Cybersecurity Education: The Emergence of an Accredited Academic Discipline?

Charles E. Wilson

University of Detroit Mercy

Center for Cyber Security and Intelligence Studies

Author Note

Charles E. Wilson, Department of Criminal Justice Studies, University of Detroit Mercy

Correspondence concerning this paper should be addressed to Assistant

Professor Charles E. Wilson, Department of Criminal Justice,

University of Detroit Mercy, Detroit, MI 48221

Contact: wilsonce@udm.edu

Cybersecurity Education: The Emergence of a New Academic Accredited Discipline?

Abstract

For the past two and a half decades, a growing threat has gained momentum and increasingly presented a serious national security and public safety threat to America's wellbeing. This growing menace is the illegal and malicious cyber-based threat in the form of cybercrime, cyber-espionage, cyberterrorism, cyberwarfare, and all other genre of computer enabled crimes. The combination of multifaceted cyber-based threats and ever changing attack methods pose a clear and present danger to the national security, economic prosperity, public safety, and social order of America. To address this imposing danger, the country must develop, implement and sustain a comprehensive program of education, training and skill development for cyber professionals and practitioners, who will operate, manage and lead the U.S. cybersecurity efforts. This paper examines the scope of the cyber threat and explains America's efforts to address the growing danger by creating a cyber-education platform and producing a professional and expert cybersecurity workforce. Additionally, one approach to the education of college students in preparation for entering the cybersecurity workforce is presented. Lastly, this paper recommends that cybersecurity education be established and sustained as a formal accredited discipline with national and international standards embedded in all curricula and programs.

Keywords: cyber security, cyber education, cyber-based threats and attacks

Introduction

In 1988, The Morris worm was the first cyberspace attack to affect the then emerging global cyberspace (Spafford, 1991). The worm used weaknesses in the UNIX system and replicated itself so much that it slowed down computers to the point that they became unusable. The worm was the work of Robert T. Morris, who stated he was just trying to determine how big the Internet was. His attack infected more than 6,000 university, research center and military computers. As a result of his illicit actions, he was the first person to be convicted under the US' computer fraud and abuse act (Dressler, 2007). This cyber attack was the first salvo of an emerging and growing phenomenon, cyber-based threats. Since that first cyber attack and over the past two and a half decades, the cyber threat has gained momentum and increasingly presents a serious national security challenge and public safety threat to America's wellbeing.

Since that 1988 attack, the United States and the international community have been battered by an onslaught of menacing attacks and criminal activities in cyberspace. The Information or Digital Age has created a new domain for illegal activity and technological threats. The number of cybersecurity-related threats and attack schemes has proliferated around the world – whether it is called cybercrime, cyberterrorism, Cyber–espionage, cyber-theft or computer crime – it has increased exponentially in scope and intensity. Individuals, groups and state actors engaging in cyber-based activities of an illicit nature have shown a remarkable ability to adapt to changing technologies, environments and situations (Britz, 2009).

To counter this growing cyber-threat, the U.S. government has instituted a number of educational programs, in partnership with business and academia, to produce capable professionals and trained practitioners for the cybersecurity field. A major step in this effort was the development of an initiative for creating an education platform and workforce framework, the National Initiative for Cybersecurity Education (NICE). This is a multiagency effort led by the National Institute of Standards and Technology (NIST) in partnership with the Department of Homeland Security (DHS). The goal of this effort is to create a Cybersecurity Workforce Framework that defines the academic standards, organizational structure and specific functional requirements for all job functions within the cybersecurity workforce. Today, there are over 160 academic programs certified as National Security Agency/Department of Homeland Security National Centers of Academic Excellence in Information Assurance.

Literature Review

Throughout the developed world, governments, military organizations, private sector businesses and industries, retailers, financial institutions, and individuals are being targeted and

damaged by a number of vicious cyber attacks. Rowe, Ekstrom, and Lunt (2012) noted that "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." Both Presidents Obama and Bush declared that the cyber security threat is one of the most serious economic and national security challenges to America, today. The nation's critical infrastructure is at risk and must be protected from cyber attacks and intrusions (White House, 2013). The national security, economic prosperity, public health and safety of America in the 21th century will depend on cybersecurity.

