Cyber-Security, IAS and the Cyber Warrior

Dale C. Rowe, J. J. Ekstrom, Barry Lunt, *Utah, Brigham Young University*

In 2008, the director of the CIA Clandestine Information Technology office concluded that the US is short of 20,000 to 30,000 skilled cyber security specialists. At that time, there were to most reckonings only 1,000 experts. Yet there remains a relatively vague definition of what constitutes a skilled cyber security specialist and what skills such an individual should possess. In this paper we discuss what constitutes a cyber-specialist and how this differs from the typical view of Information Assurance and Security. We also note the connections between the cyber and physical domains. In conclusion we recommend key knowledge points and skills that we believe are key in securing, defending and protecting cyberspace.

Keywords: Cyber Security, Cyberspace, Cyber warrior, Cyber warfare, Information Assurance and Security, Education.

I. Introduction

Sun Tsu taught that one should both know their enemy and oneself to have the best chance to succeed in battle [1]. A master of tactics, he understood clearly the value of information and its critical role in combat. He was neither the first nor last to teach this principle, but did so in a particularly eloquent manner. Likewise in the modern world, the value of information has not diminished. Many computing professionals also understand how this value may vary depending on the properties.

Information Assurance and Security (IAS) has been taught in computing subjects for decades. Industry, academia and government have spent perhaps thousands of man-years developing methodologies, frameworks and definitions that help ensure information is protected, and properly cared for. Yet in the past few years, there has been a notable increase in the call for cyber-security specialists. While true that in many ways, the term cyber-security is a rebranding of the more technical IAS term [2], it is not synonymous with IAS. This rebranding is necessary to address the subtle differences that exist between these two terms and calls for a specialist with additional expertise.

To better explain this, it is first necessary to identify some terminology and background. Information technology, as a profession and academic discipline, emphasizes the interactions between users and computers. A system, to an IT professional, is often thought of as a combination of computers, networks and users. Systems of this fashion should increase efficiency in helping to realize one or more goals or objectives. For example, a customer relations management (CRM) system should help an organization better support and manage their customers to achieve more effectively their corporate goals and objectives, such as increased sales. The CRM system itself is composed of the software, hardware, interconnections between nodes and users. As none of these by itself is of any real benefit, they operate in a synergistic fashion.

With this definition of systems, we note that the systems themselves become valuable assets. The correct operation and functioning of a system within its defined parameters is reliant on not just each component performing its role, but the interactions between these roles behaving in a known and predictable fashion.

Although in many instances it is true that systems are built to transmit, store and process information, they are no longer exclusive to this task. Take for example a power station. The role of a power station is to produce electricity that can be delivered to a consumer. While information still has a function and significance, the primary task of the power station 'system' is not to transmit, store and process that information.

As IBM recently published, today's world is comprised of systems, and systems of systems [3]. This view of technology and users has allowed us to see interactions at local, regional and even global levels. So intertwined has society become with technology, that these systems for some can even become a functional definition of life.

From this it can be deduced that there has been a change or evolution in the past twenty or so years, since the Internet became commonplace. The world has moved from a clear separation between people and technology where the primary role of technology is to handle information, to a network of systems that provide critical resources to modern living. The lines between cyberspace and the physical world are now blurred to an extent that today's youth may be barely aware they even existed.

Speaking of a multi-player online virtual environment known as Habitat, Morningstar and Randall wrote that:

> "Cyberspace is defined more by the interactions among the actors within it than by the technology with which it is implemented… at the core of our vision is the idea that cyberspace is necessarily a multiple-participant environment. It seems (to us) that the things that are important to the inhabitants of such an environment are the capabilities available to them, the characteristics of the other people they encounter there, and the ways these various participants can affect one another. Beyond a foundation set of communications capabilities, the details of the technology used to present this environment to its participants, while sexy and interesting, are of relatively peripheral concern."

Although the context of their paper is different, their terminology is very appropriate. Cyber-space is the nexus that allows for the potential and very real connections among international organized crime, terrorists, hackers, foreign intelligence agencies, military and civilians. This definition can be somewhat alarming when the latter include employees, families and children.

In this context the limitations of the traditional IAS approach can be seen. IAS was designed to protect information and it does so very well. But it was never designed to cope with the increased scope brought about by systems themselves being key assets and resources, intertwined with everyday life, critical infrastructure and global systems. This distinction is what separates IAS and cyber-security.

