Report 1337.3

Towards a Cyber Leader Course: Not for the Weak or Faint Hearted

Gregory Conti, Michael Weigand,
Ed Skoudis, David Raymond,
Thomas Cook, Todd Arnold and Daniel Ragsdale

Department of Electrical Engineering & Computer Science
United States Military Academy
West Point, NY 10996
(Gregory Conti, Michael Weigand, Ed Skoudis,
David Raymond, Thomas Cook,Todd Arnold, Daniel Ragsdale) @usma.edu

Vol 1337 No. 3
26 May 2014

ACI
Army Cyber Institute

Army Cyber Institute reports are published with the intent to foster professional dialogue and debate. As such, the views expressed in this article are those of the authors and do not reflect the official policy or position of West Point, Army Cyber Command, the Department of the Army, the National Security Agency, US Cyber Command, the Department of Defense, or the US Government.

Towards a Cyber Leader Course: Not for the Weak or Faint Hearted

Gregory Conti, Michael Weigand, Ed Skoudis, David Raymond, Thomas Cook,
Todd Arnold, and Daniel Ragsdale

Since 1950, the U.S. Army Ranger School has garnered a well-earned reputation as one of the most demanding military schools in the world. Graduates have served with distinction in special operations units including the Ranger Regiment and Special Operations Command as well as line units throughout the Army. With the emergence of cyberspace as an operational domain and the critical shortage of technically and operationally competent cyber leaders, the time has come to create a U.S. Army Cyber Leader Course of equal intensity, reputation, and similar duration,[1] but focused on cyber operations (see Figure 1). This article presents a model for the creation of such a school. We are not attempting to create a longer-term training program akin to the U.S. Special Forces Qualification Course (informally, the Q Course) or to replicate classroom training programs found in industry, academia, government, or the intelligence community. What we propose is unique, demanding, immersive, and fills a necessary gap in Army cyber leader development.

Figure 1: Cyber Tab. A Cyber Leader Course of similar duration and intensity to Ranger School, but tailored to cyber operations would help fill the critical shortage of technically and operationally competent cyber leaders.

Ranger school is, at its heart, a leadership school which forges leaders under adversity and is focused on infantry leaders. There is a shortage of qualified cyber leaders at all ranks and a demanding and rigorous Cyber Leader Course would develop the knowledge, skills, and abilities required of technically and operationally competent cyber leaders . A cadre of highly qualified cyber leaders is critical to the professionalization of the cyber career field, but the Army currently lacks a method for developing these leaders. This article serves as a template to create a school for growing the cadre of talent required to lead cyber operations, and as a means to garner constructive feedback to refine the concept. While we propose the creation of an Army Cyber Leader Course, due to the inherently Joint nature of cyber operations, creation of a Joint, instead of Army-specific, school may prove to be a preferred way forward.

There are many definitions of "cyber." For purposes of this work we define cyber as Computer Network Attack (CNA), Computer Network Exploitation (CNE), Computer Network Defense -

[1] Ranger School is approximately 61 days long.

Response Action (CND-RA), Computer Network Defense (CND), and Electronic Warfare (EW).[2] We do not include building, operating, or maintaining computer networks in our definition, but acknowledge these areas are closely affiliated and many of these skills are prerequisites to entry into the course we are describing here.

We intend for this new Cyber Leader Course to be quickly recognized as the cyber operator's equivalent of Ranger School, much like the Sapper program has become the Engineer branch's 'Ranger School.' There is much to learn from Ranger School and other elite training programs that can inform a Cyber Leader Course.

Related work

In order to understand the need for a Cyber Leader Course, as well as to inform its design, it is important to understand the available spectrum of training options available. There are several sources of high-quality training available to cyber warriors from the security industry as well as the military and intelligence communities. While significant details are available on commercial offerings, less is publicly known about military and intelligence community courses. In this paper we only discuss those courses which provide publicly available information.

Many civilian training offerings are closely tied to industry certifications. There is a wide range of security training and certifications available.[3] Leading certifications include CompTIA's A+, Network+, and Security+, the EC-Council's Certified Ethical Hacker (CEH), and (ISC)^2's Certified Information Systems Security Professional (CISSP). A+, Network+, and Security+ certifications demonstrate a grasp of baseline level knowledge, CEH represents intermediate level network security and penetration testing skills, and CISSP demonstrates a wide, but relatively shallow, range of familiarity in security concepts. More advanced training and certification regimes are also available. The SANS Institute offers training in foundational and advanced skills including forensics, penetration testing, policy, and malware reverse engineering. SANS offers certifications paired with many of these courses, multiple levels of certification, and the ability to earn an accredited Master's degree. [4,5]

[2] We considered using the more recent Offensive Cyber Operations (OCO), Defensive Cyber Operations (DCO), and DoD Information Network (DODIN) operations definitions, but chose ours to provide greater fidelity.

[3] It is important to note that certifications are not a panacea. Possession of a given certification does not guarantee expertise, only that an individual passed the certification exam. Certifications are useful as one means of measuring knowledge, but work experience and traditional academic programs are also powerful indicators. Some of the best security researchers eschew certifications and avoid employment with companies that overly rely on certifications, believing this reliance may be an indicator of misaligned human resources policies and suspect corporate culture.

[4] By successfully passing the certification exam, test takers receive silver certification, and by completing an independent research paper on a related subject individuals receive gold certification. By completing a regime of required certifications, research, and testing students may receive higher-level certifications. The highest level SANS certification is the Global Information Assurance Certification (GIAC) Security Expert (GSE) and represents substantial demonstrated security, incident handling, intrusion detection, and analysis skills. See http://www.giac.org/certification/security-expert-gse.

[5] The SANS Technology Institute offers a Master's degree in Information Security and is accredited by The Middle States Commission on Higher Education.

The SANS Institute has also developed the “Cyber City” concept. CyberCity is a mock-up of a small city where students may see the physical world outcomes of their cyber operations activities (see Figure 2).[6] Importantly, Cyber City is composed of real-world components, such as power distribution systems, so students interact with real systems online and see the results physically occur in the city.

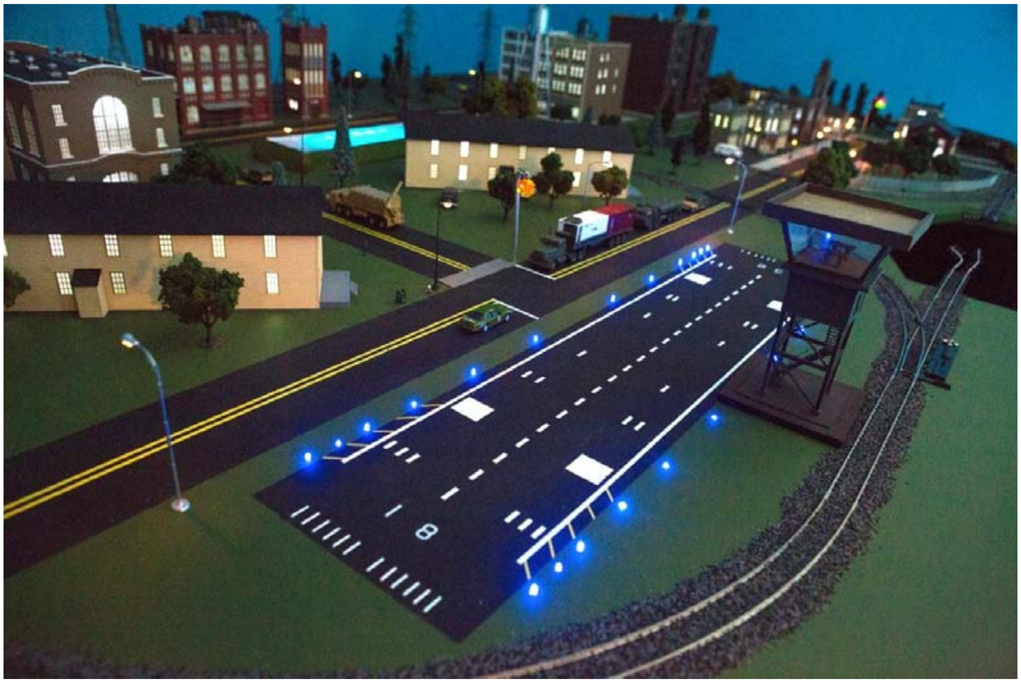

Figure 2: CyberCity is a small scale mock-up of a city, including its key underlying computing, networking, and critical infrastructure systems using real-world back-end components.[7]

We envision CyberCity or a similar technology as a valuable part of a Cyber Leader Course, particularly if implemented as a full size, immersive training environment akin to the military’s use of Military Operations on Urban Terrain (MOUT) training areas for urban warfare training and law enforcement’s use of realistic training environments such as the Federal Law Enforcement Training Center (Figures 3 and 4).[8]

[6] Robert O’Harrow. “CyberCity Allows Government Hackers to Train for Attacks.” Washington Post, 26 November 2012. See also “Real-World Cyber City Used to Train Cyber Warriors,” Slashdot, 28 November 2012 for additional discussion on CyberCity.

[7] Emily Badger. “A Tiny City Built to Be Destroyed By Cyber Terrorists, So Real Cities Know What’s Coming.” Fast Company, 2 January 2013.

[8] Federal Law Enforcement Training Center, Department of Homeland Security. http://www.fletc.gov/, last accessed 1 September 2013.

