

Developing Cyber Warriors

LtCol Jeff Boleng, Dr. Dennis Schweitzer, Col David S. Gibson

US Air Force Academy, Colorado, USA

jeff.boleng@usafa.edu

dennis.schweitzer@usafa.edu

david.gibson@usafa.edu

Abstract

The US Department of Defense defines cyberspace as a “domain characterized by the use of electronics and the electromagnetic spectrum (EMS) to store, modify, and exchange data via networked systems and associated physical infrastructures.” Cyberspace is a warfighting domain on par with air, space, land, and sea, and the US Air Force has accepted the challenge of controlling it, defending it, and operating in it. The US Air Force Academy (USAFA) in cooperation with Air University, the AF Institute of Technology and AF Cyber Command (provisional) is developing the education and training requirements for our future cyber warriors. Much of this work builds on an already established curriculum being taught at USAFA and national training standards defined by the National Security Agency and the Department of Homeland Security. Our approach is a two-pronged effort. On one hand we provide a multi-disciplinary foundation for every graduate. We accomplish this by identifying and adding specific cyber content to our existing broad based core curriculum. On the other hand we also provide a smaller number of highly skilled, very technical, cyber warriors to support the required missions in the domain of network attack (NetA), network defense (NetD), network surveillance (NetS), and network support. We accomplish this through our accredited Computer Science major and the addition of a three course sequence including Computer Security and Information Warfare, Network Security, and Cryptography. This paper will outline the vision and broad educational requirements required for 21st century officers and provide details on our two-pronged approach to developing cyber warriors.

Keywords: education, training, cyberspace, warfare, information

1. Background and Introduction

On 7 December 2005 the US Air Force adopted the following mission statement:

The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests -- to fly and fight in Air, Space, and Cyberspace (USAF 2008).

This new mission statement is most notable for the inclusion of the term Cyberspace. The US Department of Defense defines cyberspace as a “domain characterized by the use of electronics and the electromagnetic spectrum (EMS) to store, modify, and exchange data via networked systems and associated physical infrastructures.” This definition and context emphasize that Cyberspace is a warfighting domain, on par with air, space, land, and sea. It is not a mission or a mission area, but a domain in which conflicts take place and adversaries vie for dominance. Competition and conflict in cyberspace are ongoing.

In September 2007 over 65 cyberwarfare experts and career field managers from across the Air Force converged on the AF Academy to continue developing the details for the AF Cyber Forces Education and Training Plans. The Air Force director of Air, Space, and Information Operations, Plans, and Requirements (AF/A3/5) selectively invited participants from around the Air Force to contribute to the discussions and required deliverables. The group developed the required knowledge, skills, abilities, and training tasks for Professional Military Education (officer and enlisted), enlisted training and force development plans, officer accessions requirements, and inputs for future training and education budget requirements.

The AF Academy produces roughly one quarter of all new AF officers each year. AF Academy graduates enter the Air Force with a bachelor's of science in a chosen discipline and are commissioned second lieutenants. Just over half attend pilot training. The others enter a wide variety of Air Force officer specialties. Regardless of their assigned career field, all graduates of the AF Academy must possess specific knowledge, skills, and abilities in the cyberspace domain to effectively serve as AF officers in an information-dominated 21st century.

2. Broad cyberwarrior requirements

Operations and warfare in cyberspace encompass all aspects of technology and society. Military officers called on to operate in, defend, and secure cyberspace require a broad, interdisciplinary base of knowledge and skills. The days of computationally focused “hackers” are far behind us. Today’s threats in cyberspace are not only from the traditional hacker culture that claims to be pursuing only the “knowledge that they could gain access”, but a much more dedicated adversary. The most dangerous threats today are from dedicated criminals, terrorists, and competing nation states. These adversaries are not interested in fame and ego; rather they are motivated by far more powerful political, ideological, and financial concerns.

Preparing our graduates to operate in such a domain requires a broad based core curriculum. Computer science and electrical engineering are not enough. While absolutely necessary to provide a piece of the technical foundation for cyberwarriors, these topics must be augmented with large doses of ethics, legal studies, behavioral science, and military strategic studies. Our aim is to produce officers that can not only effectively operate and fight in cyberspace, but officers that do so in a legal and ethical manner with full understanding of the complexities of the human and military strategy as applied to the domain of cyberspace.

In addition to educating our students to answer questions such as

- “What are the properties of electromagnetic waves?”, and
- “How can we exploit our adversaries’ electronic systems?”

We demand they also grapple with equally important questions like

- “What legal authorities do DoD entities have to engage in cyberwarfare?”, and
- “What are the national security implications of cyberwarfare?”.

In short, the broad requirements for a 21st century cyberwarrior include all the same interdisciplinary studies and ethical foundations that have always been demanded of military officers. If there are differences from the past to the present, it is only that the technological qualifications may be higher, and the decision timelines are much shorter. Solving ill-defined problems with severely constrained resources in very short timelines is the order of the day. While this describes fundamental requirements of combat leadership in the domains of air, space, land, and sea, the change in magnitude of the time dimension in cyberspace is unprecedented. Cyberwarriors must be able to think, decide, and act in minutes and seconds on highly complex, technical operations with potentially strategic and global implications. Preparing young, aspiring officers for this role is a daunting responsibility.

