Developing the Next Generation of Cyber Leaders

Dr. Erich Devendorf[α], *Serco, Inc.*, Dr. Sarah Muccio[β], *United States Air Force Research Laboratory* and Col Fred Wieners, Ret.[γ], *Serco, Inc.*

Abstract – Our current computer and electrical engineering practices are insufficient to assure transactions through cyberspace. The critical flaw in these practices is mistaking reliability for security at the system design level. In this paper, we explicitly differentiate between reliability and security. We identify three pillars needed for an emerging cadre of cyber engineers, which include open-ended problem solving, cyber leadership and technical communication. We discuss a portion of the curriculum used for a cyber engineering semester at Syracuse University. Moreover, we map this curriculum to established Accreditation Board for Engineering and Technology desired student outcomes to establish the foundation for an emerging degree program in cyber engineering.

Index Terms – Cyber Engineering, Security, Cyber Leader

I. INTRODUCTION

In the last decade, technological advances coupled with the availability of internet services have transformed cyberspace into a pervasive domain that connects users across traditionally impassible spatial, temporal and organizational boundaries. Cyberspace provides users with unprecedented, on demand access to information resources and has increased productivity, simplified communication, and facilitated the exchange of ideas and data.

In the near future, it is likely that cyberspace will continue to penetrate and permeate all aspects of our lives. The definition of cyberspace we consider in this paper is consistent with this belief and we characterize cyberspace as *"…a global domain within the information environment consisting of the interdependent network information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers,*" [1]. Our conception of cyberspace is intentionally broad and recognizes the intrinsic interconnectedness of the cyber domain.

The United Stated Department of Defense (DoD) recently highlighted the pervasive nature of cyberspace and recognized its critical importance to the civilian and military world by officially adding it to land, sea, air, and space, as a foundational war-fighting domain [2]. The DoD further emphasized the importance of cyberspace by standing up U.S. Cyber Command in 2009 [3].

Cyberspace has empowered both civilian and military organizations to operate with increased situational awareness, flexibility and command and control. However, these enhanced capabilities have come with a cost and cyberspace is a distinct, vulnerable center of gravity for civilian and military organizations [4].

The risk associated with these vulnerabilities is so severe that Dmitri Alperovitch, the V.P. of Threat Research with McAffee, noted *"…I am convinced that every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised (or will be shortly),"* [5]. Although difficult to quantify, 2010 estimates by McAfee attribute losses of up to a trillion dollars to these breaches [6].

The cost of security breaches have prompted a number of efforts aimed at eliminating security vulnerabilities. Many of these focus on training users in information assurance and consider them to be on the front line of cyber defense [7]. Initiating corrective action focused on users inherently blames them for these breaches. A less palpable reality is that current computer science and engineering practices encourage the creation reliable systems that fail catastrophically at first contact with a contested environment [8].

[α] *Research Engineer with Serco, Inc., Rome, NY 13440, erich.devendorf@serco-na.com*
[β] *Mathematician with the United States Air Force Research Laboratory Information Directorate, Rome, NY 13440, sarah.muccio@rl.af.mil*
[γ] *Consultant with Serco, Inc., Rome, NY 13440, fred.wieners@serco-na.com*

Distribution statement A - Approved for public release - Distribution Unlimited Document #88ABW-2012-1813, dated 29 MAR 2012

We believe that transactions conducted through cyberspace cannot be secure when enabled by flawed architectures and systems. Unfortunately, the expertise required to design these fundamentally sound systems is lacking in both our educational system and the cyber work force [9].

In this paper, we address deficiencies in cyber education through a Cyber Engineering Seminar. The Cyber Engineering Seminar is a three-credit course that fits within the greater context of an 18 credit Cyber Engineering Semester conducted at Syracuse University in the fall 2011 semester [10]. This semester forms the pedagogical foundation for a four-year program in Cyber Engineering.

The Cyber Engineering Seminar emphasizes the professional development required to provide students with the core competencies needed to enact transformational changes across the cyberspace domain. We identify three core competencies necessary for emerging cyber professionals. These competencies include open-ended problem solving, cyber leadership and technical communication.