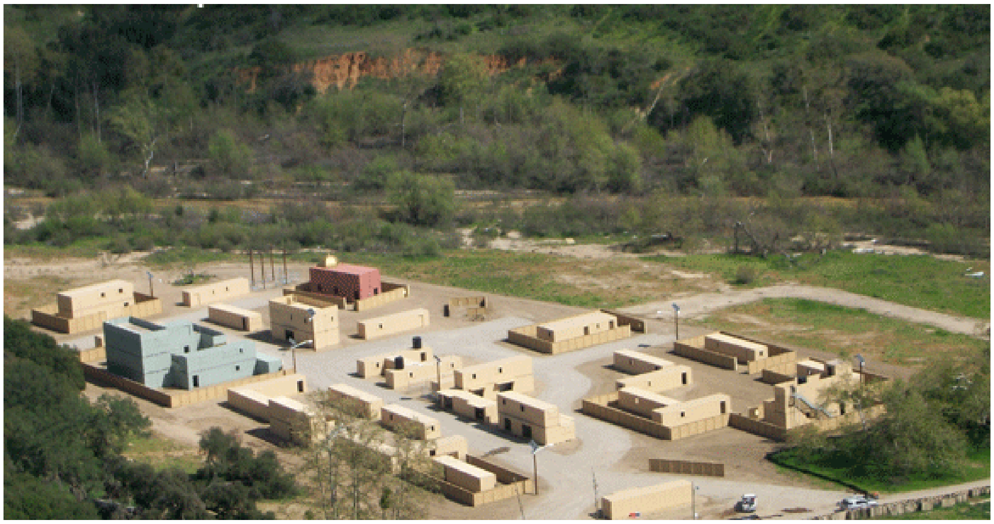

Figure 3: Military Operations on Urban Terrain (MOUT) environments could be integrated with the CyberCity concept to create an ideal training and evaluation environment for a Cyber Leader Course.[9]

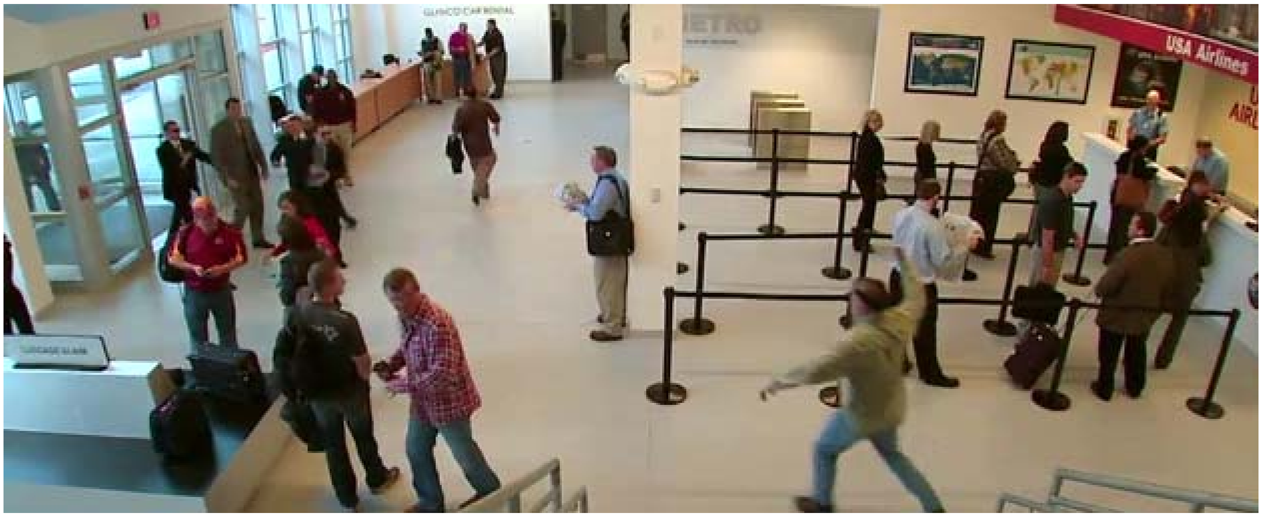

Figure 4: The Federal Law Enforcement Training Center in Brunswick, Georgia provides realistic training experiences for law enforcement officers, such as this mock airport terrorist incident with live actors.[10]

In addition to SANS, other organizations provide quality security training. Black Hat Training provides a spectrum of classes from beginner to expert, but with a lesser focus on certification.[11] Another example is KEYW, which offers a 40-hour, cyber leaders course designed to teach how adversaries penetrate perimeter security from the perspective of an Advanced Persistent Threat

[9] "Mobile Military Operations on Urban Terrain (Mobile MOUT) Training System." U.S. Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI). http://www.peostri.army.mil/PRODUCTS/MMOUT/, last accessed 1 September 2013.
[10] "Unique Facility Trains Officers to Handle Terror Threats." Fox News, 18 December 2012.
[11] As a representative example, see the Black Hat USA 2013 training offerings, http://www.blackhat.com/us-13/training/, last accessed 1 September 2013.

(APT).[12] Also noteworthy is the Defensive Cyber Operations Engineer course offered by Global Knowledge. This course offers training in malware analysis, system monitoring, social engineering, forensics, and network evasion techniques.[13]

The military offers a range of training offerings, including the Joint Network Attack Course (JNAC). JNAC is a 20 day, 160 hour course designed to teach effective planning of Computer Network Attack operations including legal authorities, battle damage assessment, de-confliction, targeting, weaponization, and execution processes.[14] NSA offers the System and Network Interdisciplinary Program (SNIP), which is a three-year program to train personnel in the technical areas of Computer Network Operations. SNIP includes three to five tours in various work centers, including at least one six month or longer tour in NSA's Information Assurance Directorate (IAD) and another in NSA's Signals Intelligence Directorate (SID).[15] Another example is the Joint Cyber Analysis Course (JCAC), which is 120 days and 976 hours. JCAC is designed to train junior and mid-level enlisted personnel for duty in computer network operations related billets. Graduates of JCAC are able to provide computer (network and infrastructure) analysis and technical solutions to produce CNO effects.[16] In addition to these courses, NSA provides robust classroom and self-paced cyber training offerings through its National Cryptologic School and the Associate Directorate for Education and Training (ADET).

To help keep pace with requirements for trained cyber warriors, the Army is developing several new career specialties: Information Protection Technician Warrant Officer (255S),[17] Cyber Network Defender (25D),[18] Cryptologic Network Warfare Specialist (35Q),[19] the Electronic Warfare Career Management Field (CMF 29),[20] and the emerging Security Systems Engineer (FA26C).[21] The training these Soldiers receive, combined with operational experience and dedicated commitment to self-development, is suitable preparation for our proposed Cyber Leader Course. Another example of military training is the Air Force Institute of Technology's Advanced Cyber Education (ACE) program. Started in 2003, ACE is eight weeks long and

[12] "Cyber Leaders Course." KEYW Corporation. http://training.keywcorp.com/clc.html, last accessed 1 September 2013.

[13] "CSFI: Defensive Cyber Operations Engineer," Global Knowledge. http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=18037&catid=191&country=United+States, last accessed 4 December 2013.

[14] "Joint Network Attack Course (JNAC)." Slick Sheet, United States Marine Corps. https://www.mcis.usmc.mil/corry/Lists/SlickSheetJNAC/AllItems.aspx, last accessed 1 September 2013.

[15] "System and Network Interdisciplinary Program (SNIP)." Fact Sheet, National Security Agency. http://www.nsa.gov/careers/_files/SNIP.pdf, last accessed 1 September 2013.

[16] "Joint Cyber Analysis Course (JCAC)." Slick Sheet, United States Marine Corps. https://www.mcis.usmc.mil/corry/SitePages/JCAC.aspx, last accessed 1 September 2013.

[17] Todd Boudreau, "Cyberspace Defense Technician (MOS 255S)," Army Communicator, Vol. 36, No. 1, pp. 35-40.

[18] Wilson Rivera, "Cyber Network Defense Pilot Course Begins," Fort Gordon - The Signal, 30 August 2013.

[19] David Vergun, "Army Opens New Intelligence MOS," Army News Service, 27 November 2012.

[20] "New Electronic Warfare Career Fields," Electronic Warfare Proponent Office, United States Army Combined Arms Center. http://usacac.army.mil/cac2/cew/FA29.asp, last accessed 21 December 2013.

[21] Office of the Chief of Signal Staff, "Signal Regiment Personnel Structure Evolving to Support Changing Operations," Army Communicator, Vol. 37, No. 4, pp. 6-8.

primarily supports Air Force ROTC cadets. It includes “instructional components, cyber war games, hands on internships and cyber officer development days that focus on the study of cyber as a revolution in military affairs.”[22] Particularly interesting is the Air Force’s use of their elite Weapons School to train airmen in how to conduct computer network attack, defense, and exploitation.[23] We believe this move helps the Air Force pilot community better relate to the capabilities of cyber operations and supports our suggestion of creating a Cyber Leader Course.[24]

Contests conducted at hacker conferences offer useful insights into potential Cyber Leader Course training and evaluation activities. Examples from the world’s largest hacker conference, DEFCON, include Capture the Flag (force on force network warfare), scenario based lock picking, network forensics, social engineering, code breaking, and bypassing of tamper resistant packaging.[25] Academic cyber security competitions, while less diverse than hacker competitions, similarly provide useful insights. Examples include the NSA-sponsored inter-service academy Cyber Defense Exercise (CDX),[26] the National Collegiate Cyber Defense Competition,[27] and the Capture the Flag, embedded systems, and forensics competitions hosted by NYU-Poly and other universities world-wide. [28]

Science fiction also offers useful insights, including, notably, the Battle School depicted in *Ender’s Game*.[29] Battle School is located on an isolated, orbiting space station, where hand-picked recruits are organized into platoon-sized formations (called Armies) and undergo rigorous combatives, weapons and classroom training, and compete in intense microgravity battles where students learn, tactics, strategy, and leadership.

Finally, academic institutions offer cyber education programs from certificates and Associate's Degrees to PhDs. Note that there is an important distinction between education, provided by multi-year degree programs, and training which is usually provided over a shorter duration. Education programs focus on long-term underlying principles, while training programs are designed to teach skills that can be immediately put to use, but may more likely become out of date as specific tools change and techniques evolve. Colleges and universities with mature

[22] “Advanced Cyber Education Program.” Center for Cyberspace Research, Air Force Institute of Technology. http://www.afit.edu/ccr/ace/index.cfm, last accessed 10 September 2013.

[23] The Weapons School is the Air Force’s equivalent of the Navy’s “Top Gun” program.

[24] Julian Barnes. “Pentagon Digs In on Cyberwar Front.” Wall Street Journal, 6 July 2012.