II. Cyber-Security, Warriors and Warfare

As noted previously, in warfare, information is a key resource. One might be tempted to refer to Cyberspace exclusively as a supporting domain, used to search for and find key information that will help in battle. However one might also note that it is also a 'fighting' domain where combat can take place with no need for attacks in the physical domain. Perhaps more concerning is that actions in cyberspace can have significant repercussions in the physical world. For example in January 2000, an attack against the Maroochy Shire Council's sewage system in Queensland, Australia caused sewage to flood a park, contaminate surface water drainage and enter a tidal canal. The attacker never left the comfort of their computer terminal. In this instance, his motivation was to try and gain employment to help 'fix' the problem [4].

A more publicized cyber-attack of late is the STUXNET virus [5]. This attack was so advanced and effective it is often referred to as the first cyber-weapon. Other more recent malicious software has been found since this attack [6] and vulnerabilities in these systems are continually being exposed [7, 8] much to the embarrassment of manufacturers and designers.

The dual nature of cyberspace to both support physical action and to be actionable calls for specialists who can work within cyberspace to help secure, defend against, respond to, and in some instances, even initiate pre-emptive attacks. While the latter is typically limited to military personnel and authorized governments, the rest are not. Organizations are rapidly becoming aware of these facts and are placing increased demand on an already under-populated profession.

As the frequency of attacks increases, organizations and nations are seeing that we are in the midst of a cyber-war that is very difficult to fight. Unlike the physical world, in cyberspace there are no geographic boundaries. No barbed wire fences and border patrol agencies exist to protect critical infrastructure. The cyber-equivalent of Psy-Ops could be networks of thousands of benign computers linked together under the control of a single group or individual, which allows attackers to strike with little fear of identification or repercussions. The enemy is faceless, nameless, and hidden behind a veil of anonymity provided by the systems on which we have become so dependent.

And now as academia, government and industry come together under a single umbrella in cyberspace, a new profession of cyber specialist, or cyber warrior, is called for. These individuals must have detailed knowledge of the systems they protect, an understanding of the cyber-environment and physical environment in which they operate, and the skills to secure from, defend against and respond to attacks. In a recent presentation, the National Security Agency referred to this as 'Cyber Operations' [9].

III. The Cyber Warrior/Specialist

The cyber warrior should be a well-rounded individual in his knowledge of computing and technology. But in addition to this, they should also understand the ethical expectations and legal surroundings of their field. Cyber specialists should have a high personal code of ethics and understanding of right and wrong.

The NSA in 2011 announced a new designation for Centers of Academic Excellence in Cyber Operations. Qualifying academic requirements consist of 13 mandatory content modules (3 of which are provided during a government organized summer school) with a further 13 optional modules. These provide insight into defining the exact skills and knowledge required of cyber specialists.

The correlation between the ACM IT Model Curriculum and the NSA Cyber Operations CAE requirements are of note [10]. Indeed in mapping our own program we noted a complete mapping of the mandatory content and if including elective and graduate classes, complete coverage of all optional modules. This is in the most part due to the pervasive security content throughout an IT program [11, 12]. For example, in our IT web development class, principles of security are taught to sophomore students, and are supplemented by a core capstone security experience, and several elective courses later in the program.

Specific core content within the CAE Cyber Operations designation consists of: low level programming, reverse engineering, operating system theory, networking, telecommunications, discrete mathematics, an overview of cyber defense, security fundamental principles, vulnerabilities and legal considerations. Elective topics include: programmable logic languages, FPGA design, wireless security, virtualization, large scale distributed systems, risk management of information systems, computer architecture and logic design, microcontroller design, software analysis, software development, embedded systems, forensics and incident response, systems programming, applied cryptography, SCADA systems and HCI/usable security.

