Every Soldier a Cyber Warrior: The Case for Cyber Education in the United States Army

Lieutenant Colonel Christopher J. Heatherly
MSIV Cadet Ian Melendez

"In the future, the cyber threat will equal or even eclipse the terrorist threat." [1]
- Robert Mueller, 2013

ABSTRACT

Cyberspace represents a new domain of warfare unlike any other in military history. Cyberwarfare practitioners be they state actors, non-state actors or individual hackers, are capable of tremendous–and readily deniable–damage to an opponent's civil or military infrastructure. While recent events have focused upon the Islamic State's ability to use the Internet for recruiting purposes, the real danger to the West comes from its two primary competitors. The Russian and Chinese governments are suspected of using the entire spectrum of cyber warfare as both a standalone capability as well as effectively incorporating it into the more traditional domains of war. When faced by so many capable opponents, cyber training takes on an even greater criticality for U.S. Army officers. This paper focuses on a vital aspect of the U.S. Army's overall cyber ability by examining the training provided to Army officers beginning with their pre-commissioning education and continuing throughout their careers. It provides recommendations for improvements in officer education to ensure that future generations of American soldiers are prepared for the exigencies of cyberwarfare.

INTRODUCTION

The Greek philosopher Plato once said, "Only the dead have seen the end of war." While the truth of that statement is eternal, the way war is fought forever evolves. Just as the Japanese attack at Pearl Harbor on December 7th, 1941, signaled the end of the

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

Lieutenant Colonel Christopher J. Heatherly enlisted in the U.S. Army in 1994 and earned his commission via Officer Candidate School in 1997. He has held a variety of assignments in special operations, Special Forces, armored, and cavalry units. His operational experience includes deployments to Afghanistan, Iraq, South Korea, Kuwait, Mali, and Nigeria. He holds master's degrees from the University of Oklahoma and the School of Advanced Military Studies. Additionally, LTC Heatherly is a freelance author with 80+ published works.

battleship and Admiral Alfred Thayer Mahan's doctrine of decisive battle, cyberwar represents a new era and a new domain of combat. Cyberwar will not be fought by soldiers armed with rifles and machine guns, or by those inside tanks or jet aircraft. Nor will cyberwar have clear front lines separating opponents or even focusing exclusively upon an enemy's military capability. Cyberwar practitioners will employ the full spectrum of available cyber weapons against multiple civilian and military targets using a variety of military and non-military platforms. Bluntly stated, every U.S. Army soldier must be ready to fight on the digital battlefield.

Understanding the threat

The Islamic State's (ISIS) use of social media and the dark web to seduce young people across the globe and spread their message both at home and abroad are what most American soldiers are familiar with when it comes to the contemporary war in the cyber world. While not "hacking" in the traditional sense, ISIS' effective use of the cyber world as a recruiting tool cannot be ignored as an estimated 27,000 foreign fighters have traveled to Iraq and Syria since 2011.[2] Similar ISIS recruiting efforts have found, inspired or trained a growing number of "home grown" terrorists who have struck targets across Western Europe and the United States (US). ISIS' success does not stem from robust networks of data but rather the unlimited and largely unregulated nature of the World Wide Web. Twitter accounts, Facebook profiles, online podcasts, YouTube and other social media platforms all serve as effective, and often redundant recruiting tools. While these accounts are quickly shut down by a host of international policing agencies, they are just as rapidly and easily reestablished as they are readily accessible, inexpensive messaging platforms.

While ISIS and other terrorist groups effective social media strategies, the US' near-peer competitors,

Cadet Ian A. Melendez of Sammamish Washington developed a deep love for history and political science at an early age. After graduating from high school in 2012, he attended Bellevue College and was involved in the colleges Model United Nations program. Ian took part in many simulations at an international level and personally lead the institution to several high-profile Model UN conferences. Ian transferred to Washington State University (WSU) in January 2016 and joined the WSU Army Reserve Officer Training Corps (ROTC) detachment. Ian is the first cadet to lecture at the U.S. Army Command and General Staff College. He will graduate from WSU with a bachelor's degree in History and will earn Minors in Political Science and Military Science. Ian will receive his commission as a Second Lieutenant in the U.S. Army in May 2019. He will serve as a military intelligence officer while pursuing admission to a doctoral program in history.