Upon taking office, President Obama ordered a thorough review of federal efforts to defend the U.S. critical infrastructure and directed the development of a comprehensive approach to securing that infrastructure. In May 2009, the President received the Cyberspace Policy Review and selected an Executive Branch Cybersecurity Coordinator with regular access to the White House. Furthermore, the President ordered various federal agencies and key players within the Executive Branch, The Department of Justice, the Office of National Intelligence, The Department of Defense, and The Department of Homeland Security to work closely with all key players in U.S. cybersecurity arena. Furthermore, he directed that all efforts should include state and local governments and the private sector, to ensure an organized and unified response to future cyber incidents; strengthen public/private partnerships to find technology solutions that ensure U.S. security and prosperity (White House, 2009).

Additionally, President Obama directed that federal resources be committed to the research and development necessary for the creation of national capabilities needed to address both the existing and emerging cyber threats. This included implementation of a campaign to promote cybersecurity education and literacy across all sectors and communities in America. A key component of this national effort is the building of a competent and skilled cybersecurity workforce in the 21st century. Finally, the president directed that these activities be conducted in a way to "…address the need to protect intelligence and law enforcement sources, methods, operations, and investigations."

The Whitehouse Policy Review describes cybersecurity professionals as being involved in activities that include:

"…strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. " (Cyberspace Policy Review, May 2009)

Nature of the Problem

The ever-increasing number of attacks, evolving threat and escalating damage resulting from cybersecurity threats are a clear and present danger to America's national security, economic prosperity, public health and safety. The extant literature illustrates the scope and nature of the cyber threats. For example, inn a hearing before the Senate Select Committee on Intelligence, John R. Clapper, Director of National Intelligence, said cyber attacks were getting worse (Clapper, 2014). He stated that "Several critical government, commercial, and societal changes are converging that threaten a safe and secure online environment…."

Similar testimony was presented to various Congressional committees and hearing panels by other key U.S. government national security officials. In his first testimony as FBI Director, James Comey spoke to the Senate Committee on Homeland Security and Governmental Affairs about threats to the nation. He stated that the diversity of the threats we face are increasingly cyber-based. He predicted in the future cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats (Comey, 2013). In a separate hearing before the Senate Armed Services committee, Army General Keith Alexander, head of the U.S. military's Cyber Command, said cyber attacks on private companies and in particular on the U.S. banking sector were getting worse. He predicted that the intensity and number of attacks will grow significantly throughout the year (Alexander, 2013). Collectively, these key government leaders expressed alarm over this growing menace, stressing that computer technology is evolving so quickly it is hard for security experts to keep up.

In 2008, The Bureau of Justice Statistics issued a special report, "Cybercrime against Business, 2005". In the report, the bureau noted that 7818 businesses responded to a National Computer Security Survey, representing 36 economic industries. The survey results showed that in 2005, the respondents:

- Detected over 22 million incidents of cybercrime
- Suffered1.5 million computer virus infections
- 126, 000 cyber fraud incidents
- 67% detected at least one cybercrime.
- Nearly 60% had at least one or more types of cyber attack
- Suffered monetary losses totaling $867 million dollars
- Had 323,900 hours of system downtime caused by cyber attacks
- Had 193,000 hours of system downtime caused by virus infections

The report noted that overall only 15% of the business reported cybercrimes to official law enforcement agencies and only 50% reported cyber thefts to police (Bureau of Justice Statistic, p 2). The overwhelming majority (86%) of the businesses not reporting cyber incidents to law enforcement indicated that they reported to the matter to other non-police authorities, such as their internal security department. Half of the businesses (50%) reported that they did not think there was anything to be gained by reporting the incident to law enforcement. The report indicated that a cyber attack could impact a number of critical infrastructure/public key infrastructure sectors in the United States, including agriculture, emergency response and preparedness systems, transportation, energy, health care, financial services, and telecommunications. Public key infrastructures (PKI) are relied upon to secure a broad range of digital applications, validating everything from transactions and identities to supply chains. However, infrastructure vulnerabilities represent a significant risk to the organizations that rely on PKI alone to safeguard digital applications. The key is for organizations to build a secure cryptographic foundation in order to fully leverage the benefits and opportunities afforded by their digital applications, while consistently safeguarding integrity and trust in their PKI environments.