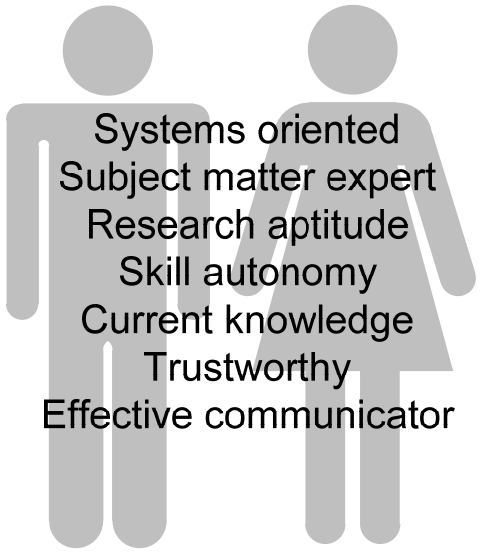

Figure 1 - Characteristics of a Cyber Warrior

These topics present comprehensive core coverage of computing at both the component and systems levels in a security context. The instruction of this in a security context is perhaps the most crucial change required throughout computing programs. Although younger than its sibling disciplines, this is one area where Information Technology has set the example for its peers. In recent recruitment seminars, national and international corporations frequently comment on how IT majors from accredited programs can fast track to become cyber security specialists. In one recent instance, a lead engineer from a major government contractor, himself a Computer Science major with a PhD, remarked how graduates were able to work autonomously in a security setting within a year as opposed to the 3-6 years for those whose education did not include a pervasive and integrated security theme.

A. Subject Matter Expertise & Skill Autonomy

In addition to an integrative and pervasive security theme, cyber security specialists require more advanced education in security topics. This may be much more varied between disciplines that should extend the CAE elective learning outcomes. The use of the term specialist, or in some instances expert, indicates a level of knowledge that distinguishes an individual from their peers. They are often referred to as subject matter experts and may make a personal goal to become the best in their field. Becoming expert in a specific area is often beyond the scope of an undergraduate degree but this should not prevent institutions offering advanced content to help students identify their area of pursuit.

The application of conceptual knowledge allows students to development usable skills [13-15]. Effective up-to-date labs where students can hone their skills in a safe and controlled environment are critical in their development. By exposure to real world problems in a controlled setting, the learner will discover not only the application of tools in a solution, but also the risks and dangers that can be involved in arriving at the solution. Cyberspace is a world where both the good guys and the bad guys share a common arsenal. Tools may be written by either party but are frequently used by both. In the instance of open-source and freeware, one should be aware that there may be a complete absence of quality control and a tool may pose more danger than the original risk it is being used to mitigate. Care should be taken in this process to ensure that a student's experience is as open as possible and not bound to a specific technology [16].

B. Research Aptitude & Current Knowledge

As Dittrich also notes, a strong research aptitude should also be part of the makeup of a cyber security specialist. However this should not be limited to helping students develop real-world experience. Rather it should be a pervasive theme across the discipline at the undergraduate level. Lateral thinking as well as keen observation can lead to the identification of new problems and derive new solutions. Researchers in cyber-security rapidly determine risk and have the ability to methodically and comprehensively conduct research to identify solutions. As many academics will note from personal experience, this is not something that can be easily taught in a classroom setting. Instead it often comes as a result of a

ISBN 1-933510-95-1/$15.00

passion or interest in a specific area. This can be problematic in classroom settings where students' undiscovered research passion might lie in different areas.

Instructors may help undergraduates nurture and develop their research interest in their early years of study by encouraging open-ended research projects or papers. Providing a problem for students to research their own solution is one approach. Other effective methods include one-to-one faculty-to-student mentoring, undergraduate or mixed research groups, graduate-to-undergraduate mentoring, and cross-discipline research projects. For each of these the time commitment from the instructor is different and not all may be possible. However we have found a mixture of the above to be extremely effective in developing students' aptitude for research. In several courses, students are given a list of topics which they can use as source ideas to generate their own individual research proposal.

Cyber warriors must continually work to keep their knowledge and skills relevant. This requires both personal motivation and commitment to undertake continual professional development. A student's awareness of this fact will often come naturally as they become more familiar with the space. The classroom and laboratory experience should reinforce this concept of continuing lifelong education to keep knowledge current.

C. Communications

The failure to communicate the radar data indicating an imminent attack on Pearl Harbor in 1941 is a catastrophic example of communications failure [17]. In this instance the precise location of the breakdown is even today the topic of some debate. The fact remains however, that the early warning data was not used to prevent an attack. The ability to effectively communicate complicated technical data to a range of audiences, and verify audience comprehension, remains a rare yet critical skill.

History is full of plenty of similar examples. One need not look far to find an instance where poor communications led to compromise. Cyber-security specialists should understand this concept and be effective communicators. They should be able to discuss in-depth the technical details of a relevant topic, and then relay key facts to managers, users and other audiences who have different levels of technical comprehension. They must be able to teach such subjects on-the-fly when required and be able to effectively present in a variety of jargons which should at a minimum include financial, managerial, project, engineering, network, and systems.

