A Proposed Curriculum in Cybersecurity Education
Targeting Homeland Security Students

Gary C. Kessler
Embry-Riddle Aeronautical University
Daytona Beach, Florida, USA
gary.kessler@erau.edu

James D. Ramsay
Embry-Riddle Aeronautical University
Daytona Beach, Florida, USA
james.ramsay@erau.edu

Abstract
Homeland Security (HS) is a growing field of study in the U.S. today, generally covering risk management, terrorism studies, policy development, and other topics related to the broad field. Information security threats to both the public and private sectors are growing in intensity, frequency, and severity, and are a very real threat to the security of the nation. While there are many models for information security education at all levels of higher education, these programs are invariably offered as a technical course of study; these curricula are generally not well suited to HS students. As a result, information systems and cybersecurity principles are underrepresented in the typical HS program. The authors propose a course of study in cybersecurity designed to capitalize on the intellectual strengths of students in this discipline and that are consistent with the broad suite of professional needs in this discipline.

1. Introduction

Cybersecurity, information security, and information assurance are widely used buzzwords in the homeland security (HS) field today and hacking, information operations, and cyberwarriors are terms that are growing in use, as well. Because all U.S. critical infrastructures, including food, water, government operations, financial services, healthcare, emergency services, energy distribution, and transportation [1], are totally dependent on the flow of reliable data, information systems are vital to the ongoing health of the U.S. economy and society at large. Information security threats are well beyond pedestrian hackers defacing any Web site that they can break into; today we see specific organizations, industries, or countries being targeted with the aim of destroying or disrupting infrastructure, stealing intellectual property, or upsetting the economy [2,3].

This situation could have hardly been underscored in a more serious fashion than the development of Executive Order (EO) 13636 and Presidential Policy Directive (PPD) 21 in early 2013 [4,5]. Exacerbating the problem, from a homeland security perspective, is the recognized national shortage of cybersecurity expertise [6,7]. It is clear that cybersecurity is one of the primary national security -- and national defense -- challenges for the U.S. Given central role that information plays in the U.S. and global economies and societies, in general, the need for cybersecurity within the realm of homeland security cannot be overstated. The last three presidents each recognized the growing importance of information security and took steps to produce plans to protect cyberspace [2,8,9,10]. The Department of Defense (DoD) U.S. Cyber Command, created in 2009, is scheduled to quintuple in size by 2017 [11]. The Department of Homeland Security (DHS) is making a concerted effort to hire cybersecurity professionals [12].

The nation's academic community has a long history of responding to the needs of industry, society, and the government. Academic programs in information security, for example, have been widely available since the 1990s. The National Security Agency (NSA) and DHS co-sponsor 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 [13]. Homeland Security (HS) programs, tasked with producing managers, analysts, and policy makers who can address

---

1 Cybersecurity is the term commonly used by the federal government although, strictly speaking, it is actually a subset of the broader discipline of information security. Information assurance has the broadest applicability, by describing the security of information and adding aspects of governance, private and public sector policy, and law. For purposes of this paper, the three terms will be used interchangeably.
current and emerging threats to national security, started to appear in the mid-2000s [14].

2. The Intersection of Homeland Security and Cybersecurity Education

The authors observe that at this time, HS and information security programs are largely disjoint. Most information security degree programs are technical in nature, usually offered through computer science, computer engineering, or computer technology departments. Their intent is to produce information security professionals who we will term tool developers; e.g., software engineers, system administrators, network administrators, and security administrators. HS degree programs, on the other hand, have largely arisen as applied social science curricula, and decidedly non-technical.

We believe that a new approach needs to be taken by the academic community to respond to the constantly evolving cyberthreats facing this nation and our response to them [15]. 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 myriad of related topics such as national defense, economics, sociology, political science, diplomacy, history, and many other social sciences. This skill set is precisely within the bailiwick of HS programs, which 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. We would term this group as tool users, those that employ and understand technology tools to understand and solve the problems of the days. Indeed, many scholars have recently observed that such skill sets are desperately needed in government [16,17].

In an earlier work, the authors introduced a set of paradigms of information security that speak to the complex, multidisciplinary nature of the field (Figure 1) [18]. In short, we observe that cybersecurity comprises three planes of study:

- **Operations**: The day-to-day functioning of the information security task.
- **Governance**: The management of the cybersecurity function, including internal policies and procedures as well as law and policy.
- **Education/training**: Transfer of knowledge to cybersecurity professionals and users, ranging from teaching specific skills and competencies to providing systemic understanding and life-long learning.

Each of these planes contains a pair of two-dimensional spaces. One axis describes actions taken in response to events (reactive) or in order to cause an event (proactive), while the other axis describes actions taken in order to defend or protect (defensive) or in order to attack (offensive).

3. HS Cybersecurity Curricula Design Principles

The Homeland Security Act of 2002 [19] 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 component of robust and responsible homeland security education. Most HS programs, especially at the undergraduate level, have matured over the last seven years as broad, applied social science programs that develop the analytical and critical evaluation skills of middle managers. The integration of cybersecurity policy and management aspects into such an HS curriculum would specifically address the academic needs of DHS and other homeland security agencies for the future.

The easiest way to integrate information security education into an HS curriculum is by having students take the technical courses that are already available at most colleges and universities. These courses, however, tend to 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, however, does not necessarily meet the needs of HS students, who need "computer security for the social sciences." While a solid foundation in technology is important for

![Figure 1. Paradigms in information security [18].](image-url)
those experts to detect, respond, and counter-attack in
cyberspace, a multidisciplinary approach is also
essential for homeland security professionals.