3. Preparation for all graduates

The US Air Force Academy’s educational outcomes are to

“Commission leaders of character who embody the Air Force core values,

- are committed to societal, professional, and individual responsibilities,
- are empowered by integrated intellectual and warrior skills, and
- are grounded in essential knowledge of the profession of arms and the human and physical worlds.” (USAFA 2008)

Adding detail to the three high level outcomes above are 19 supporting tier two outcomes available at <http://www.usafa.af.mil/df/usafaoutcomes.cfm>. We focus on six of these as containing essential cyberspace content. These tier two outcomes are:

- Ethical reasoning and action,
- Information literacy,
- Critical thinking,
- Decision making,
- Heritage and application of air, space, and cyberspace power, and
- Principles of engineering and the application of technology. (USAFA 2008)

Certainly all 19 supporting outcomes are essential to officership, but the demands of warfare in cyberspace highlight the above six attributes. A mapping of courses in the core curriculum that directly support these six attributes has been done.

The core curriculum is one of the mechanisms for achieving our educational outcomes for all graduates. The core courses directly supporting cyberwarrior development are from a variety of academic departments, such as computer science, law, electrical engineering, philosophy, physics,

chemistry, behavioral sciences, engineering, and military strategic studies. Our approach is to review the educational objectives and lesson plans of every course supporting one of the above listed six tier two outcomes. This will give us a baseline of the current cyber related content in the core. This baseline is currently in progress.

Finally, the remaining task, and the hardest to “get right”, is to evaluate the baseline cyber content and determine what is missing. Our current plan is to review the detailed cyber content given to our Computer Science majors in the Cyberwarfare track (reference section 4) and determine what learning objectives and content can be moved from this highly specialized degree into the broad core curriculum. In many ways this can be a zero sum game. Adding content to an already densely packed curriculum is not usually possible without sacrificing existing material. How and what cyber content is added to the core curriculum beyond what is currently present cannot be determined until the baseline is completed.

In addition to the broad core, several upper class courses have emerged to contribute to cyberspace education for all cadets. Example courses include:

- Law 495 – Cyberlaw,
- MSS 470 – Information Operations and Cyberspace,
- Mgt 391 – Information Technology for Organizations,
- Mgt 392 – Organizational Networks in Cyberspace, and
- Mgt 419/420 – Technology Innovation.

These courses augment the content of many academic majors and serve to fulfill optional upper-level courses requirements. Through the core curriculum and upper level courses like these, a great number of Academy graduates are provided cyberspace academic content.

One other way in which we develop cyber warriors is through organized military training events. All graduates of USAFA participate in a variety of training programs throughout the academic year and during their summers. Every attendee starts with Basic Cadet Training (BCT) before beginning their freshman academic year. The emphasis is on personal leadership and the basic skills required to support the Air Force mission. As cited in the opening paragraph, an essential warfighting domain for all AF personnel is cyberspace. BCT integrates skills training and efforts are underway to ensure adequate consideration is given to the domain of cyberspace. Several other summer programs are candidates for cyberspace training events that serve to re-enforce the academic content provided by cadet education programs. Examples of such programs include Global Engagement, an air expeditionary force deployment exercise, the summer space program, and the emerging summer unmanned aerial vehicle (UAV) program. USAFA has begun examining and expanding all its programs that touch all cadets to ensure that every graduate is provided the foundations required to “fly and fight in Cyberspace.”

4. Computer science major

The Academy, as an undergraduate institution, offers students the choice of over 30 academic majors to choose from in the sciences, engineering, humanities, and social science disciplines. The Computer Science major is nationally accredited and teaches fundamental concepts of the computing discipline using a hands-on approach. Within the major, students take a broad range of “core” computer science courses as well as optional courses that allow them to focus on a specific area of interest within the computer science discipline.

One area of specialization that Computer Science majors can choose is Cyberwarfare. This includes a focus on information assurance and the concepts associated with both offensive and defensive applications in cyberspace. Students selecting this option take courses in Cryptography, Information Warfare, and Network Security in addition to traditional computer science courses. Since 2004, USAFA has graduated 37 Cyberwarfare computer scientists. The Academy's emphasis on information assurance, both within the Computer Science major and across the curriculum and institution, has received national recognition as a Center of Academic Excellence in Information Assurance Education (CAEIA), a joint program of the National Security Agency and Department of Homeland Security (Schweitzer 2006).

To provide students with a workable knowledge of the practical aspects of cyber warfare, a project-oriented approach is taken in the classroom. This allows students to “get their hands dirty” with the offensive and defensive tools associated with cyber security. Projects such as password cracking,

intrusion detection, and vulnerability assessment give students a real-world understanding of the concepts they learn from textbooks. One significant project of note is the annual Cyber Defense Exercise (CDX), a network defense competition held between the service academies (Haynes 2003). Students must design, operate, and defend a network of services against an attacking opponent, in this case the NSA red team. Each team is evaluated on how well they design a secure system, provide required services, and react to attacks. This experience is very realistic and represents a scenario they may well be involved in within a few years of graduation and commissioning.