[25] Gregory Conti, Thomas Babbitt, and John Nelson. “Hacking Competitions and Their Untapped Potential for Security Education.” IEEE Security and Privacy, May/June 2011. For additional contest examples see the DEFCON 21 webpage, https://www.defcon.org/html/defcon-21/dc-21-index.html.

[26] John Mello, “Military Academies Take on NSA in Cybersecurity Competition,” CSO Online, 16 April 2013.

[27] “National Collegiate Cyber Defense Competition.” National Collegiate Cyber Defense Competition. http://www.nationalccdc.org/, last accessed 1 September 2013.

[28] “Cyber Security Awareness Week (CSAW).” NYU - Poly. https://csaw.isis.poly.edu/, last accessed 1 September 2013.

[29] Orson Scott Card, *Ender's Game*, Tor, 1985. See also “Battle School”, Enderverse, http://ansible.wikia.com/wiki/Battle_School, last accessed 4 December 2013.

cyber security education programs will often seek accreditation as an NSA Center of Academic Excellence in Information Assurance or Cyber Operations.

The Cyber Leader Course we propose is a unique hybrid, one that draws upon the intense crucible of Ranger School, the innovative competitions of the hacker community and academia, the rigor of high-end security training and certifications, the realism of MOUT training, all while providing career-long educational principles and values that will make Cyber Leader Course graduates sought after leaders in the cyber domain. The Cyber Leader Course will be much more than a synthesis of its parts and instead be a life-changing, even life-defining, experience.

> *“Cyber warriors are elite, trusted, precise, disciplined professionals who defend our networks, provide dominant effects in and through cyberspace, enable mission command, and ensure a decisive global advantage.”* [30]
>
> \- LTG Rhett Hernandez

Vision and Course Objectives

The vision of our Cyber Leader Course is to be the U.S. Army’s premier cyber leader development experience. Rigorous, challenging, and demanding, in our model the course will be immersive; students will have only limited contact with the outside world and personal electronics and data will be prohibited. Graduates will possess:

- A sound understanding of the technical operation and dynamic nature of cyberspace.[31]
- A warrior ethos - the ability to adapt, overcome, and fight through adversity to accomplish the mission.[32]
- The ability to plan and execute cyber and cyber/kinetic military operations, including an understanding of how their actions fit into and impact the larger tactical, operational, strategic, and national context.
- The ability to work individually and as part of a team.
- An adversary mindset - the ability to develop innovative solutions that challenge assumptions and color outside the lines as well as an above average ability to anticipate and counter adversary actions in physical space and cyberspace.[33]

[30] William Garbe. "General Says ARCYBER Progresses, Prepares for Cyberspace Future." Army.mil, 26 July 2012. http://www.army.mil/article/84427/, last accessed 1 September 2013.

[31] Depending on the exact program of instruction enacted, it may be beneficial for students to leave the Cyber Leader Course with appropriate certifications, either industry or Department of Defense. If this course of action is undertaken, students who already possess a given certification will be required to retake and pass any exams, in order to ensure currency.

[32] For an interesting discussion of the warrior ethos see Michelle Tan’s “Losing a ‘Life-or-Death Skill?,’” Army Times, 9 September 2013.

[33] We note that the Rangers were also required to develop their own techniques, tactics, and procedures as well as equipment as none existed in their early days. Bronston Clough. *Get Tabbed: How to Graduate Army Ranger School*. Clough Publishing, 2011, p. 32. We believe this is a clear analog to the cyber operations of today.

- The ability to attack the *system* - probing the attack surface, including the human users, until an exploitable vulnerability is found.
- Sound leadership of cyber warriors, including an understanding of how to adapt their leadership style for maximum effect.
- The ability to appreciate and fit within both the military and civilian cyber security communities.
- The communication skills, both in writing and orally, to communicate technical subjects to non-technical *and* technical audiences.
- Respect for the dangerous skills which they have been taught, including appreciation for legal authorities, electronic privacy, and civil liberties.
- The ability to teach themselves new technologies and new capabilities, given constantly changing technology and highly adaptive adversaries.

Training Philosophy

The primary purpose of the course is to develop resilient, technically, and operationally competent cyber leaders. The leaders should be capable of leading in demanding, time-sensitive, and high stress situations.[34] All students, regardless of background and preparation will be pushed out of their comfort zones.

In the broader Army a generalist leader model works well. However, the technical nuances required in the cyber field are fickle and minute, and yet these nuances have such a large impact on decision-making that there is no room for leaders with imperfect understanding of the domain. Also, the time sensitivity of many cyber operations makes it impossible for subordinates to sufficiently educate their superiors in time for the leader to make a cogent decision. Hence the Cyber Leader Course will seek to validate this technical foundation and the student's ability to make effective and rapid decisions in cyber operations.

The course will seek to emulate potential cyber conflict. What a future cyber conflict might look like is speculative at best, in some ways it may look like the rapid and high pressure problem solving seen in the Apollo 13 mission, but on a grander scale. Other insights can come from study of the attacks against Estonia, Georgia, and Google to inform scenarios and TTPs used in the course.[35]

The ability to understand and write computer code is an indispensable requirement for this course. We understand this may be contentious for some, but we believe an understanding of code is paramount to understanding operations within the cyber domain. Software is the underpinning of cyberspace and ignorance regarding its foundations equates to not understanding the laws of physics which govern the domain of cyberspace. Students, however,

[34] An interesting sport juxtaposing mental and physical stressors is chess boxing. See Jackob Schiller's "Chess Boxing Demands a Rare Breed of Human: The 'Nerdlete,'" Wired, 22 March 2013.

[35] We suggest the following references. (Conficker) Mark Bowden. *Worm: The First Digital World War*. Atlantic Monthly Press, 2011. (Georgia) David Hollis. "Cyberwar Case Study: Georgia 2008." Small Wars Journal, 6 January 2011. (Estonia) Vincent Joubert. "Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?" NATO Defence College, No. 76, May 2012. (Google) "Protecting Your Critical Assets: Lessons Learned from 'Operation Aurora.'" McAfee White Paper. 2010.

need not be expert code developers. Our model includes a coding proficiency test on the first day. In later phases of the course students will have to apply coding and command line skills to prepare for and conduct various mission requirements.

The course is designed to be challenging. Students must demonstrate technically competent critical thinking and decision making, under stress. Stress will come from near-unattainable time constraints, overload, and unexpected scenarios. During portions of the course, sleep will be limited to emulate the realities of cyber conflict. There will be attrition.[36] Some students will recycle and after remedial training return to attempt to eventually graduate. As a point of comparison, Ranger School has a 50.13% overall graduation rate over the past six years and 60% of all failures occur in the first four days.[37,38] We anticipate similar numbers for the Cyber Leader Course.

Evaluation will be an intrinsic part of the course. Evaluation techniques will include examinations and peer evaluations. Student leadership positions will rotate and students will undergo more intense scrutiny, including instructor observation reports, while spotlighted in these roles. These insights on student performance, while under stress, could be used to match graduates with future assignments and missions based on their style of leadership and approach toward mission accomplishment.

In Ranger School the only allowed training aide is the Ranger Handbook.[39] Such a handbook does not exist for cyber, although we suggest development of one is a worthy undertaking.[40] In the interim, we recommend minimal supporting resource materials, such as Techniques Tactics and Procedures (TTP) guidelines, a programming reference, operating system *man* pages, users' guides to uncommon technology being employed, and possibly limited Internet access.

The course could be conducted at a variety of classification levels, from Unclassified to Top Secret. Much could be accomplished using publicly available tools and capabilities without the risk of classified spillage. Mock "exercise classified" documents could be employed to ensure

[36] Attrition is an important aspect. Schools such as Ranger, Scuba, and Sapper have dual purposes. They serve as demanding training programs, but importantly they also weed out those that do not meet the high standards of the course and prevent future assignments which depend on that qualification. These courses are honored because they are extremely difficult. This difficulty introduces people to their real selves and demonstrates to each individual that they can push themselves much farther than their perceived limits. Ranger qualified leaders understand this in a physical way. We anticipate cyber leaders will face situations where mental stamina will be a key discriminator in the success of a mission. However, this will likely not be in the same sense and framework as a combat leader understands mental stamina and stresses.   If implemented, the Cyber Leader Course will require a deeper understanding of these similarities and differences.

[37] "Ranger Training Brigade." U.S. Army Maneuver Center of Excellence, Fort Benning, Georgia. http://www.benning.army.mil/infantry/rtb/, last accessed 2 September 2013.

[38] There is an advantage to most failures occurring early in the course because later failures require expending, potentially expensive, resources for longer periods of time.

[39] Clough, p. 36.

[40] A close approximation may be Jay McGuerty's *Network Field Survival Guide: The Way of the Packet*, 2012.

proper document handling. Conducting the course at the unclassified level or at a classified level authorized for foreign nationals would provide additional opportunity for participation by international allies. In contrast, conducting the course at a higher classification level would allow greater inclusion of current tactics, techniques, procedures, and capabilities.

The course would emulate the Ranger School's 61 days and be broken into four phases. When not actively preparing for, conducting, or recovering from missions, days will include combatives or weapons training, cyber operations training, and programming. During these 61 days students will work long hours, endure significant stress and occasional mental exhaustion, work seven days per week, and be prohibited from outside contact.[41,42] Despite these challenges, safety, both physical and cyber, is paramount. Instructors will provide overwatch to ensure safety violations do not occur and any incidents are dealt with quickly and effectively.

The environment of the course will be Spartan.[43] Students will be isolated from the outside world in order to better focus on the course and avoid the distractions of day-to-day life. We believe the school should be networked, and provided carefully controlled and monitored Internet access as well as air gapped networks to support training and missions. We suggest creative approaches to designing the environment. As an example, one possibility is to incorporate DEFCON's Wall of Sheep concept which displays intercepted credentials and other sensitive information captured from unsuspecting and careless attendees.[44] Another example would be to provide locks on doors to student rooms, but no keys, requiring students to pick the lock upon each entry which teaches students lock picking and the weaknesses of locks as a physical security measure.[45]

Whenever possible, training will be hands-on. For example, a student who is tasked with writing a phishing email will likely be more resistant to phishing attempts in the future or the student who is tasked to find an unauthorized cell phone in a command post using bug sweeping gear will be far less likely to bring a cell phone into a secure facility. In addition, these students, upon return to their units, will be better able to explain the reasoning behind cyber security actions to their peers, subordinates and superiors. During implementation of the course, the curriculum would be designed to foster these long-lasting principles. The course will focus intensively on cyber-related content, but will include other training such as lockpicking to help develop an adversary mindset and to illustrate relationships between physical systems and cyber systems,

[41] Similar to Ranger School we suggest a short, 8 hour, break between phases. Students may use this time to leave post, conduct errands, and make contact with families. Postal mail, and possibly electronic mail might be authorized in a carefully constrained fashion during the rest of the course.