In any given year, approximately 431 million adults globally fall victim to cybercrime, at a price of $388 billion based on time and monetary loss, costing the world significantly more than the global black market in marijuana, cocaine, and heroin combined. Cybersecurity involves protecting critical information by preventing, detecting, and responding to attacks. Many of our lives depend on digital technology, which makes cybersecurity one of our country's most important national security priorities. While the government is taking steps to keep our cyber community safe, the government alone cannot solve the problem. Cybersecurity is a shared responsibility. Securing cyberspace means that we, as a country, must develop a technologically-skilled workforce, a cyber-savvy public, and an effective pipeline of future employees. Billions of dollars are being spent on new technologies to help secure the U.S. cyberspace. It will take a national strategy, similar to the effort of upgrading science and mathematics education in the 1950's, to meet this challenge.

Cybersecurity a National Imperative

In 2005, the Bush administration impaneled the President's Information Technology Advisory Committee (PITAC) which studied the security of the information technology (IT) infrastructure of the United States. They published a report that stated:

> Improving the Nation's cyber security posture requires highly trained people to Develop, deploy, and incorporate new cyber security products and practices. The number of such highly trained people in the U.S. is too small given the magnitude of the challenge. At U.S. academic institutions today, the PITAC estimates, there are fewer than 250 active cyber security or cyber assurance specialists, many of whom lack either formal training or extensive professional experience in the field.

The U.S. Government and several of its key agencies have suffered serious cyber intrusions. These types of cyber attacks are neither a new experience nor rare event in America's history. For example, a number of early cyber-attacks, such as Moonlight Maze from Russia, in 1999; Titan Rain from China, in 2004, and others serious attacks on Department of Defense (DoD) and other sensitive national security and intelligence information systems highlighted the reality of the emerging cyberspace threat. Moonlight Maze refers to an incident in which U.S. officials accidentally discovered a pattern of probing of computer systems at The Pentagon, NASA, United States Department of Energy, private universities, and research labs that had begun in March 1998 and had been going on for nearly two years. Sources report that the invaders were systematically marauding through tens of thousands of files, including maps of military installations, troop configurations and military hardware designs. The United States Department of Defense traced the intrusion back to a mainframe computer in Russia but the sponsor of the attacks is unknown and Russia denied any involvement (Adams, 2000).

More recently, cyber intruders tied to China have managed to gather "several terabytes of data related to design and electronics systems" of the F-35 Lightning II fighter. Moreover, U.S. defense contractors such as the Lockheed Martin Corporation and Northrop Grumman Corporation have experienced penetrations from hackers based in China in the past. The U.S. National Counterintelligence agencies have documented intrusions from China into the computer systems of Congress, NASA, and U.S. oil and energy companies, Google's networks, and numerous networks of U.S. Fortune 500 manufacturing corporations (Office of the National Counterintelligence Executive, 2011). Another example of the evolving cyber threat is the STUXNET virus, described as being so advanced and effective it is referred to as the first offensive cyber-weapon (Falliere, Murchu, and Chien, 2011).

The Cybersecurity Workforce

The U.S. Bureau of Labor Statistics estimate that there will be 295,000 new IT jobs created in the United States by 2018, many of which will require cybersecurity expertise; new partnership focuses on cybersecurity training and education (U.S Bureau of Labor Statistics, 2013). The 2013 $(ISC)_2$ Global Information Workforce Study found an ever widening gap between the supply of qualified information security professionals and the demand for skilled workers to secure critical information and the cyber world. The study shows that the workforce will grow at a compound annual growth rate of 11.3% globally between now and 2017, calling for an additional 2.0 million new workers (Suby, 2013). The study noted that there is a gap between the need for information security professionals and the supply of new, skilled workers. The $(ISC)_2$ study also showed a significant increase in cyber threats driven by the rapid introduction of new technologies and personal devices that don't have integrated or embedded security protection. In addition, the number of organized attacks is increasing as the threat evolves from individual hackers to amorphous groups of transnational and international organized criminals who share techniques and conduct highly coordinated attacks. These situational factors highlight the current

and growing need for a competence and skilled cyber workforce to address this growing cyber-based threat.

