog of threats that we are dealing with, in the same way that analysts of a system's reliability define a fault model. To this effect, we catalog the set of security threats that we are facing, and we let T_1, T_2, T_3, … T_p, represent the event that a cataloged threat has materialized, and we let T_{p+1}, be the event that no threat has materialized. Also, we let PT be the vector of size p+1 such that

- PT_q, for $1 \le q \le p$, is the probability that threat T_q has materialized during a unitary period of operation (say, 1 hour).
- PT_{p+1} is the probability that no threat has materialized during a unitary period of operation time.

Then, by virtue of the probabilistic identity cited above, we can write:

$$PE_k = \sum_{q=1}^{p+1} P(E_k \mid T_q) \times PT_q.$$

If

- we introduce the IM (Impact) matrix, which has h+1 rows and p+1 columns, and where the entry at row k and column q is the probability that component Ck fails given that threat q has materialized (or, for q=p+1, that no threat has materialized),
- we introduce vector PT of size p+1, such that PT_q is the probability of event T_q, then we can write

$$PE = IM \circ PT.$$

Matrix IM can be derived by analyzing which threats affect which components, and assessing the likelihood of success of each threat, in light of perpetrator behavior and possible countermeasures. Vector PT can be derived from known perpetrator behavior, perpetrator models, known system vulnerabilities, etc. We refer to this vector as the *Threat Configuration Vector* or simply as the *Threat Vector*.

V. Application of the CSES to the MAAP Protocol

MAAP defines a qualitative protocol for analyzing operational risk in work processes [16]. In this section we identify the appropriate components of CSES that may be used to refine the MAAP protocol in a quantitative way (i.e., stake estimation for mission assurance). This refinement is preliminary, as the mathematical connections are not developed and are only described qualitatively as a so-called *crosswalk* from the CSES to the MAAP (due in part to a lack of time [and funding])[1]. The following seven guidelines collectively form the foundation of MAAP:

1. Determine mission objectives.
2. Characterize all operations conducted in pursuit of the mission.
3. Define risk evaluation criteria in relation to the mission objectives.

[1] In this context the term *crosswalk* refers to a process of mapping the contents of two tables (or sets of functions or guidelines as is the case) resulting in the linkages (i.e., the appropriate cross-references).

4. Identify potential failure modes.
5. Perform a root cause analysis for each failure mode.
6. Develop an operational risk profile of the mission.
7. Ensure that operational risk is within tolerance.

The remainder of this section describes each guideline in detail (as excerpted from [16]), juxtaposed with the applicable CSES concept.

A. Determine Mission Objectives

Goal: To set the scope of the risk analysis.

Description: In MAAP, the mission of a work process is used to define the boundaries of the risk analysis. All activities performed in pursuit of the mission are included in the analysis, no matter where they are performed. In this way, identifying and documenting the mission sets the boundaries, or limits, of the resulting analysis.

Rationale: Determining the mission objectives are important for setting the scope of the analysis (i.e., defining what will be included in the analysis as well as what will be excluded from consideration). In addition to setting the scope of the analysis, the mission also establishes the basis for measuring risk. All potential losses are examined in relation to the mission objectives during the risk analysis.

Outcome: A set of documented mission objectives that set the scope of the risk analysis.

CSES Crosswalk: CSES provides a measure of reliability, security and safety of a system (or an enterprise) that accounts for the criticality of each requirement as a function of one or more stakeholders' interests in that requirement. For a given stakeholder, CSES reflects the variance that may exist among the stakes one attaches to meeting each requirement.

B. Characterize all operations conducted in pursuit of the mission.

Goal: To characterize the operational performance characteristics of a process.

