

A Hands-on Approach to Information Operations Education and Training

Jeff Boleng and Dino Schweitzer, *United States Air Force Academy*

Abstract – Our institution prepares young men and women to enter military service each year. All of these officers are immediately integral to the ongoing conflict in cyberspace. Every mission in today’s military relies on cyberspace for successful accomplishment and every military member is an integral part of the day to day defense of our networks and information assurance. Every graduate of our institution must understand the art of the possible in the information and cyber domains and be prepared to integrate information and cyber techniques into ongoing operations to achieve the desired effects on the adversary. In order to prepare our graduates for 21st century warfare in and through the cyber domain we developed an Information Operations (IO) training program and are working to make it available to all students.

Index terms – Security education, information operations

I. BACKGROUND AND MOTIVATION

Cyberspace is ubiquitous in modern developed societies. The global economy is electronically interconnected in innumerable ways. This global integration has enabled the sharing of information at speeds never before imagined. The technology and complexity required, while a staggering achievement, is also fragile in many respects. This complexity and fragility provide opportunities for exploitation and are targeted daily by hackers, organized criminals, and nation states [1, 2]. The ongoing struggle for cyber security has led to a new type of warfare. The battle for the control of information is as old as society itself [3]. The battle for the control of digital information is what defines cyber warfare.

Our institution graduates approximately 1000 officers per year that will all be involved in cyber warfare in one way or another. For some it will define their military careers. All of them will rely on cyber capabilities to perform their warfighting mission. Graduates of our computer science, computer engineering, and electrical engineering programs appreciate the potential (both offensive and defensive) of cyber warfare [4, 5]. However, not every graduate is familiar with the art of the possible in cyber warfare and the ease to which many things can be accomplished. As a result, we have undertaken many initiatives to raise awareness of cyber threats and defenses to all students, not simply computer science majors. As part of these initiatives, we have developed a summer

training program focused on students with a diverse academic background to experience and demonstrate the potential of information operations, especially the potential of information operations in the cyber domain.

II. INFORMATION OPERATIONS VS INFORMATION ASSURANCE

An informal definition of information operations is using information to influence an adversary and achieve an outcome as well as controlling the information an adversary has targeted against you. The desire to control information has always been a critical element of warfare. The realization of the cyber domain has created a battle ground where the struggle for information dominance has accelerated dramatically.

Joint publication 3-13 formally describes Information Operations as “the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC)...[6].” These are often referred to as the five pillars or capabilities of information operations. Of note, two of the five capabilities are a direct result of the man-made cyber domain. Focusing on any one of these capabilities individually requires an in depth background knowledge and a specialized set of skills. Broadening the focus to emphasize their relationships and integration allows us to appeal to and include a much broader audience. Furthermore, the broad application of information operations is relevant to operational commanders regardless of military specialty. In fact, every soldier is directly involved in protecting our operational information from adversary exploitation, or OPSEC. It is precisely this broad applicability that led us to focus on the larger IO perspective rather than narrow our training to IA or CNO.

Our goal was to create a training program that was accessible and appealing to students from a wide variety of academic backgrounds and aptitudes. Our focus was not on the technology necessarily, but on the value of the information and the speed and accessibility enabled by the technology. As a result, we specifically designed the training to focus on the information and the value people attach to it. Information assurance as we traditionally understand it in the context of computer and network

security is a critical element of the flow of information, but not the primary focus of the training program.

III. RELATED WORK

Teaching information assurance and cyber security in colleges has increased dramatically in the last 10 years. A primary example of this is the establishment of the Department of Homeland Security and National Security Agency Centers of Academic Excellence (CAE) in Information Assurance (IA) Education program [7]. There are now 104 officially recognized CAE universities that have mapped elements of their curriculum to national training standards and demonstrated institutional commitment to IA education. Our program was first recognized in 2003 and has received re-certification through 2013.

The skills our graduates require are somewhat different than traditional computer security or IA professionals. Many of our Computer Science (CS) graduates will be called upon to not only defend the military's computer and information enterprise, but employ skills and tools in an offensive nature to gather intelligence and achieve effects in the cyber domain. The knowledge, skills, and abilities required for this are above and beyond those traditionally taught in a typical computer security course sequence. In 2001 the US Military Academy (USMA) at West Point established a student chapter of the Association for Computing Machinery's (ACM) Special Interest Group for Security, Audit, and Control (SIGSAC) [8]. This group is a part of USMA's Information Technology and Operations Center (ITOC) [9]. The experiences and success USMA has had with this program inspired faculty members at our institution to develop a similar group [5]. We leveraged the experiences gained in this focused effort to create a training program and expand its offering to our entire student population.