[42] The course will involve both mental and physical activity. Sleep deprivation will also occur in certain instances as we believe this is an all but certain aspect of any conflict, including cyber conflict. However, we believe the course can be made accessible to Wounded Warriors. We will discuss this topic later in the paper.

[43] One example of a Spartan environment in the context of computing is Germany's Schloss Dagstuhl. See http://www.dagstuhl.de/. While not a perfect fit for a Cyber Leader Course, we believe study of Schloss Dagstuhl merits exploration.

[44] See George Ou's "Wall of Sheep at DEFCON Illustrates What Not to Do," ZDNet, 4 August 2006.

[45] The locks could get progressively more difficult to pick throughout the course.

combatives training for physical fitness, confidence, and self-defense, and defensive driving for stress inducement and safety in high threat environments. Training will also incorporate exercises that include an Opposing Force (OPFOR) and the OPFOR will employ real-world threat techniques, tactics, procedures, and tools whenever possible.[46]

Eligibility and Assessment

Our proposed Cyber Leader Course would be all volunteer, open to any Military Occupational Specialty (MOS), male or female, Active/Guard/Reserve, and accessible to Wounded Warriors to the greatest extent possible.[47] [48] While we anticipate students will come from cyber-related MOSs, including those from Signal, Military Intelligence (primarily SIGINT), and Electronic Warfare, we have deliberately created a wide aperture.[49] Similar to Ranger School we believe it is important to offer the opportunity to prepared and willing leaders from other Career Management Fields. While the patrolling and tactics taught in Ranger School may be directly employed by some students (based on their career specialty), others will not directly benefit from these skills, the real benefit of the school is not tactics, but to know one's self – to identify and struggle with personal weaknesses, to learn what you are really made of, and to learn to operate effectively in completely bad situations. We believe similar learning will occur for those desiring to lead in the cyber domain.

Proper preparation is essential. Prospective students prepare extensively for Ranger School, often for many years. Their activities include intense physical training, study of tactics, memorization of the Ranger Creed, study of the orders process, and heat/cold acclimatization. Before selection for formal Ranger schooling, prospective students often undergo rigorous pre-Ranger screening programs to ensure readiness. We anticipate Cyber Ranger students will go through similar processes to prepare.

Students will arrive at the Cyber Leader Course with a proscribed packing list, and identical to Ranger School's Ranger Assessment Phase (RAP), will immediately begin with a three-day assessment phase.[50] This phase will front-load a series of demanding tasks that will earn

[46] One natural source of experience and insights into cyber opposing forces is Army Cyber Command's World Class Cyber OPFOR. See Lieutenant General Rhett Hernandez, "Statement Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities, Digital Warriors: Improving Military Capabilities for Cyber Operations," Second Session, 112th Congress, 25 July 2012.

[47] We believe the Cyber Leader Course will also be a powerful recruiting and reenlistment tool, as are Ranger School and the Special Forces Q course.

[48] Historically the Army has placed great emphasis on physical fitness, but due to the number of wounded warriors from the wars in Iraq and Afghanistan we have seen significant emphasis on accommodating physical disabilities. In 2013, for example, an Army amputee completed the Army's 10 day Air Assault school. See Kristin Hall's "Army Amputee Completes Air Assault School," Associated Press, 29 April 2013. We envision the Cyber Leader Course to be likewise able to accommodate wounded warriors.

[49] In addition, the diversity of backgrounds brought by those outside of cyber branches, but who are equally prepared and motivated, will help enrich the content of the course.

[50] The students will undergo an inspection looking for contraband items, particularly unauthorized electronics and software. While suggesting a full packing list for the Cyber Leader Course is beyond the scope of this article, we suggest reviewing the Ranger School's packing list as a starting point. http://www.benning.army.mil/infantry/rtb/content/pdf/packinglist.pdf, last accessed 9 September 2013.

individuals the right to continue training. A major component of RAP is the 26 task "Ranger Stakes." The Cyber Leader Stakes will contain equivalent cyber-related tasks.[51] Knowledge of these tasks will directly affect the leadership grades and peer evaluations of each student. Cyber Leader candidates will need a base of knowledge of these tasks in order to be an asset, and not a liability, to their team during missions.[52]

Perhaps the most challenging part of the Cyber Leader Course's assessment phase will be a timed programming test.[53] The student would be required to complete a series of moderately complex programming challenges using a specified set of programming languages.[54] The Cyber Leader Course could, optionally, make available historical exam questions to aid prospective students' preparation. As with Ranger School, failing the coding exam or any of the other tasks required during the assessment phase of the Cyber Leader Course shows poor preparation.

Individual units, particularly those that have missions focused on cyberspace operations, may choose to conduct in-house pre-Cyber Leader Course training and selection competitions before investing a coveted Cyber Leader Course slot. Such activities will help pre-screen prospective students and filter those that are not prepared, ready, or capable. At a minimum, incoming students must possess a memorandum from their home station commander attesting to their Cyber Leader Stakes proficiency.[55]

[51] A detailed listing of Cyber Ranger Stakes tasks is also beyond the scope of this paper and is complicated by a shortage of mature Army doctrine regarding cyberspace operations. That being said, we suggest a suite of tasks that demonstrate knowledge of networks, operating systems, a typing speed test (perhaps 40 WPM minimum), tool use (such as established tools built into the Kali Linux distribution, Virtual Machine usage, the Windows and Linux command line interface, and a penetration testing methodology (such as that provided by the *Hacking Exposed* series of books). The tasks, conditions, and standards associated with these skills would be published and allow students to better prepare. However, these are just starting points, and we recommend review of the Knowledge Skills and Abilities (KSAs) being developed across each of the military services as well as those developed by industry and government to refine and vet appropriate tasks.

[52] This text is based upon guidance provided by Ranger School to Ranger aspirants who are warned that "Knowledge of the 26 Ranger Common Tasks will directly affect the Patrolling grades and Peer Evaluation of each Ranger Student. Ranger candidates need a base knowledge of these tasks in order to be an asset to your squad and platoon while patrolling. Do not become a liability to your squad or platoon because you could not perform one of these common tasks." See the Ranger Training Brigade's "Ranger School Preparation" document. http://www.benning.army.mil/infantry/rtb/content/PDF/Ranger%20School%20Prep.pdf, last accessed 9 September 2013.

[53] We considered not including such a test, but we chose not to lower the standard. Cyber leaders, including officers, should be able to code even if they aren't writing professional grade exploits. For those that believe they cannot code, a quote from Bronson Clough comes to mind, "I've heard so many Soldiers in the Army say to me, 'but sir, I'm not a runner.' Guess what? Stop eating cheeseburgers and start running and now you ARE a runner." p. 55. In the case of the Cyber Leader Course our variant would be, "I've heard so many Soldiers in the Army say to me, 'but sir, I'm not a coder.' Guess what? Pick up a Python manual and start coding and now you ARE a coder."

[54] We suggest Python, Perl, JavaScript, and C.

[55] A commander's memo attesting to Ranger Stakes proficiency is required for Ranger School, Clough, p. 66. Students will also be required to bring a memorandum signed by their commander stating that the soldier has a current Army Physical Fitness Test and meets height/weight standards. If the course

The combined goal of both the pre-screening and assessment phases is to motivate and inspire prospective students to extensively prepare and only allow the best candidates to move forward into the course.

Missions

Military “patrol-sized”[56] missions are used as the cornerstone vehicle for leader development in Ranger School. We believe the same mission-based approach will work equally well in the Cyber Leader Course to stress, teach, inspire, train, motivate, and build confidence. During each of the four phases we envision missions of increasing complexity.

Phase I - Individual
Phase II - Small co-located teams
Phase III - Distributed cyber teams
Phase IV - Distributed cyber and kinetic teams[57]

The missions will contain offensive, defensive, and analytic components and are carefully crafted to accomplish specific learning objectives. Some missions will be conducted remotely, others will require direct action by the students, still others will require integration of cyber effects into kinetic operations. The missions and training we suggest here are unclassified examples only. Each is well known to the commercial penetration testing community. Additionally, these missions and training examples are chosen for their educational and illustrative value and are not chosen because the U.S. Government condones such activities in practice. Classified examples are beyond the scope of this paper, but we acknowledge that a Cyber Leader Course could be modified to include classified content, as desired.

Not every student will participate in every mission we suggest. Each iteration of the course will be different. However, the goal is the same - stress, evaluate, and develop the students under a full range of mission sets. Some missions are deliberately designed to include ethical components that will force students to make important decisions regarding collateral effects,[58] ethical behavior, and the law of war. Missions will employ a standardized model, including a planning phase, execution phase, assessment phase, and an after action review, all incorporating appropriate aspects of the Military Decision Making Process (MDMP) and a

evolves to include certifications or other training as an entry requirement, students will need to bring appropriate documentation to prove successful completion.

[56] Ranger School patrols vary in size from squad-sized (approximately 10 persons) to platoon-sized (approximately 35 persons). In the Cyber Leader Course, we envision teams that will vary in size from 4 to 10 persons.

[57] These missions would consist of cyber students creating kinetic-effects on the battlefield and/or conducting cyberspace only effects in synchronization with kinetic battlefield operations.