Instructors can help students learn the value of this key skill by offering examples of communications failures and successes. Students should be encouraged to present their failings not merely through reports, but through group presentations, interviews and discussions with individuals outside of their major. In one lab in the BYU IT program, students are required to present a technical topic to a non-STEM student or family member. They are then graded by means of a feedback form completed by their audience. As part of their senior capstone project they are also required to present a technical project to the programs industry advisory board (IAB). The IAB is comprised of chief executive officers, chief information (security) officers, vice presidents, consultants, entrepreneurs and senior managers. As with the lab assignment, they are graded by and receive detailed feedback from IAB members.

D. Systems Oriented

As highlighted in the first two sections of this paper, cyber warriors should think in a systems context. An experienced specialist will understand not just a system component, but the cause and effect relationships that exist around the component throughout the system. They will have the ability to methodically analyze, derive and decompose a system to each component, isolate and resolve vulnerabilities, concerns and potential issues and be able to calculate risks to adjacent components. In reverse they can step back from viewing components to see their interactions, interconnections, users and related systems as a complete system of systems while remaining in a security context.

Logically this process is analogous to the "Vee" model used in systems engineering, as shown in Figure 2.

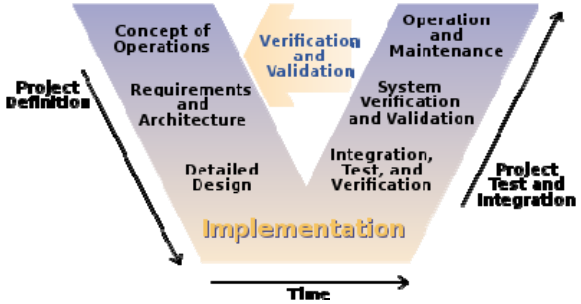

Figure 2 - Systems Engineering V Model (Wikipedia)

The idea that one must decompose for understanding and recompose and analyze for complete understanding of the system and its emergent behaviors is not often intuitive. These ideas are difficult to teach. The more effective (but not efficient) instructor is often experience, which more often than not is gained from failure. In an IT program, we have found a course on Systems Administration to be an excellent forum to teach the principles of systems thinking in a security context. Hands-on labs reinforce the studio-classroom instruction setting and are specifically designed to take a student significantly less

time if they take a systems approach as opposed to a component-level approach.

E. Trust, Ethics and Morality

An oft-quoted line from the Spiderman series is 'with great power comes great responsibility'. British Prime Minister Sir Winston Churchill also coined the phrase 'The price of greatness is responsibility'. Cyber warriors have at their disposal a potent combination of knowledge, and well-developed skills to use it. White House Press secretary Robert Gibbs implied we should not be afraid of one guy with one laptop and one keyboard. This could not be further from the truth.

Cyber warriors live in a trustworthy manner. They should be true to their word and understand the ethical complications involved in their work. Disclosure, intellectual property, honesty, personal integrity and a willingness to stand up for these are perhaps their most important attributes.

The teaching of ethics is a topic of much research and discussion. It should be discussed frequently with students. Labs can be accompanied by 'what-if' discussions to engage students in considering the ethics of various scenarios.

IV. Extending Educational Boundaries

There are several curricular and extra-curricular activities that can be of great benefit in training cyber-security specialists. Several of these can bring mutual benefits to the student and the community. All of these are offered free-of-charge, however organizations are always welcome to make a donation to the program!

A. Red Team vs. Blue Team

For some time, the final lab of both the penetration testing and information security courses has been based on a penetration test of a virtual computing infrastructure of between 10-15 servers, workstations and network devices. With the introduction of a new course on systems administration running in parallel with the penetration-testing course, students are now placed in teams against each other in a blue-team vs. red-team exercise.

Blue team students are given a 1-week long period in which they upload their lab VM's to an ESXi host, and allow them to be probed and attacked by an assigned red team. A management station verifies service uptime for each blue teams systems. At the conclusion both teams provide an oral presentation and written report in line with their roles.

Other similar activities activities have been popular for some time. Perhaps the best known is the annual national collegiate cyber defense competition. In this event students are required to defend systems against live attacks [18, 19]. These are effective tools in promoting student enthusiasm as well as skill building.