Before studying how to integrate these core competencies into a cyber engineering course, we first identify a set of educational outcomes that support their development in Section III. Using these outcomes as a guide, we discuss the details of our implementation in Section IV. First, however, we scope our cyber engineering paradigm within the greater context of cyber security education in Section II.

II. Cyber Engineering

Similar to the emergence of aeronautic engineering from the mechanical engineering discipline, we consider cyber engineering to be the natural evolution of the computer engineering curriculum [9]. In this section, we distinguish between computer and cyber engineering. In Section A we differentiate between reliability and security to form a basis for cyber engineering. We then identify and discuss the fundamental skills necessary for effective cyber engineers in Section B. Finally, in Section C we discuss the cyber engineering experiences that form the basis for our proposed implementation.

A. Reliability vs. Security

In contrast to computer engineering education, cyber engineering intrinsically distinguishes between the reliability and security properties of a system. We define reliability as a measure of a system completing its expected function during an interval of time [11]. This reliability definition is consistent with ISO 9000 guidelines [12].

Reliability is a desirable property for cyber systems and reliable system design is an important and ongoing research area [13, 14]. Reliability deals directly with availability, but does nothing to assure system confidentiality or integrity [15].

In contrast with reliability, we define security as a measure of a system completing exclusively its intended function during an interval of time. We establish our definition of security on the assumption that vulnerabilities occur when designers incorporate unintended functions into cyber systems. Although conceptually different, the written definition for security is not structurally distinct from reliability. We more succinctly differentiate between reliability and security in Figure 1.

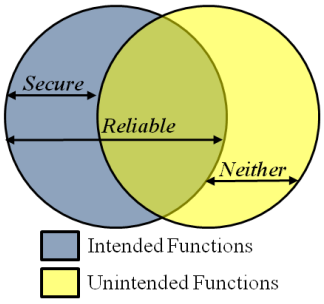

Figure 1: Security-Reliability Venn Diagram

In Figure 1 the set of intended and unintended functions are collectively exhaustive. Inspection of Figure 1 demonstrates that secure components are a subset of reliable components. Reliability is, therefore, a necessary condition for security. Reliability is not, however, a sufficient condition to prove a component is secure. Developing the necessary mathematical rules to define security is an ongoing area of current research [8].

From the differences between security and reliability in Figure 1, it is apparent that even at the component level we cannot use the same approaches to realize highly reliable and highly secure systems. Aggregating components into subsystems creates additional challenges to guarantee security. Where component reliability can be independently aggregated to evaluate system reliability, security properties change when components are coupled in a larger system.

From a pedagogical standpoint, the primary tools for reliability analysis are probability, statistics and empirical methods. Unfortunately, complete

empirical validation for security analysis is impractical and cannot provide security guarantees. Instead, security requires a mathematically rigorous approach to formal system specification, validation and verification that leverages a proven scientific foundation [16]. In the following section, we identify the fundamental skills necessary for future cyber engineers to transform cyberspace into a domain with inherent security.

B. Cyber Engineering Fundamentals

To elicit transformative change, emerging cyber engineers must be technically competent leaders with strong communication skills. We elaborate on the specific manifestation of these skills in this section.

Our conception of technically competent cyber engineers for cyber engineering is based on the realization that cyberspace is a synthetic domain. The laws governing its behavior are entirely encapsulated in the underlying mathematics defining its operation. A technically competent cyber engineer must be grounded in these underlying fundamentals, which include discrete mathematics, structural operational semantics and information theory [17]. Moreover, they must be able to formally prove and verify the security properties of their implementation. We describe our open-ended problem solving educational approach to develop the fundamental mathematical skills required to design for security in Section IV Part A.

In conjunction with technical competence, cyber engineers must be educated to be effective cyber leaders. We conceive cyber leaders as being courageous and competent technical communicators who deliver on time results. To nurture these traits in cyber engineers, we incorporate leadership education into our curriculum. This program focuses on studying historical case studies that demonstrate interdisciplinary leadership principles and techniques. We present the leadership portion of our curriculum in Section IV part B.

