SMALL WARS JOURNAL

TOWARDS A CYBER LEADER COURSE MODELED ON ARMY RANGER SCHOOL

Articles

Fri, 04/18/2014 - 12:31pm

Towards a Cyber Leader Course Modeled on Army Ranger School

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

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[i] leaders, the time has come to create a U.S. Army Cyber Leader Course of equal intensity, reputation, and similar duration,[ii] but focused on cyber operations (see Figure 1). This article presents a model for the creation of such a school, one that goes far beyond just a tough classroom experience by using tactical close-access missions as a core component. What we propose is unique, demanding, immersive, and fills a necessary gap in Army cyber leader development. This article is a condensed form of a more detailed analysis and description of the proposed Army Cyber Leader Course.[iii]

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.

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. We face a critical 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. 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 be a logical follow-on step.

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 currently available. Many civilian training offerings are closely tied to industry certifications, including CompTIA's A+, Network+, and Security+, the EC-Council's Certified Ethical Hacker (CEH), ISC^2's Certified Information Systems Security Professional (CISSP), Black Hat Training[iv], KEYW[v], and Global Knowledge.[vi] Additionally, the SANS Institute offers training in foundational and advanced cyber skills as well as its "CyberCity" range, a miniaturized mock-up of a small city with real-world components, such as power distribution systems, where students interact with and observe the kinetic outcomes of their cyber operations activities (see Figure 2).[vii]

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.[viii]

We envision CyberCity or a similar technology as a valuable part of a Cyber Leader Course, particularly if implemented as part of 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 (Figure 3) and law enforcement's use of realistic training environments such as the Federal Law Enforcement Training Center.[ix]

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.[x]

In addition to civilian training courses, the military offers a range of cyber training, including the Joint Network Attack Course (JNAC) with topics including legal authorities, battle damage assessment, de-confliction, targeting, weaponization, and execution processes.[xi] 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.[xii] Another example is the Joint Cyber Analysis Course (JCAC), designed to train junior and mid-level enlisted personnel for duty in computer network operations related billets.[xiii] 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),[xiv] Cyber Network Defender (25D),[xv] Cryptologic Network Warfare Specialist (35Q),[xvi] the Electronic Warfare Career Management Field (CMF 29),[xvii] and the emerging Security Systems Engineer (FA26C).[xviii] 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.[xix]

Contests conducted at hacker conferences offer useful insights into potential Cyber Leader Course training and evaluation activities, including Capture the Flag (force-on-force network warfare) competitions at conferences such as DEF CON, ShmooCon, and DerbyCon. Academic cyber security competitions also show great promise in teaching valuable skills, including the NSA-sponsored inter-service academy Cyber Defense Exercise (CDX),[xx] the National Collegiate Cyber Defense Competition (CCDC),[xxi] and the Capture the Flag, embedded systems, and forensics competitions hosted by NYU-Poly and other universities world-wide.[xxii] Furthermore, academic institutions offer cyber education programs from certificates and Associate's Degrees to PhDs. Colleges and universities with mature 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 rigor of high-end civilian and military security training and certifications, the realism of MOUT training, and the innovative competitions of the hacker community and academia, 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."* [xxiii]
>
> - 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, the course will be fully 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.
- A warrior ethos - the ability to adapt, overcome, and fight through adversity to accomplish the mission.[xxiv]
- 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.[xxv]
- The ability to attack the *system* - probing the attack surface, including the human users, network components, computer systems, embedded devices, and more, 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[xxvi] 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 ethics, 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.[xxvii] All students, regardless of background and preparation will be pushed out of their comfort zones. 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.[xxviii] 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.[xxix] [xxx]

Evaluation and hands-on learning will be intrinsic parts 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.

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 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.

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.[xxxi] [xxxii] 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.

Course Duration and Phases

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.[xxxiii] [xxxiv] 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.

Missions

Military "patrol-sized"[xxxv] 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[xxxvi]

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, with a small sample of representative missions listed in Table 1 (the unabridged version of this paper includes a more extensive list). 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.