Rather than attempt to force students into an
engineering-based approach to cybersecurity, HS
programs could integrate the National Response
Framework [20] 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 anti-/counter-terrorism [14,21].
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 scientists approach which
would aim to address the stated needs of DHS and the
changing face of homeland security [21,22].

Although HS students may not need engineering
expertise in order to understand the threats in
cyberspace, they do need in-depth cyber-literacy
integrated into the balance of their homeland security
education in order to understand a particular issue and
synthesize the ramifications into other aspects of
national security. If a particular cyberattack exploits a
buffer overflow, for example, it is important that the
professional understand that the solution 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.
Thus, it is essential that HS students learn real
cybersecurity content but at a level consistent with the
holistic approach of a core HS program.

Not every HS student is necessarily a good
candidate for a course of study in information security.
The goal of cybersecurity education integrated for HS
students 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
technophobia. Success in cybersecurity as a tool user
does not necessarily require heavy mathematics but
does require the ability to manipulate numbers and
symbols. Certainly, comfort with computer technology
is essential. Problem and puzzle solving skills are also
important for both cybersecurity and HS professionals.

4. Cybersecurity Curriculum Proposal

The authors both teach in the Homeland Security
program at [name of institution]. The absence of
information security as a significant topic within the
curriculum was recognized three years. The initial
response was to define a cybersecurity track composed
of computer courses offered by the Engineering
Department. The idea of a cybersecurity track within
the HS program proved very popular with the students
but the track itself was poorly subscribed because of
the requirement of several calculus and physics courses
as prerequisites to the computer science and software
engineering courses. In addition, computer science and
engineering courses do not subsume the major learning
outcomes that have become integral to homeland
security education.

Subsequent exploration of the industry and student
needs, in conjunction with external advisers, input
from students, an exploration of industry needs, and a
review of existing curricula resulted in the plan to
integrate cybersecurity into the HS curriculum in two
ways. First, we elected to create an introductory
information security course to be integrated into the
HS core that is taken by every HS student. Second, we
defined a five-course (15 credit) minor course of study
which can, ostensibly, be taken by any students on
campus but which is specifically designed with HS
majors in mind.

![Cybersecurity Course Flowchart]

**Figure 2. Proposed cybersecurity courses.**

The six courses and their general sequencing are
shown in Figure 2. Their content and role in the overall
curriculum is described below.

The first course is *Foundations of Information
Security*, a 100-level course that is being introduced as
The second 300-level course is *Introduction to Digital Forensics*. This hands-on course focuses on the tools and techniques of reactive offense and defense. The course will introduce to the broad field of incident response and digital investigations, and the gathering of digital information for evidentiary, intelligence, and research purposes. Legal aspects governing search and seizure will be described, as well as basic tools for computer, network, and mobile device forensics acquisition, analysis, and reporting.

The two 300-level courses are a prerequisite for a 400-level course named *Cybercrime and Cyberlaw*. This course will address criminal behavior in cyberspace, such as identify theft, white-collar crimes, fraud, child sexual exploitation, intellectual property theft, and online scams. Evolving laws governing cyberspace, defining criminal activity, and guiding law enforcement investigations will be covered, including U.S. decisional law guiding search and seizure of digital devices and information as well as international laws related to computer crime and privacy.

The final course, *War, Diplomacy, and Terrorism in Cyberspace*, forms a capstone of sorts for the minor. This seminar-like course will examine the impact of cyberspace on war, diplomacy, and terrorism including emergent threats and modern countermeasures, and how critical infrastructure can be hardened and made more resilient in order to reduce the impact of cyberattacks. This perspective on cybersecurity education is important and timely for HS programs as the nation has 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), 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), and the impact of social networks and the Internet on diplomacy and social change.

One of the particular challenges in creating this curriculum is the design of appropriate assessment instruments. The 100- and 200-level courses provide essential facts and concepts necessary for the understanding and assimilation of the contents of the 300- and 400-level courses. Since the intention of the early courses is not to prepare students for technical careers or jobs -- but, rather to enhance their understanding of homeland security -- the testing cannot fairly be about the technical aspects of the subject matter. Instead, assessment mechanisms must be prepared that better measure what social science students have learned about technology and addresses the learning outcomes of the courses that are relevant to homeland security policy and management. This suggests that hands-on exercises and writing
assignments are the best way to measure whether students have achieved the learning outcomes rather than a more traditional objective test.

5. Conclusion

HS education has proven to be a robust, dynamic, and valuable academic discipline. One method by which HS education might mature -- and maintain relevance -- is by formally incorporating cybersecurity into the curricula. While the basic elements of cybersecurity can be introduced in a course or two, HS programs should provide students with the opportunity to study information security in depth, just as they might choose specialties in emergency management, risk management, infrastructure protection, transportation security, resilience, or terrorism studies. Due to its technical nature, cybersecurity must take a multidisciplinary approach to offer both perspectives; doing so will provide students with a valuable skill set with which to address what might one of the most challenging homeland security and defense issues for the future.

As a final note, HS programs need to bring their own faculty up to speed with these issues as well as educating their students. Like all multidisciplinary topics, the course developers and faculty need to have subject matter expertise in both homeland security and information security. This will require a whole new set of practitioners entering the ranks of HS program faculty which will, in turn, broaden potential dissertation topics as well as subsequent teaching/learning scholarship.

6. References


[16] Little, M., "Executive order on cyber security builds steam amid criticism", Los Angeles Times Online, 2012,