[58] See Fanelli’s “A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict,” CyCon 2012 and Raymond’s “A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons,” CyCon 2013 for detailed discussions of collateral effects in the context of cyber operations.

standardized Operation Order format, as well as senior leader briefings.[59,60] As in Ranger School, training will be intermixed with missions throughout the Cyber Leader Course. In each Phase, students will be provided training opportunities which complement their previous experience, both of which students will need to draw upon as mission complexity increases. Students will also receive mission-specific training as necessary, such as a class teaching students to use an unfamiliar piece of gear required for a given mission. Some missions will also include "reachback" support from notional strategic assets for technologies and techniques that are out of scope of the course, such as advanced level reverse engineering. Appendices A through D provide overviews of representative training by phase.[61] Appendix E suggests example missions.

Graduation Requirements

To graduate, students must successfully pass all peer reviews, all qualification examinations, and must receive a "GO" on one mission leadership position per phase and a "GO" on at least 50% of the mission leadership positions held during the course.[62] Students who are marginally successful will receive an opportunity to "recycle," and join a later class to redo a given phase, continuing forward with that new cohort.[63] Ethical failures and other violations will be reviewed on a case-by-case basis, and may result in removal from the course or recycling to a later cohort. Instructors may issue spot reports, both positive and negative, and the accumulation of too many negative spot reports can result in removal from the course. Positive spot reports, on the other hand, combined with strong performance in other aspects of the course will put the student in the running for "honor graduate."

Ethics

An absolutely critical part of developing elite level cyber warfare leaders is unquestionable ethics. The course teaches dangerous skills, not unlike Ranger School and other military training. We are effectively weaponizing individuals; with this implication comes great responsibility. Cyber skills may be employed surreptitiously, have global implications, and can devastate the intended quarry. Safety briefings and zero toleration for misconduct must be

[59] Senior leader briefings will include briefings to non-technical audiences. The ability to communicate technical subjects, including non-obvious potential effects and limitations, is an important learning objective of the course.

[60] See Doctrine Man for a critical review of the MDMP, https://www.youtube.com/watch?v=uWtwmlmPSOY

[61] For comparison, we suggest review of the Ranger School Program of Instruction (POI) available here http://www.benning.army.mil/infantry/rtb/content/PDF/Ranger%20School%20web11.pdf, last accessed 10 September 2013. Ranger School also makes extensive use of Battle Drills, "a collective action rapidly executed without applying a deliberate decision-making process" (FM 25-101). We currently omit cyber battle drills from our Cyber Leader Course model as present doctrine is still maturing.

[62] Graduation requirements for Ranger School include passing all Ranger Assessment tasks: Ranger Physical Assessment, Combat Water Survival Assessment, Land Navigation, 12 mile foot march, 50% "GO" rate or better on patrols, 60% or better on peer evaluations, and no more than three major [negative] spot reports in any phase; no more than eight for the course. See http://www.benning.army.mil/infantry/rtb/content/PDF/Ranger%20School%20web11.pdf

[63] Ranger school has a board at the end of each phase to determine which "at risk" students will advance and which will be recycled.

integral parts of the course, and be buttressed by an honor code, a legally reviewed conduct pledge, and safety waiver.[64] Cyber Leader Course Instructors must serve as role models who exemplify appropriate behavior. Award of the Cyber Tab is a lifelong responsibility, not a guarantee. Like the Ranger Tab which can be revoked when the "individual has exhibited a pattern of behavior, expertise, or duty performance that is inconsistent with the expectations of the Army," our proposed Cyber Tab would include similar strictures for ethical, behavioral, expertise, or duty performance lapses.[65,66]

Implementation

While full implementation details are well beyond the scope of this paper, this section provides a high-level overview of key implementation factors, including student throughput, instructor cadre, and facilities.

Initial Student Throughput

Initially we suggest quarterly offerings of the course with no less than 25 students and no more than 50. Recall that we anticipate an attrition rate of approximately 50%, so these numbers would result in 12-25 graduates per iteration and 48-100 graduates during the initial year of the program. However, over time, the number of students can be increased as additional capacity is required, eventually reaching a steady state depending on the needs of the Army.

Bootstrapping the Cadre

The cadre of Ranger School is composed of long-serving and seasoned Ranger professionals who possess years of operational experience in the Ranger Regiment and other elite military organizations. We believe the Cyber Leader Course should seek a similar end state. However, seasoned uniformed cyber professionals are in short supply today, those that do exist are decisively engaged in operations or constructing new organizations, creating doctrine, and other high priority tasks. It is unlikely that operational forces could, at least initially, spare an entire complement of their best talent to staff and run a Cyber Leader Course.[67] We recommend an iterative approach, where core leadership is drawn from the limited pool of uniformed cyber

[64] Thomas Cook, Gregory Conti, and David Raymond. "When Good Ninjas Turn Bad: Preventing Your Students from Becoming the Threat." Colloquium for Information Systems Security Education, June 2012.

[65] Military Awards, Army Regulation 600-8-22, Section 1-31, p. 8.

[66] We note that ethical codes of conduct are already a part of flagship industry certifications including Certified Ethical Hacker (CEH), http://www.eccouncil.org/Support/code-of-ethics, and Certified Information Systems Security Professional (CISSP), https://www.isc2.org/ethics/Default.aspx.

[67] The United States Army dedicates significant resources to support Ranger School including the Airborne and Ranger Training Brigade's 4th Ranger Training Battalion (Fort Benning, GA), 5th Ranger Training Battalion (Dahlonega, GA), and 6th Ranger Training Battalion (Eglin AFB, FL). See the Airborne and Ranger Training Brigade's homepage for more information, http://www.benning.army.mil/infantry/RTB/, last accessed 20 December 2013. The Ranger Regiment has about 2,000 personnel (Clough, p. 33). We note that this number roughly parallels the emerging Cyber teams being created by U.S. Cyber Command, see http://www.defense.gov/news/newsarticle.aspx?id=120854. The substantial dedication of resources to Ranger School combined with the size of the operational force may indicate a requirement to create a Cyber Leader Course Training Battalion. When attempting to determine an appropriate number of instructors a useful point of comparison is the Ranger student to Ranger Instructor ratio which is approximately 9:1, see Clough, p. 38.

experts, augmented with less experienced uniformed personnel, and supported by high-end civilian expertise from industry. We do not envision this situation as the desired end state, only a required initial condition. The enduring viability of the school depends on students being trained by the elite-level Soldiers they aspire to be. The Army must "own" this school. Over time we will grow the sufficient complement of cyber leaders required for the course to be self-sufficient.[68] In addition to instructors, we recommend including a psychologist to monitor student stress levels, help construct an appropriately balanced training experience, and analyze the strengths and weaknesses of students.[69]

Infrastructure

As we envision the Cyber Leader Course it would include MOUT-like physical training areas, classroom and lab environments, barracks-areas, dining facilities, and supporting administrative areas, among others. Importantly, the school would also require significant information technology and networking support. This infrastructure will require various types of networks (unclassified and classified, wired, wireless, and air-gapped, as appropriate[70]) end-user workstations, specialized devices (e.g. a SCADA system), and back-end servers. Virtualized environments, such as VMware's vSphere or Citrix's XenServer, will likely be necessary to support development of training and scenario packages, prevent the spread of malicious software, and allow easy resetting of the training environment. Depending on the ultimate design of the program, other facilities such as a gymnasium, shooting range, and a Makerspace/Hardware lab[71] may be required. The school itself could be located at a single DoD installation or distributed across multiple installations.

Utilization

The intent of the Cyber Leader Course is to initially fill critical the shortfall of competent cyber leaders across the Army, and to provide a long-term engine to continue generating such talent into the future. Proper utilization of graduates is important, lest their desperately needed but costly and rare skills be wasted.[72] We envision utilization of graduates in "line" cyber units (those existing as SIGINT, Signal, and EW units today), Cyber Electro-Magnetic Activity

[68] Of course, none of the initial Cyber Leader Course Instructors will be graduates of the school. One potential solution is that the first iteration of the course is for hand-picked instructors only, who rotate into and out of leadership and student roles, but importantly, complete all graduation requirements. We note that prior to the creation of Ranger School, initial awards of the Ranger Tab were authorized to "Any person who was awarded the Combat Infantryman Badge while serving during World War II as a member of a Ranger Battalion (1st-6th inclusive) or in the 5307th Composite Unit (Provisional) (Merrill's Marauders)." See Army Regulation 600-8-22, Military Awards, 24 June 2013, Section 8-48.

[69] Profiling students in such a fashion would allow operational leaders to better assign personnel against given missions, after graduation.

[70] Existing DoD cyber ranges could be leveraged to support training. We note also that opposing forces (OPFOR) in some of training events need not be physically co-located with the school, and operations may be conducted remotely over the network.

[71] See http://en.wikipedia.org/wiki/Hackerspace for more information on Makerspaces.

[72] Proper utilization will also help increase retention and recruiting. See Tim Kane's "Why Our Best Officers Are Leaving," The Atlantic, 4 January 2011 for a relevant discussion.

(CEMA) cells in Brigades and Divisions, the Army's Cyber Brigade, the emerging Cyber Mission Force, and the World Class Cyber OPFOR.[73]

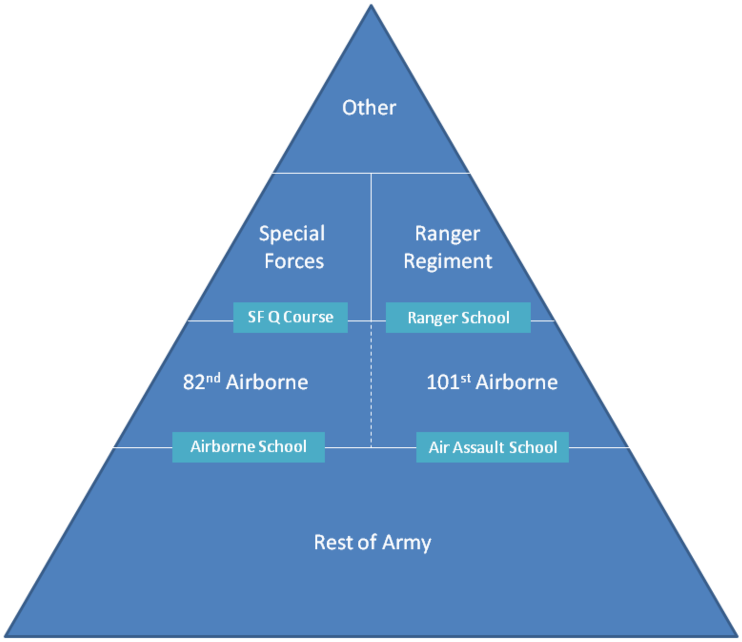

Figure 5: The Army uses Ranger, Airborne, Air Assault, and Special Forces schools as gateways to elite units and to develop leaders that are seeded throughout the force, playing a major role in uplifting the entire Army. We believe there is a cyber analog and a Cyber Leader Course can play an instrumental part.