IV. OUR PROGRAM

At our institution, we teach information assurance, information warfare, and information operations concepts in a number of academic courses. All of our Computer Science students are required to take an introductory course in Information Warfare and Computer Security. In addition, the majority of our CS students take both Cryptography and Network Defense. Students completing all three courses receive an Information Warfare Track designation on their academic transcript. Outside of the CS major, we teach all students in a freshman course the fundamentals of computer security, including concepts in cryptography, public key infrastructure, password security, and current threats.

In addition to our normal academic year, we have opportunities to provide education and training in specific areas of interest to the military during summer programs. All students are required to take two 3-week summer programs in addition to their summer leave. Programs include activities such as Survival Training, Basic Training, Summer Academics, Summer Research, and various orientations to operational capabilities. Summer programs are highly focused since student's time is not divided among several disciplines as is the case during the academic year, and students can be fully immersed in day-long activities. While some academic activities exist, the emphasis is more on hands-on training to motivate and teach students about a topic in-depth.

We proposed and implemented a summer program in 2009 to provide students a hands-on experience in Information Operations. The goals of the program were to:

- Provide information about IO doctrine and tactics
- Demonstrate both defensive and offensive capabilities
- Increase awareness of the threat by focusing on the "art of the possible"
- Allow students to practice their craft in a controlled real-world exercise

In an attempt to reach as wide an audience of students as possible, we specifically did not require any previous knowledge or background to participate in the program. We believe that all of our graduates will be facing various cyber threats in their careers, and should be aware of the dangers as well as defensive measures. We did not want to limit the experience to just a small cadre of computer science or technically-oriented students. Rather, we wanted to provide students from all academic specialties the opportunity to learn about IO. As the program was a pilot offering, we limited the number of students and length of time. For this initial offering, 19 sophomores participated in the 10-day program which was offered over two different time periods.

Because of the decision to not limit students based on background or academic major, it was important to provide sufficient background with each topic so that students understood the context and basic concepts at some level. To avoid student burn-out, we broke each day into morning lectures followed by hands-on activities through the afternoon. The program consisted of the following eleven blocks:

1. Threat brief and IO / IW overview
2. Password cracking

3. IO doctrine overview and campaign plan objectives
4. Phones, radios, GPS, and wireless
5. SQL injection
6. Hands-on phones radios, GPS, and WiFi
7. Cyber warfare and hacker methodology
8. Single machine penetration, Backtrack and Metasploit
9. Scanning and enumeration
10. FAA attack scenario
11. Email spoofing and phishing

Lessons included both lecture and hands-on labs to reinforce concepts. Many of the labs used locally developed web-based approaches that allowed students to practice activities in a controlled environment and did not require extensive technical background knowledge.

In addition to the lecture portion of the program, a large part of the summer experience was to develop and execute an IO campaign plan against a live adversary. The live adversary in this case was another student summer program named Global Engagement (GE). GE is a bare-base deployment training exercise that runs in parallel with the summer IO program. The purpose of GE is for students to stand up, operate, and defend a base in a semi-hostile environment. Instructors act as an opposing force (OPFOR) aggressor group that plans and executes activities against the base. We worked with the GE organizers to allow our students to provide IO support to the aggressor group and conduct operations that simulated an actual environment.

As part of the IO campaign plan, students were given the following intelligence collection objectives. Obtain or otherwise determine:

- a full camp roster,
- the guard and shift schedule,
- radio call signs and frequencies,
- radio authentication codes,
- a phone roster,
- the organization chart and key personnel list, and
- the camp layout with critical nodes identified.

In addition to collecting intelligence, the campaign plan had to include one or two diversion tactics in support of the OPFOR kinetic attacks and one or two false information injects. Students were provided time at the end of each day to work on their campaign plan, brainstorming IO activities, performing intelligence gathering, and practicing techniques.

Upon completion of the plan, students briefed it to both the IO program organizers and the GE staff. Permission was obtained to execute several portions of the plan to

achieve different effects on their adversary. For example, they staged multiple protest demonstrations in and around the camp to provide a diversion for the OPFOR kinetic attacks.



One of the more effective attacks was a man in the middle attack executed with a radio obtained in a previous diversionary attack. The students intercepted a frequency change order and used it to keep one flight of GE students (approximately 30) isolated on a separate channel. By acting as higher headquarters to the “lost” flight and as the “lost” flight to higher headquarters, they were able to keep the flight roaming around the woods on a wild goose chase for nearly two hours. During this time, the camp was guarded by only two-thirds of the original force and the OPFOR attack success went up dramatically.