In addition to the specialized cyberwarfare track and the courses created to support it, there is content fundamental to understanding and operating in cyberspace included in a number of other courses in the computer science (CS) major. For example, computer networks, operating systems, beginning and advanced programming, and a number of other skills are taught and re-enforced in the many of the other CS classes.

5. Research and Community involvement

In addition to classroom instruction in cyber warfare, students and faculty at the Academy have the opportunity to participate in state-of-the-art research projects across a wide range of cyberspace topics. Students work on research projects as part of Independent Study courses, as class projects, and during the summer in the Cadet Summer Research Program (CSRP). The CSRP, similar to a civilian internship, typically sends students to an operational Air Force Base for six weeks during the summer to work on specific projects. In recent years, Computer Science students have participated in projects at the National Security Agency (NSA), the National Reconnaissance Office (NRO), and the Air Force Information Operations Center (AFIOC).

The Computer Science department established the Academy Center for Information Security (ACIS) in 2004 as a focal point for coordinating faculty and student research in cyberspace topics. The charter of ACIS is to enhance cadet education through innovative research opportunities for students and faculty in a wide range of information assurance topics. Several projects and publications have been produced from ACIS in topics such as:

- Jam-resistant communication (Baird 2007)
- RF signal detection and operational management
- Fault-tolerant overlays (Shelly 2007)
- Security education (Schweitzer 2007b)
- Security visualization (Schweitzer 2007c)
- Biometrics and bio-monitoring using neural networks

The Academy's goal of educating cyber warriors extends beyond the bounds of future Air Force officers. Initiatives within the local community are aimed at increasing cyber awareness of higher education schools along Colorado's Front Range. One initiative is the Front Range Information Security Conference (FRISC), an annual meeting of schools along the front range to share educational and research experiences in information assurance. The goals of the meeting are to encourage interaction between regional schools teaching information security, share ideas and experiences, and identify areas for interschool collaborations. FRISC was founded in 2004 by the Academy and now includes over 30 professors and students from nine front range institutions.

Another initiative is the Computer and Network Vulnerability Assessment Simulation (CANVAS), an annual competition of students from schools to get hands-on experience of assessing the security strengths and weaknesses of a specific information system application. It was founded co-operatively with Colorado State University (CSU) who hosted the first event in the spring of 2006. The event alternates between CSU and USAFA. The competition is unique to Colorado and extends the typical Capture-the-flag activities to teaching true assessment skills. The competition is not between schools but between ad-hoc teams created when the competitors arrive. The teams are created by randomly assigning members from each participating institution. This mixing of skills presents an accurate situation most computer security professionals experience upon entering the work force. It emphasizes working with the team, resources, and schedule you are given. The exercise does provide experience with offensive techniques but emphasizes the use of those tools to improve the critical security infrastructure of the system. Over half the score is made up of reports on weaknesses and recommended solutions to improve system security. Approximately 60 students and ten faculty members from five different institutions participate annually.

6. Summary

The United States Air Force Academy is a leader in cyber education, training, and research. Educational and training content focuses on the knowledge, skills, and abilities that every graduate must have to effectively serve as Air Force officers in an information-dominated 21st century. A select number choose to pursue a highly technical Computer Science degree with an emphasis in Cyberwarfare. Additional higher level classes are available for a broad spectrum of cadets as a reflection of the interdisciplinary nature of strategy, operations, and issues in the domain of cyberspace. Cadet education is enhanced with the opportunity to participate in world class research through the Academy Center for Information Security, as well as collaboration and cooperative events and exercises with the community of Colorado Front Range colleges and universities. USAFA's rigorous education and constant infusion of operational military experiences create a unique environment that attracts, educates, and graduates past, current, and future cyberspace leaders.

References

USAF 2008, Mission Statement quoted from <http://www.af.mil/main/welcome.asp>

USAFA 2008, Educational outcomes quoted from <http://www.usafa.af.mil/df/usafaoutcomes.cfm>

Schweitzer, D., Humphries, J., and Baird, L., "Meeting the criteria for a center of academic excellence (CAE) in information assurance education," *J. Comput. Small Coll.* October 2006.

Haynes, A. and Stratton, T. "Cyber Defense 2003 & Information Assurance Education," In *Proceedings IEEE 2003 International Conference on Systems, man & Cybernetics*. Oct 2003.

Baird, L., Bahn, W., and Collins, M., "Jam-Resistant Communication Without Shared Secrets Through the Use of Concurrent Codes", U.S. Air Force Academy Technical Report USAFA-TR-2007-01, 14 February 2007.

Shelly, N., Jensen, N., Baird, L., and Moore, J., "Fault-tolerant overlay protocol network", IEEE Workshop on Information Assurance, West Point, NY, June 2006.

Schweitzer D., Collins M., Baird L., "A visual approach to teaching formal access models in security," Proceedings of the 11th Colloquium for Information Systems Security Education, June 2007 (b).

Schweitzer, D., Brown, W., Boleng, J., "Locating rogue access points using visualization," *J. Comput. Small Coll.* October 2007 (c).