U.S. Government Initiatives

As previously noted, the U.S. Government has recognized the challenges presented by the contemporary cyber-based threat to critical areas of America's national security, economic prosperity, and social order. In 2009, the Cyberspace Policy Review, advocated for a national strategy to create a cybersecurity workforce sufficient in numbers and competency to secure the United States in cyberspace. President Barak Obama accepted the recommendations of the Cyberspace Policy Review, and directed that the U.S. Government and its agencies implement specified actions to implement the recommendations of the Cyberspace Policy Review. The President directed that the activities be conducted in a way that is consistent with the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) in January 2008. The CNCI serves as a key component of the updated national U.S. cybersecurity strategy. It included a number of key and mutually reinforcing initiatives with the following major goals designed to secure the United States in cyberspace:

• To establish a front line of defense against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.

• To defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.

• To strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

It is the third goal which gives synergy to contemporary academic efforts and operational activities aimed at addressing the cybersecurity challenges and threats menacing America today. Specifically, within the CNCI, Initiative #8., Expand cyber education; it states that" it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success." The extant literature indicates that there are not enough cybersecurity practitioners within the Federal Government or private sector to implement the CNCI, nor is there an adequately established cybersecurity educational capacity to produce sufficient cyber workforce personnel. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-skilled workforce and create an effectual source of future employees. It will

take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950's, to meet this challenge.

In 1958, America faced a similar challenge in the form of a perceived threat of Russian superiority in technological development and intellectual capital. As a result, the National Defense Education Act (NDEA) was signed into law on September 2, 1958, providing funding to United States education institutions at all level. It was one of a set of academic based initiatives implemented by President Dwight D. Eisenhower to increase the technological competencies and intellectual capacities of U.S. students. The launch of the Russian satellite was assessed as a major humiliation for the country, proclaimed it a dangerous threat to the nation's security" (Ravitch, 2000). To address the situation, government officials called for improvements in American public education and its mathematics, science, and foreign languages areas (Leiding, 2009; Zharo, 2009). Seemingly overnight, a nationwide clamor arose for higher academic standards in U.S. high schools and greater attention to A series of federal laws were passed that focused on educational content and improvement of educational quality, and provided federal funding so that state and local governments would have an incentive to change curricula and make improvements (Schwegler, 1982). The National Defense Education Act of 1958 (NDEA) supported education improvement at all levels. (Schwegler, 1982; Urban, 2010). This historical national education reform and transformational academic effort is a model approach for current national cybersecurity education programs.

All sectors of American society (government and private industry) must take steps to identify, recruit, educate, and train competent leaders and skilled professionals for the varied roles needed in the cybersecurity workforce. The U.S. has implemented several cybersecurity educational initiatives aimed at improving cybersecurity capabilities and providing a competent workforce. For example, the U.S. National Initiative for Cybersecurity Education (NICE) strategic plan established several objectives for "Building a Digital Nation". The plan suggests five strategies to achieve this objective:

1. Increase the quantity and diversity of computer science courses in high schools
2. Increase the quantity and diversity of undergraduate and graduate cybersecurity curricula
3. Champion cybersecurity competitions
4. Advance excellence in cybersecurity research and development
5. Coordinate a learning network of virtual national cybersecurity laboratories

University of Detroit Mercy's Cybersecurity Education Approach

It is within the framework of the National Initiative for Cybersecurity Education (NICE) that the University of Detroit Mercy established its Center for Cyber Security and Intelligence Studies (CCSIS) and adopted its pedagogical approach to cybersecurity education. In 2004, the University was designated as a National Centers of Academic Excellence in Information Assurance Education. In 2009, the University opened the CCSIS and created two specific cyber laboratories: one for intelligence analysis and studies, and another for computer information studies. These two cyber-based laboratories serve as the core of the cybersecurity education

curriculum. Moreover, the faculty understands and adheres to the scholastic precepts and criteria of the National Centers of Excellence program. The faculty, courses and curriculum are focused on providing students with the essential knowledge, skills, and abilities that cybersecurity practitioners, professionals, and leaders should possess

While it is recognized that cybersecurity requires a solid foundation of technical skills, there are other knowledge, skills and abilities that a cyber-practitioner and competent leader must possess. For example, criminal justice, critical thinking, intelligence analysis, security of critical infrastructure assets, knowledge of the social legal and policy underpinnings of cybersecurity, cyber ethics, and risk management are just a few other disciplines that have a role in a holistic cybereducation. At the University of Detroit Mercy the students are provided with a solid liberal arts education that complements their cybersecurity education. Moreover, during their academic experience, students are exposed to the right balance of disciplines associated with cybersecurity in order to create the cybersecurity education needed for development of the expertise, competence and ability required to succeed in the cybersecurity profession. This fosters an integrated education experience across multiple disciplines in both cybersecurity and other educational areas of study.

