2013

Paradigms for Cybersecurity Education in a Homeland Security Program

Gary C. Kessler
Embry-Riddle Aeronautical University, kessleg1@erau.edu

James Ramsay
Embry-Riddle Aeronautical University, ramsa301@erau.edu

Paradigms for Cybersecurity Education in a Homeland Security Program

GARY C. KESSLER Embry-Riddle Aeronautical University
gary.kessler@erau.edu

JAMES RAMSAY Embry-Riddle Aeronautical University
james.ramsay@erau.edu

ABSTRACT

Cybersecurity threats to the nation are growing in intensity, frequency, and severity and are a very real threat to the security of the country. Academia has responded to a wide variety of homeland security (HS) threats to the nation by creating formal curricula in the field, although these programs almost exclusively focus on physical threats (e.g., terrorist attacks, and natural and man-made disasters), law and policy and transportation . Although cybersecurity programs are commonly available in U.S. colleges and universities, they are invariably offered as a technical course of study nested within engineering (or other STEM) programs. We observe that technical and calculus-based courses might not be well suited to HS students and do not necessarily meet a broad suite of professional needs in this discipline. As a result, cybersecurity principles, and strategies tend to be under-represented in the typical HS program. This paper proposes paradigms that could be included in a cybersecurity curriculum that are consistent with the broad array of outcomes now evident in many HS degree programs.

INTRODUCTION

Cybersecurity and *information assurance* are widely used buzzwords in the homeland security (HS) field today. The fact that all U.S. critical infrastructures, including food, water, financial services, healthcare, emergency services, energy distribution, and transportation (U.S. Department of Homeland Security [DHS], 2009a), are totally dependent on the flow of reliable data makes information systems vital to the ongoing health of the U.S. economy — and society. Further, these same systems are both aged and vulnerable to cyberattacks, either by hackers with criminal intent, from natural disasters, or through breaches by terrorists. Cyberattacks today are not just about defacing any website that someone can break into, but instead tend to target specific organizations or industries with an aim of destroying (or otherwise adversely affecting) infrastructure, stealing intellectual property, or disrupting the economy (Center for Strategic and International Studies [CSIS], 2008; Homeland Security Advisory Council [HSAC], 2012). Complicating matters is the fact that there is a national

shortage of cybersecurity expertise (Beidel & Magnuson, 2011; Finkle & Randewich, 2012).

Recently, there have also been highly publicized warnings from the defense community. For example, U.S. Secretary of Defense Leon Panetta has warned of an impending "cyber Pearl Harbor" (Fryer-Biggs, 2012), which was perhaps influenced by a 10-year-old book titled *Pearl Harbor Dot Com* (Schwartau, 2002). National Security Agency (NSA) Director General Keith B. Alexander publicly asked the attendees of the Defcon hacker conference for their help to secure cyberspace (Constantin, 2012). And the Defense Department's Cyber Command is slated to quintuple in size in the next several years (Nakashima, 2013). Clearly, cybersecurity has entered into the broader realms of national defense and national security.

Taken together, it is clear that cybersecurity is on the short list of the national security challenges for the U.S. The Clinton, Bush, and Obama administrations have each recognized the growing importance of securing the U.S. cyberspace and have taken steps to produce plans to protect cyberspace (CSIS, 2008; The White House, 2000, 2003, 2011).

Homeland Security degree programs are clearly charged with producing managers, analysts, and policy makers who can address current and emerging threats to national security. Academic programs in information security have been available since the 1990s. The NSA and Department of Homeland Security (DHS) cosponsor the Center of Academic Excellence in Information Assurance Education (CAEIAE) program that recognizes academic curricula and institutional commitment to information security education at two-year, four-year, graduate, and research institutions (NSA, 2012). At this time, however, there is no recognized academic accreditation body or agency for HS or cybersecurity programs, much less any organized plan to address the DHS's stated needs of hiring cybersecurity professionals (U.S. DHS, 2009b, 2012).

Infusing academic HS programs with principles of cybersecurity. We believe that academia needs to apply new ways of thinking, new understanding, and new strategies to our nation's response to cyberattacks (Kessler, 2012). Just as cybersecurity is about process rather than technology, our response to cyber-related security challenges of the day are not solely about technical solutions but must also involve a myriad of related topics such as national defense, economics, sociology, political science, diplomacy, history, and many other social sciences. Over the last six or seven years, academic HS programs have largely arisen as broad field, applied social science programs (Ramsay, Cutrer, & Raffel, 2010). As such, they are ideally suited to providing a context in which to efficiently place the principles, tools and concepts required by this new set of professionals charged with managing infrastructures critical to the U.S. economy. Indeed, many scholars have recently observed that such skill sets are desperately needed in government (Little, 2012; Reeder, Chenok, Evans, Lewis, & Paller, 2012).