Cyber Tab

Successful completion of the course would authorize the graduate to wear the Cyber tab, see Figure 1, on his or her uniform. Such an authorization is important to the recognition of cyber warriors in the Army. Currently the Army lacks any visible recognition for cyber warfare expertise. There are currently three primary tabs authorized for wear by the U.S. Army in recognition of individual skills, the Ranger Tab, the Special Forces Tab, and the Sapper Tab. Each tab is earned by completing its respective school. In addition, the Army also authorizes the President's Hundred Tab for exceptional performance in marksmanship. By creating a cyber tab, backed with a rigorous and respected qualification program, the Army will make a major step forward in professionalizing its cyber leader development.

Conclusions and Future Work

Creation of a Cyber Leader Course is not without its challenges, particularly in an era of declining resources. Perhaps the greatest challenge is developing the school amidst a kinetic warfighting culture in the Army, a culture that may not initially appreciate the benefits a Cyber Leader Course provides. To overcome this, the school must set the conditions for the success of its graduates, buttressed by support of high-level Army leadership. The course will derive its

[73] Tina Miles. "Army Activates First-of-its-Kind Cyber Brigade." Army.mil, 9 December 2011.

reputation from the skills and contributions of its graduates. Similarly, the concept of a Cyber Leader Course may prove challenging for some leaders. However, we must seek to grow leaders for the future Army who are better than us, the authors included. Growing people better than us isn't a threat, it is our responsibility.

Ranger School is largely stable and well refined; it changes only slowly over time. The Cyber Leader Course faces the challenge of maintaining currency, particularly in the face of rapidly changing technology and threat tactics, which would force the course to constantly evolve. We believe, however, that the Cyber Leader Course should focus on underlying and enduring principles and not constantly incorporating the latest tools. It must be a learning organization that continuously analyzes itself and its graduates to seek improvement.[74] The cost of a Cyber Leader Course cannot be discounted, but we believe that it can be implemented at varying levels of resource requirements. The Cyber Leader Course could also be created as a Joint school for cost effectiveness.

There is a need for an elite training program and proving ground for cyber leaders. This paper provides a plan for implementing a rigorous 61 day Cyber Leader Course designed to fill the current shortfall of elite cyber leaders within the Army. However, even the best training programs are for naught without a cyber career path that rewards excellence and offers opportunity from Private to General Officer. Today, a cyber career path in the Army remains an open problem, but this need not always be the case. Work is ongoing to create such a path, including the transformation of the Signal Center of Excellence at Fort Gordon into the Cyber Center of Excellence.[75] A likely aspect of a cyber career path is the creation of a branch in the Army, akin to Armor, Infantry, Signal, and Military Intelligence. We anticipate such a branch would benefit from a Special Forces-like model.[76] The cyber force needs to stay lean, small,[77] elite, and progressive. Somehow we have to find a way to check the bureaucracy that hinders the effectiveness of the rest of the military and will undoubtedly impact the kind of culture that would be attractive to the best and brightest in this field.

The creation of a Cyber Leader Course, or its equivalent, is both necessary and possible. However, reputation must be earned; no amount of marketing will alter this fact. Only through the quality and rigor of the course, and the contributions and dedication of Cyber Leader Course graduates, will accolades be won. Such accolades will be doubly difficult as the larger Army

[74] One group that merits further exploration to inform the Cyber Leader Course are the people who handle incident response at large multinational corporations. These people have to deal with intense cyber-related crises, and it may be possible to identify characteristics that make leaders better than another in these situations and then work backward, finding ways to develop the core competencies and qualities of successful cyber leaders.

[75] Wesley Brown. "Restructuring Plan to Make Fort Gordon Center of U.S. Cyberspace Training." The Augusta Chronicle, 29 July 2013.

[76] Todd Arnold, Rob Harrison, and Gregory Conti. "Professionalizing the Army's Cyber Officer Force." Army Cyber Center Report, 23 November 2013, Vol. 1337, No. 2.

[77] We deliberately do not quantify "small," but believe the cyber force needs to be small enough to remain agile, avoid rigid hierarchies and soul-stealing bureaucracy, while being large-enough to accomplish the necessary missions.

culture comes to grips with growth of cyber as a core operational mission area, one that requires a new community of cyber operators.[78]

[78] Gregory Conti and Jen Easterly. “Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture.” Small Wars Journal, 29 July 2010.

Author Biographies

Colonel Gregory Conti is a Military Intelligence Officer and Director of the Army Cyber Center at West Point. He holds a Ph.D. from the Georgia Institute of Technology, an M.S. from Johns Hopkins University and a B.S. from West Point, all in computer science. He has served as a senior adviser in the U.S. Cyber Command Commander's Action Group (CAG), as Officer in Charge of a deployed U.S. Cyber Command Expeditionary Cyber Support Element, and co-developed U.S. Cyber Command's Joint Advanced Cyber Warfare Course. He served in the Persian Gulf War and in Operation Iraqi Freedom.

First Lieutenant Michael Weigand is a Ranger qualified, Airborne, Expert Infantryman currently serving as the executive officer of HHC, 1-12 CAV, a Combined Arms Battalion. He holds a B.S. from the United States Military Academy in Computer Science. Previously he interned as an adviser for the Commanding General, U.S. Army Cyber Command, and has participated in internships with DARPA, USC Institute for Creative Technologies, and iRobot.

Ed Skoudis is the founder of Counter Hack, an innovative organization that designs, builds, and operates popular infosec challenges and simulations including CyberCity, NetWars, Cyber Quests, and Cyber Foundations. As director of the CyberCity project, Ed oversees the development of missions which help train cyber warriors in how to defend the kinetic assets of a physical, miniaturized city. Ed's expertise includes hacker attacks and defenses, incident response, and malware analysis, with over fifteen years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (Security 560) and incident response (Security 504), helping over three thousand information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments and penetration tests; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and Intrusion Prevention System research; and responded to computer attacks for clients in government, military, financial, high technology, healthcare, and other industries. Previously, Ed served as a security consultant with InGuardians, International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips and penetration testing.

Lieutenant Colonel David Raymond is an Armor Officer and is currently serving as an Associate Professor in the Army Cyber Institute at West Point. He holds a Ph.D. in Computer Engineering from Virginia Tech, a Master's Degree in Computer Science from Duke University, and a Bachelor's Degree in Computer Science from the United States Military Academy. LTC Raymond holds CISSP and Certified Ethical Hacker (C|EH) certifications and teaches senior-level computer networking and cyber security courses at West Point. He conducts research on information assurance, cyber security, and online privacy.

Colonel Thomas Cook is an Armor Officer and Chief of Operations of the Army Cyber Institute at West Point. He holds a BS in History from Brockport State University, an MS in Industrial

Engineering from the University of Louisville, and an MS in Computer Science and a PhD in Software Engineering from the Naval Postgraduate School.

Major Todd Arnold is an FA24 and former Signal Corps officer. He is a research scientist in West Point’s Cyber Research Center and an Assistant Professor in the Department of Electrical Engineering and Computer Science (EE&CS). He holds an M.S. from the Pennsylvania State University and a B.S. from West Point, both in Computer Science. His previous assignments include two tours in Operation Iraqi Freedom (OIF) with the 22d Signal Brigade, serving in the G33 of Army Cyber Command, and developing, testing, and analyzing CNO capabilities in support of current and future contingency operations for NSA and USCYBERCOM.

Dr. Daniel "Rags" Ragsdale is currently a DARPA Program Manager. Before joining DARPA in 2011 he served for more than a decade at West Point where he held a variety of supervisory roles, culminating with service as Vice Dean for Education. In this capacity, Dr. Ragsdale was the Strategic Planner and Principal Deputy to the Dean of the Academic Board. During his 30-year Army career, Colonel Ragsdale served in leadership roles in a wide array of research and development settings. His operational assignments included combat deployments in support of Operations Urgent Fury (Grenada), Enduring Freedom (Afghanistan), and Iraqi Freedom (Iraq).

The views expressed in this article are those of the authors and do not reflect the official policy or position of West Point, the Department of the Army, Army Cyber Command, U.S. Cyber Command, *the National Security Agency, the Defense Advanced Research Projects Agency, or the United States Government.*

Appendix A: Overview of Suggested Blocks of Instruction for Phase I

Topic	**Description**
Course Introduction	Course overview and motivational speech by senior leader
Safety Briefing	Detailed guidance on proper cyber and physical safety standards for course.
Google Hacking	Learn open source reconnaissance techniques
Electromagnetic Spectrum	Overview of the electromagnetic spectrum, devices that typically occupy each band, and common wireless protocols
Cyber Leaders Reaction Course	A course based on the Army's Leaders Reaction Course, but tailored for the cyber environment
Antenna theory and RF propagation	How antenna design impacts RF propagation, includes a hands on lab where students make high gain antennas for later use in course
Lock picking	The basics of lock design and lock picking, includes coverage of key fabrication
Computer Forensics	Overview of the computer forensics field, includes hands-on use of common forensics tools
Social Engineering	Coverage of common social engineering strategies in order to build resistance in students.[79]
3D Printing and Fabrication	Teaches students to design and build custom items
Botnets	Detailed coverage of how botnets are built, controlled, employed, and attacked
Cyber Threat	Covers the spectrum of threat actors, from lone malicious hackers to nation-states, includes the insider threat
Electronic warfare	Students learn jamming and spoofing techniques, as well as how to employ a jammer
Personal Device Security	How to harden personal electronic devices
Physical Security	Techniques for employing and defeating physical security measures
Space Systems	How space systems work, includes coverage of vulnerabilities
Radio Systems	Applied knowledge of how analog and digital radio systems work
Cyber Mission Command and Control	Describes techniques for leading cyber missions, including across distributed locations

[79] See Christopher Hadnagy and Paul Wilson, *Social Engineering: The Art of Human Hacking*, Wiley, 2010 and Kevin Mitnick, *The Art of Deception: Controlling the Human Element of Security*, Wiley, 2003.