Critical to successful professional and technical leadership is the ability to communicate effectively. The emerging generation of cyber engineers will be introducing ideas, concepts, tools and techniques that are foreign to the current reliability focused cyber community. To break through organizational barriers and academic inertia, cyber engineers must be able to state succinctly the case for security minded design practices and must be leaders. We describe our approach to developing verbal and written communication skills in Section IV Part C.

C. Experience developing Cyber Leaders

History often recognizes great leaders during moments of extreme duress. However, these leaders develop the skills and instincts that they rely heavily on over the course of a lifetime leading up to the defining event. To prepare our future cyber leaders we have created and delivered a variety of education to meet the growing national need. For eight years, AFRL successfully delivered the Advanced Course in Engineering Cyber Security Boot Camp (ACE) to classes of civilian, Scholarship for Service (SFS), Air Force Reserve Officers Training Corps (ROTC), Army ROTC and Navy ROTC cadets during the summer. The course met for ten weeks each summer from Memorial Day until the beginning of August from 2003-2010. ACE sought to produce the next-generation cyber security leaders from the top cadets at US colleges and universities, targeting the best in computer engineering, electrical engineering, computer science, mathematics and physics. ACE developed the cadets into problem solvers, original thinkers and technical leaders.

ACE achieved its stated objectives through focused instruction with a strong emphasis on problem solving. The ACE faculty employed real-world problems to teach the cadets to formulate clear problem statements, make reasonable assumptions, apply engineering tools and techniques, formulate solutions to the problem, apply risk analysis to the solutions and deliver those solutions on time. In addition to solving problems and delivering solutions on time, cadets learned to communicate through written reports and oral presentations.

The ACE partnership included SERCO, ITT Corporation and the Information Directorate at the Air Force Research Laboratory (AFRL). ACE recruited faculty from cyber security experts working in academia, government and industry, who provided the cadets with an expansive spectrum of cyber security experiences.

In addition to teaching a broad curriculum on cyber security, ACE placed the cadets with internship mentors from AFRL and local government industry where they contributed their newfound knowledge to ongoing research and development projects. A 10-week mini-hackfest curriculum and a capstone Hackfest provided the forum for the cadets to put into practice the educational concepts learned in the course, to test state-of-the-art tools and to gather data for use in ongoing activities.

The Air Force Research Laboratory sought to promote growth in the cyber research field, increase

emphasis on in-house research, and attract, employ, and retain highly qualified scientists and engineers [18, 19]. In response to those aims, the AFRL Information Directorate (AFRL/RI) implemented the Information Assurance Internship (IAI) program to identify and recruit the best and brightest science and engineering students from around the nation. Acceptance criteria dictated the students must maintain high academic standards (average GPA > 3.7), exemplify outstanding leadership potential through extracurricular activities, demonstrate an ability to solve problems, and qualify for interim secret clearance as US citizens.

The IAI 2011 focused on the science of mission assurance in cloud computing environment, with emphasis on assuring Air Force mission essential functions in a contested environment

In addition to solving this larger problem, the IAI 2011 also looked to the initiatives laid out in the July 2011, the Department of Defense Strategy for Operating in Cyberspace (DoDSOC). This document described the dependence of the Department of Defense and the nation on cyberspace and expressed the hazards posed by this dependence. DoDSOC requested development of "*…new defensive operative concepts,"* [20]. The IAI fulfilled this initiative by evaluating older concepts such as network defense as well as researching new concepts such as mission assurance and information assurance.

To support the goal of assuring missions through the cloud, the internship developed a strategy to develop the interns and immerse them in every aspect of their objective. First, facilitated weekly discussions in mathematics and information assurance provided the interns an academic understanding of the problem. Second, the staff introduced weekly research challenges related to the overall research objective. Team reports and oral presentations of the weekly solution provided interns with advanced problem solving and communication skills. In addition, case studies familiarized the interns with engineering and military concepts. Lastly, trips to operational military units provided the interns an opportunity to interact with operators and gain a real-world perspective of their research.

The benefits of the IAI go beyond its contributions to the fields of information and mission assurance. For instance, the Air Force benefits from the strengthened relationship developed with top universities and colleges. This institutional tie allows the recruitment of the highly qualified individuals required to solve the technical challenges facing the country. In addition, the interns provide AFRL with fresh perspectives for in-house research efforts.