Although *cybersecurity* is the term commonly used by the federal government (e.g., it is used in the White House's *National Strategy to Secure Cyberspace* and in the U.S. military's cyber command planning document), it is, strictly speaking, actually a subset of the broader discipline of *information security*. While to the average practitioner this might be a slightly fine hair to split, it is nonetheless an important one. The prefix *cyber* implies computers and/or networks, yet there are a large number of information security policies and procedures that address neither computers nor networks. Information security, in contrast, refers to all aspects of securing and protecting information from unauthorized access or use. Indeed, the term *information assurance* has the broadest applicability, by describing the security of information and adding aspects of governance, private and public sector policy, and law. This paper will use the term *cybersecurity* because that is the word that the federal government tends to use in its security and planning documents. The reader is asked to think broadly.

The Homeland Security Act (2002) mandates that academia take an active role in homeland security education. Although the Act does not provide specifics, cybersecurity education in furtherance of DHS' mission and goals is an obvious task. To date, the DHS Science and Technology (S&T) Directorate has been the main point-of-contact between the academic community and DHS. The S&T Directorate currently supports 12 Centers of Excellence (COE) through its Office of University Programs. These Centers represent a comprehensive network of universities who develop basic and applied research in science, technology, engineering, and mathematics (STEM) programs that directly support the strategic plan for the S&T directorate and that of the entire DHS. A very real question, though, is whether STEM curricula are the *only* appropriate path for integrating cybersecurity education into the larger homeland security academic enterprise. STEM-oriented cybersecurity programs are heavily based in the physical sciences and concentrate on programming, tool development, and implementation of security mechanisms rather than the managerial, analysis, or policy components of applied cybersecurity (writ large). In contrast, most (especially undergraduate) HS programs tend to be broad field, applied social science programs that develop the analytical and critical evaluation skills of middle managers. The integration of cybersecurity policy and management aspects in an HS curriculum would specifically address the academic needs of DHS and other homeland security agencies for the future.

An obvious approach for a HS program to integrate information security education into the curriculum is by having students take these courses as offered by the computer science, computer technology, or computer engineering departments, and focus on computer design and programming, operating systems, network architectures and protocols, and other computer science topics that are essential to the study of the science and technology of cybersecurity.

This approach does not necessarily meet the needs of HS students, however. One issue is that these courses often have prerequisites (or, at least, an assumption that

students have a background) in calculus, physics, and/or programming, and are not focused on "computer security for the social sciences." While a solid foundation in technology is important for those experts to detect, respond, and counterattack in cyberspace, a multidisciplinary approach is also essential for homeland security professionals.

In particular, rather than attempt to force students into an engineering-based approach to cybersecurity, HS programs should integrate the *National Response Framework* (U.S. DHS, 2008) and, in particular, the *all-hazards* approach, into a curriculum that fully explores intelligence gathering, threat analysis, planning, management, policy development, risk analysis and mitigation, as well as antiterrorism/counterterrorism (Bellavita, 2008; Ramsay et al., 2010). These are the subjects in which HS programs concentrate and they are not generally taught in the classical engineering curriculum.

The combination of a cybersecurity curriculum within a more social science-based HS undergraduate curriculum, then, would attempt to bridge the gap between an engineering approach to cyber security education and that of a social scientist's approach which would aim to address the stated needs of DHS and the changing face of homeland security (Bellavita, 2008; Ragan, 2012). This perspective on cybersecurity education is important and timely for HS programs as we have already entered an era of cyberterrorism and cyberwarfare, as evidenced by Advanced Persistent Threat-class attacks, specific attacks on hardware (e.g., Stuxnet and Flame), and attacks on information systems for political and ideological goals (e.g., by groups ranging from Anonymous to the Cyber Fighters of Izz ad-din Al Qassam).

Paradigms of cybersecurity. Although HS students may not need engineering expertise in order to understand the threats in cyberspace, they do need in-depth cyberliteracy integrated into the balance of their homeland security education. It is essential that HS students learn real cybersecurity content but at a level consistent with the holistic approach of the core HS program.

Like homeland security writ large, cybersecurity is not a monolithic discipline. It is a complex and dynamic construct that integrates multiple disciplines. To most people, the term "cybersecurity" most likely immediately conjures up thoughts of antivirus software and firewalls. Within the context of a homeland security program, cybersecurity — or, more broadly, information assurance — instead comprises multiple dimensions, all of which have a real HS component, as shown in Figure 1.