Representative Cyber Leader Course Missions and Descriptions

- *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.
- *Build and Defend a Network*: Team must build a network, provide proscribed services (such as email, chat, and web), lock it down, and undergo an attack by a determined adversary.
- *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.[xxxvii]
- *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 Café*: The local cyber cafe is a hotbed of adversary activity. The team is tasked to collect information.
- *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.[xxxviii] The "water plant" could be replaced with a bank, library, hospital, power plant, Internet provider, cell phone provider etc.
- *DDOS Me Not*: The team employs a Distributed Denial of Service (DDOS) Tool,[xxxix] but the tables are turned when they must mitigate a counterattack.[xl]
- *Judgment Day*: An army of robots is approaching. The team must reverse engineer a captured bot and devise a countermeasure.
- *The General's Laptop*: The General wants to hook a laptop to an official network. The team only has 30 minutes to make it safe to do so.[xli]
- *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.

Some missions are deliberately designed to include ethical components that will force students to make important decisions regarding collateral effects,[xlii] ethical behavior, rules of engagement, 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 standardized Operation Order format, as well as senior leader briefings.[xliii] [xliv]

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. Safety briefings and zero toleration for misconduct must be integral parts of the course, and be buttressed by an honor code, a legally reviewed conduct pledge, and safety waiver.[xlv]

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.

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.[xlvi] We recommend an iterative approach, where core leadership is drawn from the limited pool of uniformed cyber 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.

Infrastructure: As we envision it, the Cyber Leader Course 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[xlvii]), end-user workstations, specialized devices (e.g., Industrial Control Systems), and back-end servers with virtualization software. The school itself could be located at a single DoD installation or distributed across multiple installations for each phase of the training.

Cyber Tab

Successful completion of the course would authorize the graduate to wear the Cyber tab (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

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

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 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 absolute responsibility.

Acknowledgements

We would like to thank COL(R) Daniel "Rags" Ragsdale, former Commander, C Company, 5th Ranger Training Battalion for his advice and feedback.

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, or the United States Government.

End Notes

[i] 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 - Response Action (CND-RA), Computer Network Defense (CND), and Electronic Warfare (EW).

[ii] Ranger School is approximately 61 days long.

[iii] When available, the unabridged report will be posted at http://cyber.army.mil

[iv] As a representative example, see the Black Hat USA 2013 training offerings, http://www.blackhat.com/us-13/training/ (http://www.blackhat.com/us-13/training/), last accessed 1 September 2013.

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

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

[vii] 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.

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

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

[x] "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/ (http://www.peostri.army.mil/PRODUCTS/MMOUT/), last accessed 1 September 2013.

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

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

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

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

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

[xvi] David Vergun, “Army Opens New Intelligence MOS,” Army News Service, 27 November 2012.

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

[xviii] 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.

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

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

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

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

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

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

[xxv] We note that the Rangers were also required to develop their own techniques, tactics, and procedures as well as equipment as little 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.

[xxvi] We acknowledge that achieving the ability to fit within the civilian cyber security community is a difficult, albeit admirable, goal and may only be partially achieved by the course.

[xxvii] 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.

[xxviii] 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.

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

[xxx] 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.

[xxxi] 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.

[xxxii] 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.

[xxxiii] 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.

[xxxiv] 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.

[xxxv] 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.

[xxxvi] 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.

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

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

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

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

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

[xliii] 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.

[xliii] 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.

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

[xlv] 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.

[xlvi] 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.

[xlvii] 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.

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

About the Author(s)

Todd Arnold (/author/todd-arnold)

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.

Thomas Cook (/author/thomas-cook-0)

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.

David Raymond (/author/david-raymond)

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.

Ed Skoudis (/author/ed-skoudis)

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.

Michael Weigand (/author/michael-weigand)

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.

Gregory Conti (/author/gregory-conti-0)

Colonel Gregory Conti is a Military Intelligence Officer and Director of the Army Cyber Institute 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 USCYBERCOM Commander’s Action Group (CAG), as Officer in Charge of a deployed USCYBERCOM Expeditionary Cyber Support Element, and co-developed USCYBERCOM’s Joint Advanced Cyber Warfare Course. He served in the Persian Gulf War and in Operation Iraqi Freedom.