III. EDUCATIONAL OUTCOMES

After considering our prior experience in the development of cyber leaders, we composed several education outcomes based on Bloom's Taxonomy that we expected to achieve during the Cyber Engineering Semester. These served to focus our curriculum development, lectures and hands-on exercises. We list a sample of these course outcomes below:

1. Comprehension
Translate between various formal representations for design and analysis, (e.g., translate instruction set architecture to data path and control path) and interpret the meaning of the various formal representations.

2. Application
Restate the descriptions, concepts of operations and policies in higher order logic (HOL) of a given access-control description, concept of operations, or policy.

3. Analysis
Reason about trust in complex cyber systems using tools such as access control logic

4. Synthesis
Synthesize technical solutions to realistic problems with resource constraints

5. Evaluation
Real-time critical assessment of proposed solutions

IV. COURSE CONTENT

In this section, we present the curriculum developed as part of a cyber engineering semester. This includes the content from a 3 credit hour course at Syracuse University, CSE 400 - Cyber Engineering Seminar, and a once a week internship with the Air Force Research Laboratory in Rome, NY. We present each of the three critical skills discussed in Section II part B as part of this curriculum.

A. OPEN ENDED PROBLEM SOLVING

We recognize the primary responsibility of engineers is to analyze and design systems and processes using science and mathematics. The Accreditation Board for Engineering and Technology (ABET) required Outcome c reinforces that engineering graduates must have *"an ability to devise a system, component or process to meet desired needs within realistic*

constraints," [21]. In this section, we describe three projects that support Outcome c using open-ended analysis and design challenges. In support of ABET required Outcome e, these projects task students to "*identify, formulate, and solve engineering problems,"* [21]. We scope all three projects in the context of formal methods using access control logic as described by Chin and Older [22]. Students manually proved security properties in the first project and by the final project are required to generate machine verifiable proofs. We discuss the formal methods results for these projects in [10]. In this paper, we discuss the overall problem structure and demonstrate how our curriculum supports achievement of ABET required outcomes.

1. Modeling Real Systems

The compromise of the Sony PlayStation Network (PSN) was one of the most well publicized and significant security breaches of 2011 [23]. To engage students with a study of current cyber events and support ABET Outcome j to develop "*a knowledge of contemporary issues,"* [21] we tasked the students to develop an access control model for the PSN and to use it to identify the root of trust for user authentication and transactions. The problem statement provided to students is:

> *The PlayStation Network is under attack, again. Is it that hard to believe? Due to the nature of the attacks on the PlayStation Network, a model to rigorously account for the trust assumptions that underpin the PlayStation Network design is necessary. Develop an adequate model that captures the primary capabilities of the PlayStation Network.*

The problem statement provided to students is deliberately open-ended. We challenged students to define the scope of their solution and to determine an appropriate level of granularity for their models. To assist the students we provided them with a set of prompt questions to guide them in developing their model.

1. *What are the capabilities of the PlayStation Network?*
2. *Which of these capabilities need to be modeled?*
3. *How do users access the PlayStation Network (computer account, console)?*
4. *What kind of verification do users provide to access the network?*
5. *What authorities certify the trustworthiness of entities in the network?*

Student solutions to this problem varied widely based on their educational and experiential background. Although they all applied access control logic, some emphasized implementation level vulnerabilities while others considered the larger trust considerations and system architecture. The second project guided students to focus on the prescribed system architecture.

2. Modeling an RFC

For this assignment, we presented students with the challenge to model RFC-1421 [24] using access control logic and formal methods. RFC-1421 introduces the students to the RFC process and provides a framework to discuss the development of networking standards.

RFC-1421 also introduces students to symmetric/asymmetric encryption and hashing in an implementation independent specification. Further, the Network Working group deprecated RFC-1421 and there are not implementations readily available for students to study. This requires students to interpret the RFC themselves and scour the entire document for the information they need to develop their models.

3. Modeling Theoretical Systems

With the experience students gained modeling two well-defined systems, students were equipped to consider challenges that are more open-ended. We introduced the students to two protocols that previous student interns created to secure communication and control in the cloud.