Description: Once mission objectives are identified, all operations performed in pursuit of those objectives must be characterized to provide a benchmark of operational performance. At a minimum, one must define the following performance parameters for the process being analyzed:

- the sequence and timing of all activities needed to achieve the mission objectives, including all relevant interrelationships and dependencies among the activities
- roles and responsibilities for completing each activity
- the key objectives of each activity (i.e., the local mission of each activity)
- the relative strengths and weaknesses of each activity
- the acceptable range of normal, or expected, operating conditions for the process, including expected workflow capacity and parameters of technological performance
- known history of operational problems

The above parameters in combination with the mission objectives define an operational model for a process.

Rationale: An accurate model of operational performance characteristics is essential when characterizing operational risk. It is used to illustrate where actual performance deviates from the desired or expected performance, thus providing the basis for risk identification.

Outcome: An operational model of the work process being analyzed.

CSES Crosswalk: Inherent in CSES is the Dependency Matrix (DM). The DM links requirements (stakeholder's missions) with components (i.e., one or more components are needed to satisfy a given functional requirement). The concept is to link the probability of failing a particular requirement with the probability of failure of a component of the system. The explanation of this probabilistic link involves an analysis of the system's architecture, to determine which component contributes to meeting which requirement. However, to illustrate our method, we present a possible solution to this problem, under a simplifying hypothesis, which is that security violations affect no more than one component at a time.

C. Define risk evaluation criteria in relation to the mission objectives.

Goal: To define one explicit standard against which operational risk can be uniformly measured.

Description: All potential losses in a risk analysis are measured in relation to mission objectives. Risk evaluation criteria define the parameters for estimating the values of impact and probability. However, the individual values of impact and probability do not directly provide a measure of operational risk. A separate measure, called risk exposure, is needed to reflect the amount of operational risk affecting each mission objective. Risk exposure combines the values of impact and probability to produce a single measure of risk. To determine risk exposure, you must establish specific criteria for combining individual measures of probability and impact. The same set of risk evaluation criteria must be uniformly applied to all operations related to the process.

Rationale: Risk evaluation criteria are important because they provide a common benchmark against which operational risk is measured. Having a single set of criteria for all operations is an essential part of establishing a uniform operational risk tolerance in a distributed process.

Outcome: A documented set of criteria used to measure impact, probability, and risk exposure.

CSES Crosswalk: The Impact Matrix (IM) addresses the failure of a component as the result of a threat materializing (i.e., risk exposure). The IM is derived by analyzing which threats affect which components and assessing the likelihood of success for each threat. The IM gives the probability of component failure which depend on three factors: (1) armor (e.g., technical controls or mitigations) that the component is provided to protect against threats and to mitigate damage in the case of successful attacks, (2) pattern of threats that the

component is subjected to, (3) degree of verification and validation that the component has undergone, be it through testing, inspection, static analysis, etc.

D. Identify potential failure modes.

Goal: To identify the ways in which a process can fail to meet its specified performance characteristics.

Description: All relevant failure modes for a process are identified by analyzing performance as defined by its operational model. As used in this context, a failure mode is any situation where the process does not meet its specified performance parameters. It typically occurs when actual performance deviates from the desired or expected performance, which, in turn, can affect the ability to achieve either a local objective or one of the mission objectives. During the analysis, failure modes are identified for:

- normal, or expected, operational conditions
- unpredictable circumstances, or occurrences, triggered by events

This two-pronged approach examines process performance for various operational situations, which is essential when establishing mission assurance.

Rationale: Identifying the potential failure modes establishes the types of impacts that can be expected during operations and provides critical information needed when identifying operational risks.

Outcome: A documented list of all failure modes for a work process.

CSES Crosswalk: This list is documented in the IM and furthered addressed and utilized in the Mitigation Costs Matrix during operational use of CSES [1]. The items described above for the IM should also be considered for matching failure modes to threats and the likelihood of a compromise.