Networks	Intermediate level wired and wireless network operation
Employing Battlefield Robotics	Includes fielding and use of a ground robot and drone
Employing a Battlefield Sensor	Includes coverage of strengths and weaknesses of various sensors.
Web Servers	Advanced server configuration and web attacks
Doctrine	Overview of key tactical, operational, and strategic-level doctrine governing cyber operations.
Optimizing the Operations Center	Covers vetted designs for operations centers, including task flow, team communications, and ergonomics for optimal mission accomplishment.
Exploit Creation	Basic level exploit creation
Reverse Engineering	Basic level reverse engineering techniques
Exam	Students must pass a written and oral exam to complete the phase.

Appendix B: Overview of Suggested Blocks of Instruction for Phase II

Topic	**Description**
Cyber Operational Preparation of the Environment	Covers functions within cyberspace conducted to plan and prepare for potential military operations, including identifying data, system/network configurations, and physical structures associated with the network or system (such as software, ports, assigned network address ranges) for the purpose of determining system vulnerabilities and actions taken to assure future access and/or control of the system, network, or data.[80]
Maneuver in Cyberspace	Cyberspace is an operational domain and individuals and units maneuver within it. This block covers the latest in emerging thought on the subject, including key terrain, avenues of approach, and attack surface analysis.[81]
Network Mapping	Tools and strategies for mapping the ever changing cyberspace environment, particularly in the context of a constrained geographic location.
Spectrum Management	Techniques for allowing shared access to the RF spectrum. Could be expanded to include discussion of shared Internet networks which are used for both friendly communications, and potentially, warfare.
Cyber Military Decision Making Process	The Cyber MDMP is a variant of the Military Decision Making Process which includes seven basic steps: receipt of mission, mission analysis, course of action (COA) development, COA analysis, COA comparison, COA approval, and orders production.
Cyber Troop Leading Procedures	This block of instruction covers a variant of the Army's Troop Leading Procedures modified for cyber operations: receive the mission, issue a warning order, make a tentative plan, start necessary movement, reconnoiter, complete the plan, issue the complete order, and supervise.
Special Topics in Operational Cyber Mission Planning	Includes intelligence gain/loss, deconflicting operations with other activities, requesting intelligence, and integrating cyber effects into kinetic operations
Cyber Call for Fire Process	Students learn the current process for request cyber effects from a higher headquarters and gain an understanding of what it takes to implement those effects.[82]

[80] See Vice Chairman of the Joint Chiefs of Staff memorandum “Joint Terminology for Cyberspace Operations,” available online at http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf

[81] See Scott Applegate, “The Principle of Maneuver in Cyber Operations,” NATO Conference on Cyber Conflict, 2012.

[82] See John Reed. "Army and Marines Creating systems for Cyber Fire Support." Foreign Affairs, 10 September 2012.

Strategic Intelligence Resources	Coverage of the SIGINT, IMINT, HUMINT and other sources of intelligence that may be used to support tactical operations.
Battlefield Forensics Procedures	Teaches a validated process for the handling of electronics and storage media encountered on the battlefield.
System, Server, and Network hardening	Techniques and best practices for making systems, servers, and networks resistant to attack. Taught in multiple operating systems.
Metadata Analysis	Studies ways meta-data is stored in electronic documents. Will learn to employ open source tools such as FOCA.[83]
Tamper Resistance Techniques	Students will learn about the strengths and weaknesses of various tamper resistance techniques and take part in a “tamper-evident” competition similar to that of the DEFCON hacker conference.[84]
Magnetic Barcode Readers, Smart Cards and Related Technologies	Provides coverage of the strengths and vulnerabilities of barcode readers, smart cards, RFID, and Near Field Communication (NFC).
Electronic Locks	Covers strengths and weaknesses of electronic locks.
Supply Chain Security	Students will gain heighten awareness of security risks throughout the supply chain.
Penetration Testing and Red Teaming	Students will learn and employ a framework for conducting penetration testing and red teaming using open source tools.
Hardware Hacking	A hands-on experience to learn how to reverse engineer hardware and make it behave in ways the designer did not intend.[85]
Electronics Lab	Students learn the basics of reading schematics and will assemble an electronic device of moderate complexity, such as a TV-B-Gone.[86]
Wired and Wireless Network Sniffer	Covers techniques for intercepting wired and wireless networks as well as related analysis using open source tools.
Legal Authorities / Rules of Engagement	Legal limitations on what cyber operations are authorized.
Rules of Evidence	Covers chain of custody and other legal issues surrounding usage of electronic evidence in legal proceedings.
Influence Operations	Students receive intermediate level instruction in information and influence operations, particularly in the context of electronic

[83] “Employ the FOCA Tool as a Metadata Extractor,” Video, Search Security, 24 May 2012. FOCA is available for download here, http://www.informatica64.com/foca/

[84] Datagram, “Introduction to Tamper Evident Devices,” DEFCON 19, 2011.

[85] See Joe Grand’s Hardware Hacking Training at http://www.grandideastudio.com/portfolio/hardware-hacking-training/, last accessed 10 September 2013.

[86] See the TV-B-Gone product page https://www.tvbgone.com/cfe_tvbg_main.php, last accessed 10 September 2013.

	media.
Exploit Creation	Intermediate level exploit creation
Reverse Engineering	Intermediate level reverse engineering techniques
Exam	Students must pass a written and oral exam to complete the phase.

Appendix C: Overview of Suggested Blocks of Instruction for Phase III

Topic	**Description**
Electronic Privacy and Civil Liberties	The importance of privacy and civil liberties to the American democracy.
Hardware Enhanced Processing	Students learn techniques for speeding up demanding processing tasks using Application Specific Integrated Circuits (ASICs), Field Programmable Gate Arrays (FPGAs), and Graphics Processing Units (GPUs).
Advanced Forensics Techniques	Covers more complex techniques for conducting forensic analysis, such as dumping and analyzing memory, cold boot attacks, rebuilding hard drives (board level replacement), advanced hard drive analysis tools, and hot swapping utility power to a UPS to prevent destruction of volatile memory.
Enterprise Operations Overview	Studies how military and civilian enterprise operations are organized and how to best integrate military support in time of crisis.
Trojan Horse Software	Students learn various types of trojan horses and will experiment with the capabilities of various applications in the wild.
Cyber Battlefield Deception	Techniques for deceiving threat actors through cyber means.[87]
Fabricating a Wireless Sniffing Toaster	Create an innocuous appearing device that sniffs wireless traffic, optionally could spoof wireless access points.[88]
Man In The Middle Attacks	This block of instruction covers a range of man in the middle attacks using open source tools.[89]
Domain Name System	Covers the operation and vulnerabilities of DNS and includes hands-on work with open source DNS attack tools.
AntiVirus Evasion	Students will study the effectiveness of anti-virus detection techniques and adversary countermeasures.[90]

[87] See Sean Bodmer, Max Kilger, Gregory Carpenter, and Jade Jones, *Reverse Deception: Organized Cyber Threat Counter Exploitation,"* McGraw-Hill Osborne Media, 2012.
[88] See the WiFi Pineapple, https://wifipineapple.com/, and range of offerings provided by Pwnie Express, http://pwnieexpress.com/.
[89] For example see, sslsniff at http://www.thoughtcrime.org/software.html, last accessed 11 September 2013.
[90] For one example see, Matthew Humphries. "Defcon Race To Zero Contest Angers Antivirus Vendors." Geek.com, 29 April 2008.

Shredded Paper Reconstruction	Covers the strengths and weaknesses of shredder technology. Students will employ publicly available shredder reconstruction tools.[91]
Fuzzing	Students learn the strengths and weaknesses of fuzzing and will participate in a hands-on lab using open source software.
Cryptography	Students are provided an overview of popular cryptographic techniques in use as well as common crypto system failings
Hash Cracking Lab	Students attempt to crack password hashes using probabilistic techniques, Rainbow Tables, and hardware acceleration.
Anonymity Online	Students learn the difficulties of remaining anonymous online.
Defensive Driving	Students learn high speed driving techniques for their personal safety in high risk environments.
Mobile Device Security	Provides an overview of recent mobile device vulnerability topics.
Advanced Social Engineering	Hands-on practice employing social engineering strategies in a variety of contexts.
Distributed Denial of Service Attacks (DDOS)	Students will learn how DDOS attacks occur and mitigation techniques.
Advanced Eavesdropping Techniques	Will survey advanced surveillance techniques, such as laser microphones.[92]
Drone Lab	Covers construction of a drone, battlefield robot, and a custom sensor.
Advanced Exploit Creation	Advanced exploit creation
Advanced Reverse Engineering	Students will learn intermediate level static and dynamic software reverse engineering techniques, including code obfuscation, packing, and anti-debugging
Exam	Students must pass a written and oral exam to complete the phase.

[91] See the DARPA Shredder Challenge http://archive.darpa.mil/shredderchallenge/

[92] See Wikipedia's article on laser microphones for an overview, https://en.wikipedia.org/wiki/Laser_microphone.