These protocols possess known flaws and are generally incomplete. Students used access control logic to model the system and identify the flaws from a formal design perspective. We also challenged the students to recommend remediation to address the flaws discovered. The remediation proposed by students demonstrated a strong understanding of the underlying principles governing the trust assumptions and access control policies underlying the protocols. In some cases, students recognized the need to standardize file formats, and procedures and in others recognized vulnerabilities that could compromise the communication protocol.

B. Cyber Leadership

One of the desired outcomes of the Syracuse University Cyber Semester program is to develop highly competent, credible and confident leaders who can make critical decisions during periods of uncertainty in a timely manner to ensure mission success and avoid catastrophic failure. This outcome

aligns with required Outcome f to develop *"…an understanding of professional and ethical responsibility,"* [21].

Given the academic competency and demonstrated work ethic of these students, they will likely find themselves in leadership roles supporting critical technical, operational and policy decisions in the near future. Our intent is to motivate and prepare these future civilian and military engineers to engage in a myriad of leadership roles and responsibilities that demand a high degree of decision making confidence and competence [25].

We use case studies relevant to future decisions in the cyber domain to demonstrate the important models, theories and research dealing with leadership and critical decision making at the individual, group and organizational levels. Students are required to analyze and critique various leadership styles and decision processes in each case and determine what lessons they should learn. This course uses a framework throughout all the case studies for the students to:

- Identify common problems and cognitive biases inherent in decisions,
- Determine when taking the initiative is appropriate,
- Analyze the importance of clear communications and the need to 'speak-up',
- Appreciate why a leader's example is critical in implementing decisions.

We summarize the desired learning objectives in seven case studies.

1. Revolutions in Military Affairs

We presented several examples of 20th century technological changes to give an overall understanding of how to shape a revolution in military affairs (RMA). Students analyze each example to identify patterns and conditions in successful RMAs as well as to understand the causes of military failures and the dislocating impact of surprise. We emphasize important transformational leadership lessons relating to changing an organizational culture [26].

2. Gettysburg - A Study in Command

This unique case study takes place during a 'leadership staff ride' to the Gettysburg National Military Park. This practical experience enhances the students' understanding of the nature of war, military strategy and operational art, course of action development, decision making, command styles and leadership principles as well as human behavior in combat [27]. The students analyze the impact of cognitive biases and erroneous assumptions and the importance of the appropriate use of decisive initiative will become readily apparent.

3. Cuban Missile Crisis - Thirteen Days

Students analyze this Cold War era nuclear crisis using Graham Allison's 'rational, organizational and political actor' decision models [28]. In addition, they determine how leaders can constructively stimulate conflict and debate to avoid problems associated with 'group think.'

4. Apollo 13 - A Successful Failure

We stress analysis of individual and group problem solving along with the requisite leadership principles and character virtues required in crisis decision making throughout this study. Students evaluate various conflict resolution techniques vital in any time and resource constrained situation. We use NASA's Mission Control model for 'professional excellence' to identify those factors that enhance trust and confidence and earn loyalty and respect [29].

5. Challenger and Columbia Shuttle Disasters - A Flawed Culture

Students learn how and why 'decision failures' happen in complex and high risk organizations. The concept of 'normalizing deviance' is highlighted in both disasters, and students are asked to identify and explain how NASA's cultural and structural flaws contributed to these disasters [30]. Lastly, given the benefits of their retrospective analysis, students are required to recommend different courses of action and leadership styles for the individual engineers and key managers that could have averted these tragedies.

6. Black Hawk Shoot Down - Friendly Fire

The 1994 shoot down of two U. S. helicopters by friendly fighters over Iraq identifies flawed decisions at the individual, group and organizational levels. Students appreciate the importance of adhering to published procedures. We challenge students to recognize opportunities to make appropriate changes to these procedures. Students also analyze how expectations shape cognition and how status shapes behavior [31]. Lastly, students identify ways to prevent diffusion of responsibility, which contributes to inaction.