B. Real-World Red-Team

Many organizations that are not required to undertake regular PCI compliance assessments do not consider penetration tests to be part of their security activities. Others who may be required might find the cost of a test too expensive and decide to make do with an internal audit performed by the same security team who implement their security countermeasures. In both instances critical vulnerabilities can easily be missed.

The Cyber Security Research Lab (CSRL) at BYU is comprised of 8 students, two of whom are currently graduate students. These students, once mid-way through IT567 Cyber Security & Penetration Testing class, are encouraged to undertake formal penetration tests for University departments and external organizations. In each case, the assessment is performed in the same manner as a real-world test. Students and a faculty mentor meet with the customer to discuss security concerns and to establish a documented scope and the rules of engagement. These documents normally take 2-8 weeks to finalize and are signed by both parties. At the start of the test, a permission memo is signed by the team lead, faculty mentor and a client representative with authority to instruct the test to proceed.

With constant supervision, students then perform the assessment using CSRL-issued imaged laptops. The less experienced are paired with a more experienced mentor. A private wiki, IRC channel and file share are used to coordinate attempts, successful breaches, credentials and other information and are made available to the client via VPN. At the end of the test, all notes, information and other resources are transferred to the file share and the laptops are securely wiped and re-imaged. The team is then required to produce a report containing at a minimum the following sections: executive summary, detailed summary, testing performed and environment, findings, mitigation, and recommendations. Students currently enrolled in a security course may use their efforts to receive credit for a lab assignment on a related topic.

So far these exercises have proved extremely beneficial to both students and the client. The CSRL team works closely with the IT department at the University to coordinate any activities that may be noticed by the University's own security team. The team is typically successful in finding exploitable vulnerabilities. In one-

instance students successfully breached an organization's load-balanced webservers and were able to pivot further attacks into the organizations internal networks. Infiltrations at this level are shared in real time with the organization.

C. Forensics and Blue Team Activities

A recent request was made of the CSRL to provide blue-team incident response and malware analysis capabilities. This effort is currently underway, but is hoped to provide opportunities for students to gain experience handling real world attacks. The team will act as consultants and work closely with their clients to support activities.

In addition to providing skill development and experience, it is hoped that these activities will lead to productive research in reverse engineering, malware analysis and finding vulnerabilities. This will further increase the benefits to all parties involved.

D. Community Reachout

A campaign is currently underway to work with local high schools and community colleges to enhance both their security posture and student awareness. Senior students, CSRL members and graduate students may receive extra course credit for creating a learning 'pack' of slides, notes and pamphlets. (The credit is limited to one per student). These are targeted towards a specific age group and individuals of limited technical understanding and cover topics such as 'online banking security', 'choosing and remembering passwords' and 'removing malware'. While ideally a student and faculty member would visit the establishment to give a short seminar on the topic, these are also provided online at cybersecurity.byu.edu.

E. Undergraduate Research

Undergraduate students have a distinct advantage over more experienced individuals in research. Typically an undergraduate student does not know something is impossible. We have found that well-motivated undergraduate students often are themselves surprised by their productivity in various research subjects. Students initially volunteer for a probationary period, and if successful are paid as research assistants. This has also increased enrollment in the graduate program as students realize an MS emphasizing cyber-security is within their capabilities.

V. VALIDATION

The validation of these characteristics is the subject of ongoing work. Preliminary signs indicate that students exposed to these methods and completing courses that emphasize the listed characteristics command higher graduate salaries. In several instances, faculty members have been contacted by managers who have expressed surprise at the skills and knowledge of their new employees. One cyber-security expert who visited BYU to recruit cyber security specialists recently said 'If you had told me over the phone that I would be looking for IT students with a cyber security emphasis more than the traditional computer science kid, I wouldn't have believed you'. Others have expressed a belief that this curriculum can reduce the time required for a graduate to become self-sufficient in their work from 3-5 years to 1-3 years. We hope to report back with more detailed information and results as time provides this.

VI. CONCLUSION

The system-of-systems approach needed in cyber-security represents an evolutionary step on the foundation of information assurance and security. As our planet becomes more connected, there is a need for skilled individuals with unique set of attributes to deal with the growing threats to this environment. As the traditional IAS discipline is rebranded to cyber-security, there is a call for cyber-warriors, specialists in the domain of cyber security, to deal with the growing threats faced by government and organizations throughout society.