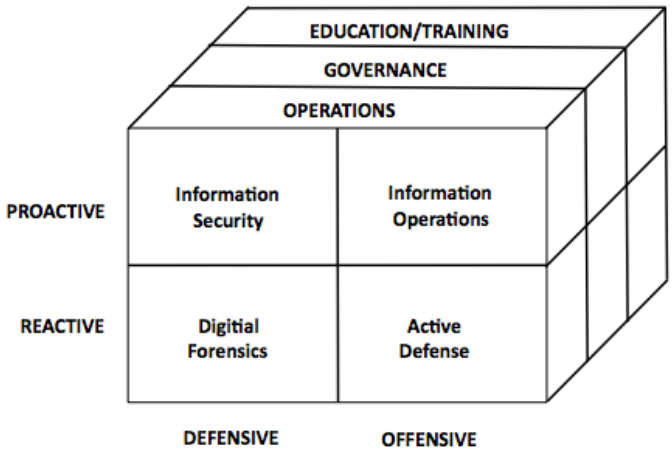

Figure 1. Paradigms in information assurance/cybersecurity.

First, we observe that cybersecurity comprises three planes of study. *Operations* addresses the day-to-day functioning of the information security task. Operational issues include staffing, implementation of policies and procedures, incident response, business continuity, disaster recovery, systems management, tool acquisition and deployment, log analysis, investigations, and more. It is in this plane that an organization needs to identify, assess — and understand — its information security needs and select the systems, tools, and technologies required in order to carry out its mission.

Governance addresses the management of the cybersecurity function. Most critically, the governance function includes the development of the organizational structure and command chain that oversees, manages, and handles information and information systems. Roles and responsibilities of individuals in this personnel chain include the chief information officer, chief information security officer, information security administrators and technicians, data managers, and other information stakeholders.

Governance tasks also include the development of policies and procedures that drive the operational aspects, as described above. Governance informs users about appropriate use of systems and information, I.T. staff as to appropriate procedures during normal and emergency operations, and management as to the relationship between information, technology, and the organizational mission. Risk assessment is also an important governance function, as it is essential that an organization's management understand the pertinent threats, vulnerabilities, and risk level of information in order to define the risk tolerance. Tools and methodologies with which to assess performance, analytics, personnel management, and budgeting would also fall under governance.

Finally, governance also includes the laws and policies that set the societal expectations of individual and organization activities. The cultural mores of a

society drive the ethical standards that, in turn, drive the laws of the society. In the U.S., there are a wide range of laws that govern our citizens. Categories of law include criminal law (statutes guiding actions that are deemed to threaten or harm public safety or welfare), civil law (procedures governing noncriminal disputes between people and/or organizations), and administrative law (rules defining the activities of governmental agencies). In the U.S., laws cover a wide range of privacy, due-diligence, and other issues, such as the Electronic Communications Privacy Act (ECPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act, Sarbanes-Oxley (SOX) Act, Controlling the Assault of Nonsolicited Pornography and Marketing (CAN-SPAM) Act, Digital Millennium Copyright Act (DMCA), Identity Theft and Assumption Deterrence Act, Security and Freedom Through Encryption Act, and Privacy Protection Act (PPA).

Education/training addresses knowledge transfer to cybersecurity professionals, organization staff, the user community, and others. *Training*, in this context, refers to teaching individuals specific skills and competencies that are usually task- or project-oriented, whereas *education* provides individuals with a systemic understanding of a particular discipline. Training makes people become quickly functional with a tool or methodology while education is the basis for life-long learning, critical thinking, innovation, and subsequent skill acquisition.

Second, cybersecurity actions can take place in a pair of two-dimensional spaces that include:

- Actions taken in response to events (*reactive*) or in order to cause an event (*proactive*)
- Actions taken in order to defend or protect (*defensive*) or in order to attack (*offensive*)

Given those two axes, there are four general categories of cybersecurity education that need to be addressed across all three planes. *Proactive, defensive (PD)* actions are those that actively defend information assets from compromise, unauthorized use, or other activity that violates information security policies. The ubiquitous CIA (confidentiality, integrity, and availability) triad or Parkerian hexad (CIA plus authenticity, possession, and utility) comes into play here, as these are the typical goals of information security activities. The operations aspects of the PD space include the use of such tools as antivirus software, malware detection, firewalls, and intrusion detection/prevention systems. Governance issues would include appropriate use policies for users and best practice configurations for the I.T. staff, as well as ensuring that organizational activities are in compliance with appropriate laws. One would expect that users would receive some level of information security awareness education, as well as training in the use of specific tools and technology that they need to employ in order to do their jobs.