7. 9 / 11 - Failure of Imagination - Inability to Connect the Dots

Students appreciate the nature of ambiguous threats and why surprise occurs. Again, we emphasize determining how individuals can change entrenched organizational views and mindsets and help foster collaborative decision making [32]. Students hear first-hand from military officers involved with many of the decisions made on that fateful day.

We recognize that emerging cyber engineers will be responsible for changing a complacent culture in their organizations. In addition to open ended problem solving and leadership skills, emerging cyber engineers must be able to communicate effectively to engage in transformative organizational changes. We discuss our approach to developing student technical communication skills in the next section.

C. TECHNICAL COMMUNICATION

A truly effective cyber leader must have technical competence and develop leadership skills. However, the inability to communicate the technical challenges, solutions and impacts to a variety of audiences degrades the effectiveness of a leader. Technical communication skills build the foundation of successful leadership. ABET recognizes this in Outcome g "*an ability to communicate effectively*," [21].

During the Cyber Engineering Semester, all courses and instructors emphasized the importance of strong technical communication skills. Oral presentations as well as written reports provided mean of practicing these skills.

Each course requires written solutions. The format for these includes laboratory notebooks, descriptive documentation and formal reports. The instructors placed emphasis on providing an appropriate amount of detail and explanation on a technical topic without losing the audience.

The writing style emphasized sought to achieve clarity of communication through brevity and simplicity. For example, in the seminar course assignments included providing executive summaries. The executive summary must stand alone as a self-contained document. A concise summary of the problem, bounding assumptions and solution provide a one-page review. Often times in industry, academia and government settings entities must make decisions quickly. The ability to communicate all pertinent points in a single page provides an increased advantage for future dealings with higher management, proposal review committees and senior officers.

Presentations required students to plan and practice ahead of time. Classroom demonstrations on professional presentation skills afforded students the opportunity to see polished presentations. Additionally students practiced briefing with questions and answer session. They received feedback on their oral presentation skills, including time management. Additionally instructors addressed the importance of solid slide creation, posters presentation and whiteboard skills. Students completed the semester by presenting a final project to an audience consisting of military officers, industry professionals, academics and government civilians. This large varied audience witnessed the effective communication skills presenting solutions to challenging problems.

V. CONCLUSION

The Cyber Engineering Semester presented opportunities for students to learn, practice and develop the skills required as cyber leaders. We identified three foundational pillars needed for the emerging cadre of cyber engineers. During the semester, the courses emphasized these necessary skills, which include open ended problem solving, cyber leadership and technical communication. The next generation of cyber leaders will face the challenge of designing systems with security, not just reliability at the forefront of the architecture. The educational foundation and skills acquired during this curriculum provides the starting point to accomplish this mission. We developed this curriculum to address the national need for cyber leaders. This 18 credit semester leads the way for developing a full four year curriculum in Cyber Engineering.

VI. ACKNOWLEDGEMENTS

This research was supported by the U.S. Air Force Research Laboratory/Information Directorate. All opinions expressed in this paper are the authors and do not reflect the official policy or position of the Air Force Research Laboratory, the United States Air Force, Department of Defense, or the United States Government.

VII. REFERENCES

[1] Director for Operational Plans, 2009, *Joint Publication 1, Doctrine for the Armed Forces of the United States*, Department of Defense, Washington, D.C.