E. Perform a root cause analysis of each failure mode.

Goal: To identify specific risks that can result in process failures

Description: A root cause analysis of each failure mode must be performed to determine the specific circumstances that trigger it. A broad range of factors must be considered in the root cause analysis, including applicable threats from the five categories, emergent threats, and inherited risks. A root cause analysis is a common technique for identifying the conditions that lead to an undesired state, such as a failure mode. This type of analysis is especially useful when identifying complex risks because it illustrates how vulnerabilities, threats, and controls combine to produce a single failure mode. It essentially produces a causal chain of risk factors that can produce a given failure mode and adversely affect process performance. When viewed together, a failure mode and the conditions that trigger it define a specific instance of operational risk.

Rationale: Performing a root cause analysis is important for establishing the combination of vulnerabilities, threats, and controls that can produce a specific failure mode. This analysis is essential for capturing complex interrelationships and dependencies among the conditions that lead to each specific occurrence of operational risk.

Outcome: A set of operational risks.

CSES Crosswalk: This is one technique that the system architect may use to identify the conditions that lead to a failure mode. These operational risks are identified in the Threat Vector, documented in the Impact Matrix and utilized in the Mitigation Costs Matrix.

F. Develop an operational risk profile of the mission.

Goal: To develop a comprehensive view that accurately reflects how operational risk can affect the mission.

Description: Developing an operational risk profile for the mission requires three additional analysis activities. First, risks are linked in a prescribed manner, producing an aggregate view of the operational risk to the mission. In essence, a single causal chain of risk factors affecting the mission is developed. Second, the value of operational risk exposure for the mission is determined using the defined risk evaluation criteria and all relevant data collected throughout the analysis. Finally, a critical path analysis of the risk causal chain is performed to identify which factors are driving the operational risk exposure to the mission. Overall, an operational risk profile must

- track inherited and imposed risk
- effectively characterize risk arising from the interrelationships and dependencies among threats and controls
- account for the operational risk arising from the emergent properties of distributed processes
- estimate the mission's operational risk exposure

Rationale: Before substantial mitigation activities can be initiated to improve the mission assurance of a process, it is essential to develop an operational risk profile of the mission. The profile forms the basis for all operational risk management activities that follow.

Outcome: A operational risk profile of the mission.

CSES Crosswalk: CSES addresses multiple missions from multiple stakeholders simultaneously and tracks inherited and imposed risks. Additionally, CSES identifies how those risks change (e.g., in relation to implemented mitigation strategies) over time as the various Matrices are updated. The outcome is a dynamic operational risk profile of multiple missions.

G. Ensure that operational risk is within tolerance.

Goal: To develop a mitigation plan for ensuring that operational risk is within tolerance

Description: The value of operational risk exposure for the mission has been established. Now, management must decide whether that value is acceptable. A tradeoff analysis is performed to weigh the relative costs associated with various mitigation options against the potential for reducing the aggregate operational risk. The operational risk profile provides a basis for the tradeoff analysis, where residual risk is

examined under several mitigation scenarios. The best available option is selected based on the relative costs and benefits of each scenario. The value of residual risk projected for the chosen option defines management's tolerance for operational risk.

Rationale: Organizational constraints always limit the amount of mitigation resources that can be applied in any given situation. Weighing the relative costs and benefits associated with mitigation options is essential for ensuring that risk is brought within acceptable limits and maintained at that level over time, giving management reasonable confidence in mission success.

Outcome: A documented mitigation plan.

CSES Crosswalk: CSES can produce not only can produce a documented mitigation plan, it can be updated dynamically. Operational risk profile documented in the stakeholders, dependency impact and mitigation costs matrices provide a basis for the dynamic tradeoff analysis, where residual risk is identified and examined under several mitigation scenarios.

VI. CONCLUSIONS:

We have discussed the CSES infrastructure with respect to how it may be leveraged within the subject domain of mission assurance (i.e., as a full life-cycle engineering process to identify and mitigate design, production, test, and field support deficiencies of mission success). We further cross-referenced the underlying quantitative concepts of the Cyberspace Security Econometrics System (CSES) to the Mission Assurance Analysis Protocol (MAAP) tenets. Further work is necessary in this subject domain. We must explore how mean failure costs can concretely be applied to the tangible elements of mission assurance (as described) and investigate other mission assurance indicators/quantifiers to broaden the scope of our analysis to include other studies beyond CSES.