Proactive, offensive (PO) actions are those activities meant to disrupt the information assets of another organization (or agency or country, etc.). The

military commonly refers to these types of activities as information operations. Operationally, the tools used here would include penetration testing software, port scanners, packet sniffers, packet spoofing tools, remote access Trojans (RATs), password crackers, war dialers, vulnerability testers, denial-of-service (DoS) tools, and a whole host of other so-called "hacker toolz." Governance — namely, the rules of engagement — become critical here, particularly maintaining compliance with national and international laws. The education needs of the actors in the PO space are obvious; they need to know how to use these tools of cyberwar and the legal framework of their actions.

Reactive, defensive (RD) actions are those taken in response to an information security event. These actions are generally in the realm of some aspect of digital forensics, which includes the investigation and analysis of computers, software, network hardware, and data traffic. The RD space is broad, and covers incident response, policy enforcement, and formal or informal investigations and analysis. RD operations include the activation of an incident response plan when a cyberattack occurs, invoking a business continuity plan, and preparing for disaster recovery. The governance issues include the policies and procedures in the development of such plans, and ensuring that all legal requirements are met during the incident, including the reporting of breaches of security and privacy. Education and training includes ensuring that all parties know their role if and when any of the plans mentioned above are invoked, as well as the periodic testing of such plans.

Reactive, offensive actions are a response to some sort of event. A subset, in some ways, of information operations, responding and reacting includes understanding the stimulating event (which might or might not be a cybersecurity incident), preparing an appropriate response, and then executing that response plan. This so-called *active defense* posture combines vigilant (some might say, aggressive) protection of assets, identifying — and learning from — adversaries, and neutralizing a threat before it becomes a successful attack (Reed, 2012).

Pedagogy and curriculum design. The goal of cybersecurity education integrated into an HS program is to provide technical literacy for a student population that is, in general, not overly technically inclined and that may, in fact, have some level of techno- and/or math-phobia. Success in cybersecurity does not require heavy mathematics but does require the ability to manipulate numbers and symbols. Certainly, comfort with technology is essential. Problem and puzzle solving skills are also essential for both cybersecurity and HS professionals.

In particular, HS students need to understand cybersecurity at a level that allows them to understand a particular issue and synthesize the ramifications into other aspects of national security. If a particular cyberattack employs a buffer overflow, for example, it is important to understand that the solution to the problem is better software practices rather than a bigger firewall. Intelligence gathering, analysis, and policy creation tasks depend upon the professional understanding some detail

below the surface; it does not require, however, that they have the ability to actually write the same attack code that they understand and appreciate.

To that end, students need courses that systematically present the following major topical areas:

- A survey of the subject matter, as suggested in Figure 1 and subsequent discussion, that addresses operations, governance, applications, purposes, and strengths and limitations to information assurance and incident response activities
- Computer and network technology for mid-level managers (i.e., tool users)
- Defensive and offensive cybersecurity tools, methods, and procedures
- Cyberlaw history, evolution, case law, and a survey of international efforts that aim to organize and synthesize efforts to offset security threats to financial, environmental and other social systems
- The impact of cyberspace on war, diplomacy, and terrorism including emergent threats and modern countermeasures and how critical infrastructure can be hardened in order to reduce the impact of cyberattacks

CONCLUSION

In this paper, we have presented a rationale for how cybersecurity education fits into a homeland security curriculum, targeting the traditional HS student and capitalizing on the analytic strengths of the traditional HS curriculum. We also assert that HS education programs should have some form of accreditation in order to meet the homeland security (write large) needs of the country in the future.

HS education programs cannot ignore a formal inclusion of cybersecurity into the curricula. Cybersecurity, however, is not merely a course or two that should be added on to a HS curriculum; it is, instead, a discipline of its own that has many facets and perspectives. We believe that the model proposed here provides the basis for designing a cybersecurity course of study that is consistent within a HS curriculum.