Seven key attributes that we believe are critical in these specialists are discussed and suggestions are provided for how these might be taught. These 7 attributes are: systems orientation, subject matter expertise, research aptitude, skill autonomy, current knowledge, trust, and effectiveness in communications. We also discuss several methods of methods used within our own Information Technology program that we believe are effective in placing students on a fast-track to becoming cyber-security specialists.

We invite feedback and collaboration in finding new and effective means of helping the current deficit of specialists to be countered.

VII. REFERENCES

[1] Tsu, S., *The Art of War (English Translation)*.

[2] Agresti, W. W., The Four Forces Shaping Cybersecurity, *IEEE Computer*, Vol 43, Iss. 2, pp 101-104, 2010.

[3] Korsten, P. and Seider, C., The world's 4 trillion dollar challenge: Using a system-of-systems approach to build a smarter planet. *IBM*.

[4] Abrams, M. and Weiss, J., Malicious Control System Cyber Security Attack case Study - Maroochy Water Services, Australia. *NIST*, Washington DC.

[5] Falliere, N., Murchu, L. O. and Chien, E., W32.Stuxnet Dossier. *Symantec*, February 2011.

[6] Symantec, W32.Duqu Dossier. *Symantec*, November 2011.

[7] Rosslin John Robles, M.-k. C., Eun-suk Cho, Seok-soo Kim, Gil-cheol Park, Sang-Soo Yeo, Vulnerabilities in SCADA and Critical Infrastructure Systems, *International Journal of Future Generation Communication and Networking*, Vol 1, Iss. 1, pp 99-104, 2008.

[8] Mills, E., SCADA hack talk canceled after U.S., Siemens request. *CNET*, May 18, 2011. http://news.cnet.com/8301-27080_3-20064112-245.html (Last Accessed: May 30, 2011).

[9] LaFountain, S., Cyber Operations Centers of Academic Excellence. NSA/CSS, 2011. http://csrc.nist.gov/nice/Sept2011-workshop/presentations/Thursday/Thurs_CyberOps-CAE_SLaFountain.pdf (Last Accessed: 22 Feb 2011).

[10] Lunt, B. M., Ekstrom, J. J., Gorka, S., *et al.*, Information Technology 2008: Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. *Association for Computing Machinery (ACM); IEEE Computer Society*, November 2008.

[11] Dark, M. J., Ekstrom, J. J. and Lunt, B. M., Integrating Information Assurance and Security into IT Education: A Look at the Model Curriculum and Emerging Practice, *Journal of Information Technology Education*, Vol 5, pp 389-403, 2006.

[12] Rowe, D. C., Lunt, B. M. and Ekstrom, J. J., The Role of Cyber Security in Information Technology Education. *In Proceedings of the 12th Annual Conference on IT Education (SIGITE 2011)* (Westpoint, New York), Association of Computing Machinery.

[13] Stohr-Hunt, P. M., An Analysis of Frequency of Hands-On Experience and Science Achievement, *Journal of Research in Science Teaching*, Vol 33, Iss. 1, pp 101-109, 1996.

[14] Nersessian, N. J., Conceptual change in science and in science education, *Synthese*, Vol 80, Iss. 1, pp 163-183, 1989.

[15] Ma, J. and Nickerson, J. V., Hands-on, simulated, and remote laboratories: A comparative literature review, *ACM Computing Surveys*, Vol 38, Iss. 3, pp 7, 2006.

[16] Dittrich, D., On Developing Tomorrow's "Cyber Warriors". *In Proceedings of the 12th Colloquium for Information Systems Security Education* (Dallas, Texas, USA), June 2-4, 2008.

[17] McDonald, G., Joseph P. McDonald Remembers the Pearl Harbor Attack, December 7, 1941. *University of Houston*, http://www.uh.edu/engines/mcdonald.htm (Last Accessed: 22 Feb 2012).

[18] White, G. B. and Williams, D., Collegiate Cyber Defense Competitions. *In Proceedings of the Ninth Colloquium for Information Systems Security Education* (Atlanta, Georgia), The ISSA Journal, October 2005.

[19] White, G. B. and Williams, D., The National Collegiate Cyber Defense Competition. *In Proceedings of the Tenth Colloquium for Information Systems Security Education* (Baltimore, MD), June 2006.