Note, that a study was conducted of anti-virus comparatives (www.av-comparatives.org) to evaluate how well CSES tracks the effectiveness of such countermeasures in terms of the return on investment. The results are discussed in [3] and should be considered in light of the CSES/MAAP crosswalk.

VII. 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, the Department of Energy, or the U.S. Government.

REFERENCES

[1] F. T. Sheldon, R. K. Abercrombie, and A. Mili, "Methodology for Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission," presented at the Proceedings of 42nd Annual Hawaii International Conference on System Sciences (HICSS-42), Waikoloa, HI, 2009.

[2] R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Synopsis of Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission Value," presented at the 11th IEEE High Assurance Systems Engineering Symposium (HASE '08), Nanjing, China, 2008.

[3] A. Ben-Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, " Quantifying Security Threats and Their Potential Impacts: A Case Study," *Innovations in Systems and Software Engineering, A NASA Journal,* in press.

[4] R. Hefner, H. Silva, and R. Patrican, "Mission Assurance and Capability Maturity Model Integration (CMMI)," presented at the CMMI Technology Conference & User Group Meeting, 2004.

[5] "Cyberspace Policy RevIew - Assuring a Trusted and Resilient Information and Communications Infrastructure," ed: The White House, 2009, p. 76.

[6] K. Rhodes. (2010, January 15). *Cybersecurity must start with mission assurance*. Available: http://washingtontechnology.com/Articles/2010/01/13/Predict-globally-protect-locally.aspx?s=wtdaily_190110&Page=1

[7] M. R. Grimaila, R. F. Mills, and L. W. Fortson, "Improving the Cyber Incident Mission Impact Assessment (CIMIA) Process," presented at the Proceedings of the 4th Annual Cyber Security and Information Intelligence Research Workshop, Oak Ridge, TN, 2008.

[8] H. Yates and M. R. Grimaila, "A Systematic Approach to Securing our Space Assets," *High Frontier Journal,* vol. 4, pp. 48-53, 2008.

[9] M. R. Grimaila, L. W. Fortson, and J. L. Sutton, "Design Considerations for a Cyber Incident Mission Impact Assessment (CIMIA) Process," in *Proceedings of 2009 International Conference on Security and Management (SAM09)*, Las Vegas, NV, 2009, pp. 386-391.

[10] D. L. Pipkin, *Information Security Protecting the Global Enterprise*: Hewlett-Packard Company, 2000.

[11] C. Kelly. (2004, March 8). *Mission Assurance - Gov't Needs To Manage Risk Differently in Face of New Operating Realities*. Available: http://www.boozallen.com/consulting-services/services_article/659316

[12] "Department of Defense INSTRUCTION NUMBER 8500.2 Information Assurance (IA) Implementation," ASD(C3I), Ed., U.S. DoD ed, 2003.

[13] B. Hale, M. R. Grimaila, R. F. Mills, M. Haas, and P. Maynard, "Communicating Potential Mission Impact Using Shared Mission Representations," in *Proceedings of the 5th International Conference on Information Warfare and Security (ICIW 2010)*, Wright-Patterson Air Force Base, Ohio, USA, 2010, pp. 120-127.

[14] A. Mili and F. T. Sheldon, "Challenging the Mean Time to Failure: Measuring Dependability as a Mean Failure Cost," presented at the Proceedings of 42nd Hawaii International Conference on System Sciences (HICSS-42), Waikoloa, HI, 2009.

[15] R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Managing Complex IT Security Process with Valued Based Measures," presented at the 2009 IEEE Symposium on Computational Intelligence in Cyber Security (CICS 2009), Nashville, TN, 2009.

[16] C. J. Alberts and A. J. Dorofee, "Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments," Carnegie Mellon University, Pittsburgh, PA CMU/SEI-2005-TN-032, 2005.