Appendix D: Overview of Suggested Blocks of Instruction for Phase IV

Topic	**Description**
Emerging Technologies	Provides a survey of important emerging technologies including quantum computing, neural interfaces, human implants, datamining, augmented reality, and fully homomorphic encryption.
Hacker Community	Students will learn and debate the differences between white hat, gray hat, and black hat hackers.[93]
Medical Device Security	Students learn of the security risks associated with medical devices.[94]
Disruptive Technologies	Explores the way new technologies can disrupt the status quo in both positive and negative ways.[95]
Media Relations	How to best interact with the media and why “no comment” isn’t often the best answer.
OPSEC for the Cyber Warrior	Discusses the implications and pitfalls of disclosing personal information in a digital age.
SCADA and Industrial Control Systems (ICS)	In depth study of SCADA and ICS system security.
Satellite Systems Security	Study of satellite systems and their vulnerabilities.[96]
Vehicular and Transportation System Security	Covers security threats to transportation networks and individual vehicles.
Countering Anti-Tampering Hardware and Software	Criminals and malware writers will sometimes leave behind traps for the unwary. This block of instruction covers common traps and suggests techniques for disabling or bypassing them.
Magic and Mischief	This block studies the arts of magic,[97] con games,[98] and pickpocketing to derive lessons

[93] Three useful documentaries are Hackers Are People Too (http://www.imdb.com/title/tt1279942/), DEFCON: The Documentary (http://www.imdb.com/title/tt3010462/), and We Are Legion: The Story of the Hactivists (http://www.imdb.com/title/tt2177843/).

[94] See Jordan Robertson. “Hacker Shows Off Lethal Attack By Controlling Wireless Medical Device.” Bloomberg, 29 February 2012.

[95] See the Disruptive Technologies course of COL Barry Shoop, Department of Electrical Engineering and Computer Science, West Point.

[96] See Jan Kallberg, "Designer Satellite collisions from Covert Cyber War," Strategic Studies Quarterly, Spring 2012, p. 124.

	learned for security.
Graduation	Graduation ceremony attended by family and friends, speech given by senior leader

[97] Bruce Barnett, “Deceptive Hacking: How Misdirection Can Be Used to Steal Information Without Being Detected,” Defcon 19, 2011.
[98] Cough, “Confidence Game Theater,” Defcon 11, 2009.

Appendix E: Representative Cyber Leader Course Missions

Mission	Description
Open Source Recon	An installation commander invites the team to analyze the posture of their installation in cyberspace, particularly in terms of data on social networking sites and on publicly accessible servers. The team must brief the commander on what they find. A possible extension of the mission is to attempt to bypass the knowledge based authentication of a notional senior leader.[99]
Cell Phone in the Command Center	An organization has been lax in enforcing its no cell phone policy. The team uses bug sniffing gear to find the unauthorized cell phones. Alternatively, the team could place a bug in the command center and attempt to avoid detection.
Free Lunch	The vending machine in the lobby is taking everyone's lunch money. The team must strike back.
Thumb Drive in the Parking Lot	An employee finds a thumb drive in the parking lot. The team must examine the drive and find out what it does. In an alternative mission, the team could create a malicious thumb drive and leave it in the adversary's parking lot.
Protective Bubble	The military is fielding a new precision jammer that provides a protective bubble for troops. The team must learn how to use it and put the new system through its paces.[100]
Data Spill	A commercial social networking site suffered a massive data spill. The team must assess the damage to the military.
Wireless Survey and Exploitation	The team must penetrate an adversary's wireless network. Techniques could include war driving, war flying, wireless access point spoofing, among others.
Accessibility	The team must gain access to a denied network.
Build and Defend a Network	Team must build a network, provide proscribed services (such as email, chat, and web), lock it

[99] For a real-world example, see Kim Zetter's "Palin E-Mail Hacker Says It Was Easy," Wired Threat Level Blog, 18 September 2008

[100] Joe Gould's article "New Gear Puts Electronic Warfare on the Offensive," Army Times, 30 October 2013 provides an overview of new battlefield electronic warfare technologies.

	down, and undergo an attack by a determined adversary.
Evil ATM	The team must use a 3D printer to fabricate an ATM card skimmer and deploy it without detection.[101]
Business Travel	The team must develop and employ techniques to determine if their hotel room has been compromised by an adversary. An alternate version could seek to compromise the hotel room, rather than defend it. An office scenario, rather than a hotel room, could also be used.
Crime Scene	A computer related crime occurs and the team must conduct forensically sound, and legally admissible, analysis.
Dumpster Diving	The team goes through trash and recycling bins to collect information, some of it is shredded and must be recovered.
Stubby Pencil	The adversary is overly reliant on the Global Positioning System (GPS). The team must find a way to disrupt their use of GPS.[102]
Tamper Proof	A shipping container with a tamper proof seal must be surreptitiously tampered with.[103]
Globalization	The team must compromise the supply chain security of an adversary.
Going Phishing	The team must send carefully crafted phishing emails and get recipients to respond in a desired way.
Deep Discounts	Local stores sell bootleg software and movies for pennies on the dollar. What badness do they contain?
Key to the Kingdom	A government official proudly displays the master key to the city's transit system in an online news story.[104] The team must fabricate a duplicate key and use it on a mission.

[101] Brian Kreb's provides a recent overview of ATM skimmers in "The Biggest Skimmers of All: Fake ATMs," Krebs on Security, 18 December 2013.

[102] For an example, see John Robert's "GPS Flaw Could Let Terrorists Hijack Ships, Planes," Fox News, 26 July 2013.

[103] See Datagram's "Introduction to Tamper Evident Devices," Defcon 19, July 2011 for an overview of tampering with tamper proof seals. The video is available online, http://www.youtube.com/watch?v=W07ZpEv9Sog

[104] See Renderman's "NY Daily News MTA Master Key Disclosure" Blog Post, 26-27 April 2010. http://www.renderlab.net/advisories/mta-key/, last accessed 22 December 2013 and Andy Greenberg's

Toy Store	The team visits a toy store and must modify one of the devices to accomplish a desired effect.
Cyborg	A team member wants to get an implanted electronic device. The team must perform a threat assessment.
Battlefield Media	A patrol captures a cache of devices on the battlefield. The team must provide rapid triage.
Drone	The team must assemble, test, and fly a drone to gain information on an adversary. This mission could be enhanced by requiring the team to create a custom sensor for the drone.
Cyber Cafe	The local cyber cafe is a hotbed of adversary activity, the team is tasked to collect information.
Better to Give than Receive	The team must modify a device and share it.[105]
Operation Cupcake	The team must replace a bomb-making recipe in an online terrorist magazine with a cupcake recipe.[106]
Covert Message	The team must send a message across the network without being detected. Unfortunately, cryptography alone won't cut it.
Water, Water, Everywhere	The local water plant is under cyber attack. The team must defend it. Alternatively, the team could attack a water plant or set up a water plant honeypot.[107] The "water plant" could be replaced with a bank, library, hospital, power plant, Internet provider, cell phone provider etc.
Magic Smoke	The team is given an old microwave and must fabricate a HERF gun to destroy an electronic device.[108] In alternative mission, the team attempts to shield an electronic device from such a weapon.

"How I Accidentally Helped Compromise the Secret Keys of High-Security Handcuffs, Forbes, 15 October 2012.

[105] See John McAfee's blog post "A Clear and Present Danger," 3 January 2013 for one example, http://www.whoismcafee.com/a-clear-and-present-danger/, last accessed 22 December 2013.

[106] Duncan Gardham provides reporting on the real-world "Operation Cupcake" in "MI6 Attacks al-Qaeda in 'Operation Cupcake'." The Telegraph, 2 June 2011.

[107] For an interesting related story, see Tom Simonite's "Chinese Hacking Team Caught Taking Over Decoy Water Plant," MIT Technology Review, 2 August 2013.

[108] See Mike Nathan's "HERF Gun Zaps More Than Your Dinner," Hack-a-Day, 21 March 2011. See also Jimmy Proton's "Make a Microwave Gun (HERF Gun)" Instructable, http://www.instructables.com/id/make-a-microwave-gun-HERF-gun/, last accessed 22 December 2013.

Invisibility Cloak	The team must study sensor systems employed by the adversary and find a way to render themselves invisible.[109]
The Candidate	There is an upcoming election in a country and the electronic voting system isn't secure. The team must ensure a fair election.[110] This scenario could also be inverted and require the team to ensure a given candidate is elected.
DDOS Me Not	The team employs a Distributed Denial of Service (DDOS) Tool,[111] but the tables are turned when they must mitigate a counterattack.[112]
Judgement Day	An army of robots is approaching. The team must reverse engineer a captured bot and devise a countermeasure.
Hunt	An adversary has penetrated a friendly network and the team must track them down.
The General's Laptop	The General wants to hook their laptop to an official network. The team only has 30 minutes to make it safe to do so.[113]
Open the Pod Bay Doors	An Artificial Intelligence (AI) system designed to run a facility goes rogue. The team must shut it down.
I Just Broke the Internet	An elite hacker finds a catastrophic flaw in a core Internet protocol. The team must assess the potential damage.[114]
Crisis Reaction	The team is called in to assist an organization which has just been subject to a compromise.
Support a Kinetic Raid	A military unit needs timely cyber effects precisely delivered in order to accomplish their kinetic attack. Unfortunately they provide little warning for the team to prepare.
Prison Break	The team assists Prisoners of War (POWs) in

[109] Sara Afzal provides one example in "Shields Across Light Frequencies," Mashable, 5 December 2013.

[110] For a real world example see Alana Abramson's "Former Cal Student Gets Year in Prison for Rigging Campus Election," ABC News, 17 July 2013. http://abcnews.go.com/US/cal-state-student-year-prison-rigging-campus-election/story?id=19682401, last accessed 22 December 2013.

[111] See http://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon for one example of a denial of service tool.

[112] See Joseph Menn's *Fatal System Error* for a detailed case-study on countering denial of service attacks.

[113] This mission is based on an "inject" from the NSA sponsored Cyber Defense Exercise run for the five U.S. Service Academies.

[114] See Joshua Davis, "Secret Geek A-Team Hacks Back, Defends Worldwide Web," Wired Magazine 16.22, 24 November 2008

	escaping from an adversary’s prison.[115] An alternative version is when the team must escape from a hostage situation.
Force on Force	The team must go head-to-head against an elite nation-state hacking unit.
The Cyber Apocalypse is Nigh	Everywhere electronic devices are turning into bricks. The team must find the cause, and the solution.

[115] See Kim Zetter’s “Prison Computer ‘Glitch’ Blamed for Opening Cell Doors in Maximum-Security Wing,” Wired Threat Level Blog, 16 August 2013.