Because all sectors, such as defense, the intelligence community, law enforcement and businesses are putting greater emphasis on cybersecurity and the management of risks in cyberspace, there is a growing need for professionals with interdisciplinary skills and knowledge. The incorporation of other disciplines into the cybersecurity educational process provides a broader perspective of the complexity and broad array of challenges facing America and the International Community, today. Due to the rapidly changing and constantly evolving nature of the cybersecurity threats, the daily discovery of new vulnerabilities in software and hardware, and the increasing number of cybersecurity intrusions, the cybersecurity workforce must have the knowledge, skills, and abilities to effectively counter current and emerging cyber-based threats.

Today, criminals such as “hackers,” transnational organized crime organizations, gangs, and terrorist groups are increasingly exploiting cyberspace for illegal purposes and creating new techniques for employing the Internet to perpetrate and facilitate cybercrime activities. The cybersecurity workforce must be able to identify and response to, investigate, and minimize the damage caused by the cybercriminal subculture. A multidisciplinary education in forensic sciences, intelligence analysis, criminal law and procedures, cyber-terrorism, deviant behavior, and abnormal psychology can enhance the critical thinking and cognitive analysis skills of the cybersecurity students.

Clearly, cybersecurity has become more than a technical issue centered only in a technological context of software, computers and networks; it is a much broader national security issue and is much more prevalent as an essential enabler across an array of domains. In fact, according to the U.S. Department of Homeland Security, most of America’s critical infrastructures, including key utilities, food, water, financial services, public health, first responders, energy distribution, and transportation, are totally dependent on information

technology for essential operations and activities (U.S. Department of Homeland Security [DHS], 2009). The incorporation of other disciplines into the cybersecurity education process enables the growth and development of intellectual processes in cybereducation students by fostering an in depth examination and understanding of related aspects such as the impact of social science, governance, private and public sector policy, law and ethics. Kessler (2012) suggested that academia needs to apply new ways of thinking, new understanding, and new strategies to the nation's response to cyberattacks. Furthermore, several researchers have argued that cybersecurity should be fused with homeland security in a curriculum that incorporates the all-hazards approach focused on aspects of intelligence gathering, threat analysis, planning management, policy assessment, risk analysis and threat mitigation, as well as antiterrorism/counterterrorism (Bellavita, 2008; Ramsey et al., 2010).

To that end, the University of Detroit Mercy has established a Center for Cybersecurity and Intelligence Studies. The center utilizes a comprehensive cybersecurity educational approach that is a multidisciplinary model incorporating the technical context of information technology with the broader liberal arts and social science disciplines. The model described in this paper is illustrative of a cybersecurity educational model that capitalizes on the strengths of a diverse and comprehensive interdisciplinary education. The model recognizes the diversity and depth of the current and emerging cybersecurity threats and strives to provide the students with the cognitive abilities, critical thinking skills, and knowledge necessary to effective address the challenge.

Conclusion

This paper examined how cybersecurity attacks, and emergent threats have impacted American cyber security, economic prosperity, and public safety areas. It also described how cybersecurity has entered into the broader realms of national defense and homeland security. It examined and explained the nature, scope and intensity of the cybersecurity threat menacing all sectors, facets and aspects of American society. The paper considered the critical role that academia plays in education of the cybersecurity workforce and ensuring that America has the capability to identify, response to and mitigate the dangers associated with cybersecurity threats and attacks. There is emergent literature that suggest that cybersecurity and information assurance are multidisciplinary fields of study and sufficient in pedagogy, body of knowledge (content), and maturity to be an accredited academic discipline (Dark, Ekstrom and Lunt, 2006). In conclusion, there are multiple reasons and sufficient evidence to support establishing cybersecurity as an accredited academic discipline. The University of Detroit Mercy's Center for Cyber Security and Intelligence Studies and the other 159 National Centers of Academic Excellence are proof positive that American academia can serve as a force multiplier for producing the cybersecurity workforce; perform as a facilitator for advancing cybersecurity as an accredited academic discipline. Lastly, the National Centers of Academic Excellence are clearly the foundation of cybersecurity education in America and with adequate resources can ensure that cybersecurity graduates gain the required knowledge, skills, and abilities to be effective and capable professionals in the U.S. cybersecurity workforce.