[2] U.S. Joint Chiefs of Staff, 2006, National Military Strategy for Cyberspace Operations, Department of Defense, Washington, D.C.
[3] Sanger, D. E., Markoff, J., and Shanker, T., 2009, "U.S. Plans Attack and Defense in Web Warfare," *The New York Times*, 28 April, pp. A1, NY, NY.
[4] Rattray, G. J., 2001, *Strategic Warfare in Cybersapce*, The MIT Press, United States of America.
[5] Alperovitch, D., 2011, *Revealed: Operation Shady Rat*, McAfee.
[6] Arora A, et al., (2011), *Unsecured Economies: Protecting Vital Information*, McAfee, Santa Clara, CA.
[7] Chilton, G.K.P., 2009, "*Cyberspace Leadership: Towards New Culture, Conduct and Capabilities*," *Air and Space Power Journal*, 22(3), pp. 5-10.
[8] Jabbour, K., and Muccio, S., 2011, "The Science of Mission Assurance," *Journal of Strategic Security*, 4(2), pp. 61-74.
[9] Jabbour, K., 2010, "The Time Has Come for the Bachelor of Science in Cyber Engineering," *High Frontier*, 6(4), pp. 20 - 23.
[10] Chin, S.-K., Devendorf, E., Muccio, S., Older, S., and Royer, J., 2012, Formal Verification for Mission Assurance in Cyberspace: Education, Tools and Results," *Colloquium for Information Systems and Security Education*, Lake Buena Vista, FL, (Under Review).
[11] Rausand, M., and Hoyland, A., 2004, "System Reliability Theory: Models, Statistical Methods and Applications," *Wiley Series in Probability and Statistics*, John Wiley & Sons, Hoboken, NJ.
[12] International Organization for Standardization, 2005, "Quality Management Systems," *Fundamentals and Vocabulary*, Standard: 9000:2005.
[13] Bouroche, M., Hughes, B., and Cahill, V., 2006, "Building Reliable Mobile Applications with Space-Elastic Adaptation," Sympsoium on the World of Wireless, Mobile and Multimedia Networks, Niagara Falls, NY.
[14] Gokhale, A., Mcdonald, M., Drager, S., and Mckeever, W., 2010, "A Cyber Physical Systems Perspective on the Real-Time and Reliable Dissemination of Information in Intelligent Transportation Systems," *Network Protocols and Algorithms*, 2(3), pp. 116-236.
[15] National Institute for Standards and Technology, 2004, *Standards for Security Categorization of Federal Information and Information Systems*, Computer Security Division, Gaithersburg, MD.
[16] Jabbour, K., 2010, "Cyber Vision and Cyber Force Development," *Strategic Studies Quarterly*, 4(1), pp. 63 - 73.
[17] Irvine, C. E., Chin, S.-K., and Frincke, D., 1998, "Integrating Security into the Curriculum," *IEE Computer*, 31(12), pp. 25-30.
[18] Air Force Research Laboratory, 2010, *Scientific Advisory Board's FY10 S&T Quality Report*, Department of Defense.
[19] Air Force Research Laboratory, 2010, AFRL Science and Technology Strategy, Department of Defense.
[20] Department of Defense, 2011, DoD Strategy for Operating in Cyberspace, Washington, D.C.
[21] Engineering Accredidation Comission, 2011, *Criteria for Accrediting Engineering Programs*, Accredidation Board for Engineering and Technology, Baltimore, MD.
[22] Chin, S.-K., Older, S., 2010, "Access Control, Security, and Trust: A Logical Approach," *Crc Cryptography and Network Security Series*, Chapman & Hall, Washington D.C., New York, London, Boca Raton.
[23] Tabuchi, H., 2011, "Sony Struggling with Online Attack and a TV Defect," 13 October, pp. A3, New York Times, New York.
[24] Linn, J., 1993, "Part I: Message Encryption and Authenticaion Procedures," *Privacy Enhancement for Internet Electronic Mail*, Network Working Group, RFC-1421.
[25] Roberto, M. A., 2009, *The Art of Critical Decision Making*, *Course Guidebook*, The Teaching Company, Chantilly, VA.
[26] Mandeles, M. D., 2007, *Military Transformation, Past and Present*, Praeger Security International, Westport CT.
[27] Spruill, M., 2011, *Decisions at Gettysburg*, University of Tennessee Press, Knoxville TN.
[28] Allison, G. T., 1971, *Essence of Decision, Explaining the Cuban Missile Crisis*, HarperCollins, New York, NY.
[29] Kranz, G., 2000, *Failure Is Not an Option*, Berkley Publishing Group, New York, NY.
[30] Perrow, C., 1999, *Normal Accidents, Living with High-Risk Technologies*, Princeton University Press, Princeton, NJ.
[31] Snook, S. A., 2000, *Friendly Fire: The Accidental Shootdown of U. S. Black Hawks over Northern Iraq*, Princeton University Press, Princeton, NJ.
[32] The National Comission on Terrorist Activities Upon the United States, 2004, *The 9/11 Commission Report*, W.W. Norton & Company, New York, NY.