As another example of a hard lesson learned by the GE force, part of the campaign plan was to use a suicide bomber. The students, in their creative enthusiasm, built a fake suicide vest, along with a hand detonator.



A student wearing the vest under his coat was taken into captivity and taken to a secure area. When he threw open his coat to reveal the “explosive” vest and threatened to blow everyone up, the GE students did not know how to react. They called in the remaining security forces to view the vest and determine how to react. Thus, rather

than blowing up a single security team, the suicide bomber was successful in “eliminating” all of the security forces in the camp at the time.

To help evaluate the effectiveness of the IO program, we conducted pre and post-surveys of students regarding their attitudes and knowledge toward information warfare and the cyber threat. The table below shows the results on a 1-5 Likert scale.

	Pre	Post
Knowledge of IW	1.8	3.4
Knowledge / experience w/ computer hacking	1.4	3.2
Desire to learn offensive computer attacks	3.7	3.9
Desire to learn defensive comp techniques	3.4	3.7
How important is IW knowledge going to be for you in your career	3.5	3.9
Do you believe the next major war will be fought in the information domain	3.3	3.8
Do you believe we are heading for a “Cyber Pearl Harbor”	3.4	3.3

Most of the areas showed an increase after students completed the program. There were significant increases in the student’s perceived knowledge level, and slight increases in their desire to learn more. Interestingly, their perception of the likelihood of a catastrophic cyber event went down slightly. It is unclear whether this is a result of a more realistic view of the current state of the threat and technology, or increased optimism about our ability to respond.

Student responses to individual activities within the program indicated they enjoyed the activities with every block rated above 3.1 on a Likert scale. The least favorite activities were Password Cracking and Phones / radios / GPS / wireless. Their favorite activities were Email spoofing and phishing, the FAA scenario attack lab, and the actual Campaign plan execution. Individual comments on the survey were universally positive.

V. CONCLUSIONS

Effectively operating in and using the cyber domain is a critical element in current and future warfare. For the majority of people, the focus is on the quality, speed, and accuracy of the information exchange that modern cyber technologies make possible. Information assurance is not about firewalls, anti-virus software, proxy servers, etc. It is about assuring the information required to make better informed decisions faster than your adversary. Understanding the technologies that enable this is absolutely critical for the relatively few technicians supporting the communications and computers systems. However, understanding and experiencing the what is

possible and the resulting effects of information compromise and corruption are essential elements in every warriors training. We have developed a set of training modules into an integrated curriculum that allows military members of any academic background and aptitude the ability to take part in both offensive and defensive information operations and cyber warfare. The experiences obtained provide a valuable foundation available to all future warriors as they develop their skills and abilities to defend their nation’s vital interests.

VI. REFERENCES

- [1] Baker, Wade H., et al. 2009 Data Breach Investigations Report. http://www.govinfosecurity.com/external/2009_databreach_rp.pdf. Last accessed 15 Mar 2010.
- [2] Baker, Hylender, and Valentine. 2009 Data Breach Investigations, Supplemental Report. http://www.govinfosecurity.com/external/rp_2009-data-breach-investigations-supplemental-report_en_xg.pdf. Last accessed 15 Mar 2010.
- [3] Sun Tzu. The Art of War. Translator Lionel Giles. Chapter 13, “The Use of Spies” or “The Use of Intelligence.” Specifically rules 22 and 23. <http://www.gutenberg.org/etext/132>. Last accessed 15 Mar 2010.
- [4] Boleng, J., Schweitzer, D., and Gibson, D. “Developing Cyber Warriors,” 3rd International Conference on Information Warfare and Security, 2008, Omaha, Nebraska.
- [5] Boleng, J., Henson, M. “Expanding Cyberspace Education and Training,” 5th International Conference on Information Warfare and Security, 2010, Dayton, Ohio.
- [6] Joint Publication 3-13 “Information Operations”, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf. Last accessed 15 Mar 2010.
- [7] NSA National Centers of Academic Excellence. http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml. Last accessed 15 Mar 2010.
- [8] Gregory Conti, Daniel Ragsdale, Scott Lathrop, and Christopher Gates. “Implementation and Lessons Learned from an Undergraduate Special Interest Group in Information Security”, Proceedings of the 2004 Colloquium for Information Systems Security Education.
- [9] USMA Information Technology and Operations Center (ITOC), <http://www.itoc.usma.edu/>, last accessed November 19, 2009.

Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010