REFERENCES

Beidel, E. & Magnuson, S. (2011, August). Government, military face severe shortage of cybersecurity experts. *National Defense Magazine*. Retrieved from http://www.nationaldefensemagazine.org/archive/2011/August/Pages /Government,MilitaryFaceSevereShortageOfCybersecurityExperts.aspx

Bellavita, C. (2008). Changing homeland security: What is homeland security? *Homeland Security Affairs Journal*, *4*(2). Retrieved from http://www.hsaj.org /?fullarticle=4.2.1

Center for Strategic and International Studies (CSIS). (2008, December). *Securing cyberspace for the 44th Presidency*. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Washington, D.C.: Technology and

Public Policy Program, CSIS. Retrieved from http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

Constantin, L. (2012, July 28). NSA Chief asks hackers at defcon for help securing cyberspace. *PCWorld*. Retrieved from http://www.pcworld.com/article/260007 /nsa_chief_asks_hackers_at_ defcon_for_help_securing_cyberspace.html

Finkle, J., & Randewich, N. (2012, June 13). Experts warn of shortage of U.S. cyber pros. *Reuters*. Retrieved from http://www.reuters.com/article/ 2012/06/13/us-media-tech-summit-symantec-idUSBRE85B1E220120613

Fryer-Biggs, Z. (2012, October 12). Panetta lays out new cybersecurity policy. *ArmyTimes*. Retrieved from http://www.armytimes.com/news/2012/10/dn-panetta-new-cyber-policy-101212/

Homeland Security Act of 2002, Public Law No. 107-296, 6 USC 188, § 308 (2002).

Homeland Security Advisory Council (HSAC). (2012). *HSAC* web page. Retrieved from http://www.dhs.gov/homeland-security-advisory-council-hsac

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

Little, M. (2012, October 2). Executive order on cyber security builds steam amid criticism. *Los Angeles Times Online*. Retrieved from http://www.latimes.com/news/politics/la-pn-obama-executive-order-cyber-security-20121002,0,6786970.story

Nakashima, E. (2013, January 27). Pentagon to boost cybersecurity force. *The Washington Post*. Retrieved from http://www.washingtonpost.com/world/ national-security/pentagon-to-boost-cybersecurity-force/2013/01/19/ d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html

National Security Agency (NSA). (2012, August 17). National centers of academic excellence. *NSA* web site. Retrieved from http://www.nsa.gov/ ia/academic_outreach/nat_cae /index.shtml

Ragan, S. (2012, October 3). DHS secretary discusses cybersecurity hiring with advisory board. *SecurityWeek*. Retrieved from http://www.securityweek.com/dhs-secretary-discusses-cybersecurity-hiring-advisory-council

Ramsay, 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/?article=6.2.4

Reed, J. (2012). Inside one of U.S. cyber command's offensive units. *Foreign Policy Group, National Security* web site. Retrieved from http://killerapps. foreignpolicy.com/posts/2012/10/24/inside_one_of_us_cyber_commands_offensive_units_0

Reeder, F.S., Chenok, D., Evans, K.S., Lewis, J.A., & Paller, A. (2012, October). *Updating U.S. federal cybersecurity policy and guidance: Spending scarce taxpayer dollars on security programs that work.* A report of the CSIS Technology and Public Policy Program. Washington, D.C.: Center for Strategic and International Studies. Retrieved from http://csis.org/files/publication/121019_Reeder_A130_Web.pdf

Schwartau, W. (2002). *Pearl Harbor dot com*. Interpact Press.
The White House. (2000). *National plan for information systems protection, version 1.0: An invitation to dialogue*. Washington, D.C. Retrieved from http://www.fas.org/irp/offdocs /pdd/CIP-plan.pdf
The White House. (2003). *The National strategy to secure cyberspace*. Washington, D.C. Retrieved from http://www.us-cert.gov/ reading_room/cyberspace_strategy.pdf
The White House. (2011). *International strategy for cyberspace: Prosperity, security, and openness in a networked world*. Washington, D.C. Retrieved from http://www.whitehouse.gov/sites/default/files/rss_viewer/ international_strategy_for_cyberspace.pdf
U.S. Department of Homeland Security (DHS). (2008). *National Response Framework*. Washington, D.C. Retrieved from http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf
U.S. Department of Homeland Security (DHS). (2009a). *National infrastructure protection plan: Partnering to enhance protection and resiliency*. Washington, D.C. Retrieved from http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
U.S. Department of Homeland Security (DHS). (2009b, October 1). Secretary Napolitano announces new hiring authority for cybersecurity experts. U.S. DHS Office of the Press Secretary. Retrieved from http://www.dhs.gov/news/ 2009/10/01/secretary-napolitano-announces-new-hiring-authority-cybersecurity-experts
U.S. Department of Homeland Security (DHS). (2012). Cybersecurity. Retrieved from http://www.dhs.gov/cybersecurity