REFERENCES

Adams**,** J. (2000). Chief Executive Officer, Infrastructure Defense, Inc., testimony before the Senate Armed Service Committee, Washington, D.C. March 2, 2000.

Alexander, K, (2013). U.S. Army General, head of the U.S. military's Cyber Command, testimony Before the Senate Armed Services committee, Washington, D.C. March 12, 2013.

Bellavita, C. (2008). Changing homeland security: What is homeland security? Homeland Security Affairs Journal, 4 (2). Retrieved from http://www.hsaj.org.

Britz, M.T. (2009). Computer forensics and cyber crime. Upper Saddle River, NJ: Prentice Hall

Clapper, J. R (2014). Director of National Intelligence, testimony Before the Senate Committee on Intelligence, Washington, D.C. January 29, 2014.

Comey, J. B. (2013). Director Federal Bureau of Investigation. Statement before the Senate Committee on Homeland Security and Governmental Affairs, Washington, D.C. November 14, 2013.

Dark, M., Ekstrom, J.J., and Lunt, B. (Integrating *Information Assurance and Security into IT Education: A Look at the Model Curriculum and Emerging Practice*. *Journal of Information Technology Education, 5*.

Dressler, J. (2007). "United States v. Morris". *Cases and Materials on Criminal Law*. St. Paul, MN: Thomson/West.

Kessler, G.C. (2012). Information security: New threats or familiar problems? IEEE Computer Magazine, 45(2), 59-65.

Leiding, D. (2009). *Reform Can Make a Difference: A Guide to School Reform*. Lanham, MD: Rowman & Littlefield Education.

Office of the National Counterintelligence Executive (2011). *Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011: Foreign Spies Stealing U.S. Economic Secrets in Cyberspace*, October 2011.

President's Information Technology Advisory Committee. (2005). *Cyber Security: A Crisis of Prioritization.* Arlington, VA: National Coordination Office for Information Technology Research and Development.

Ramsey, J., Cutrer, D., & Raffel, R. (2010, May). Development of an outcomes-based, undergraduate curriculum in homeland security. Homeland Security Affairs Journal, 6 (2). Retrieved from http://www.hsaj.org/

Ravitch, D. (2000). *Left Back: A Century of Failed School Reforms*. New York, NY: Simon & Schuster.

Rowe, D.C., Ekstrom, J.J., and Lunt, B. (2012). Cyber-Security, IAS and the Cyber Warrior, Proceeding of the 16th Colloquium for Information Security Education

Schwegler, S. J. (1982). *Academic Freedom and the Disclaimer Affidavit of the National Defense Education Act: The Response of Higher Education*. Dissertation: Teacher's College, Columbia University.

Spafford, E.H. (1991). The Internet Worm Program: An Analysis. Purdue University Technical Report CSD-TR-823

Suby, M. (2013). Frost & Sullivan market study, 2013 (ISC) Global Information Security Workforce Study.

The White House, (2003), *The National Strategy to Secure Cyberspace* Washington, D.C. http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

The White House, (2003) Cyberspace Policy Review. Washington, D.C.: The White House, May, 2009. http:// www.whitehouse.gov.

Urban, W.J. (2010). *More than Science and Sputnik: The National Defense Education Act of 1958*. Tuscaloosa, AL: University of Alabama Press.

U.S. Department of Homeland Security (DHS*), National Initiative for Cybersecurity Careers and Studies, Professionalization*, http://niccs.us-cert.gov/careers/professionalization.

U.S. Department of Homeland Security (DHS), 2009. National Infrastructure protection plan: Partnering to enhance protection and resiliency. Washington D.C. Retrieved from http:// www.dhs.gov/library/NIPP_Plan.pdf.

Zhao, Y. (2009). *Catching Up or Leading the Way.* Alexandria, VA: Association for Supervision & Curriculum Development.