China and Russia, present a more capable and dangerous cyberwar threat to the West. For the past 16 years, the US and its allies focused heavily on global counterterror operations with specific priority placed upon the Iraqi and Afghan theaters. During this same period, China and Russia developed, operated, and refined their own cyber capabilities. These nation states will employ, and indeed have already employed, both overt and covert means of cyberwarfare using a variety of military, paramilitary, third party, criminal organizations, and other proxies. Cyberwarfare incorporates many forms not all of which will entail a traditional offensive operation. Many cyber operations will instead focus upon information or intelligence gathering in preparation for or in concert with other traditional forms of attack.

The threat from China

China is a near peer competitor to the US already expanding its influence across the Asia-Pacific region with the long-term goal of becoming a global superpower. While not above using military force in pursuit of its objectives, the Chinese are masterful at employing cyber warfare against both military and commercial targets, particularly in information-gathering. To cite one high profile case, a Chinese national named Su Bin, spent several years hacking US defense contractors for data on the U.S. Air Force's newest fighter and transport aircraft. This information could be used to advance China's own aviation capabilities through reverse engineering or exploitation of perceived weaknesses in US aircraft. It should be noted that while the U.S. Department of Justice alleged Su worked in concert with China's government, specifically People's Liberation Army (PLA) Unit 61938, Beijing denied any involvement. [3] Following a lengthy investigation, in 2016 an American court sentenced Su to 46 months in prison and a fine of $10,000. Unfortunately, the damage was already done in that China retained the information gathered in these attacks. Su's cybercrime was hardly unique and serves as evidence that the PLA has established dedicated units to act on the offensive in the cyber world. According to the New York Times, Unit 61398 is the source of several deliberate attacks by the PLA against the US military's cyber network. [4] A US National Intelligence Estimate, representing the analysis of all 16 US intelligence bodies, pointed to Chinese PLA officers or civilian contractors working at Unit 61938. [5]

While many of the details surrounding Unit 61938 are not fully known, such as its personnel composition, there is little doubt as to its past cyber activities and threat to Western interests. Unit 61398 is only one example of China's cyber playbook options. Author Joe McReynolds describes three different, but complimentary, approaches that Beijing employs against its competitors. These include operational military units, specialized civilian units and third party "external entities." [6] Additionally, a 2007 Foreign Policy article estimated China has 50,000 to 100,000 civilian hackers whose common interests bring them into occasional partnership with their nation's government. [7] Clearly, these groups represent a very real, highly skilled and robust danger to US national interests. A 2016 report from the US-China Economic and Security Review Commission bluntly stated, "among the most serious threats are China's efforts at cyber and human infiltration of US national security entities." [8]

The threat from Russia

Another primary US competitor, the resurgent Russian government, is widely believed to utilize similar tactics in its own cyber arsenal. According to a 2017 *Christian Science Monitor* article, the Russian government uses criminal computer hackers as proxies against targets in the West. This tactic provides two tremendous benefits: it ensures Moscow retains access (and control) over some of the most capable cyber operators and gives the Russians plausible deniability against Western reprisals. [9]

The successful employment of cyber warfare, either as a standalone capability or in conjunction with other systems, is nothing new to the Russian government. Indeed, the Russians employed cyber in support of conventional attacks during their 2008 invasion of Georgia–a first in military history. In that engagement, Russia allegedly overwhelmed Georgia's internet and computer infrastructure limiting Tbilisi's ability to coordinate its defense. [10] No doubt their capabilities have improved and perhaps been further refined in other operations over the past 9 years.

Like China, Russian cyber operations also target non-military entities as evidenced by the 2010 "cyberbomb" discovered in the NASDAQ exchange. [11] A near successful attempt at what could have been the largest data leak in the history of the US stock market caused many corporations and investors to seriously question the security of both their data and personal information, as well as the legitimacy of the market itself. [12] During the subsequent investigation, the National Security Agency (NSA) successfully traced the attack back to several Russian citizens including one Aleksandr Kalinin of St. Petersburg, Russia. Kalinin had previously stolen millions of credit card numbers and placed malware on major American corporations like Dow Jones, 7-Eleven, JetBlue, and JC Penny. [13] US federal prosecutors charged Kalinin and his co-conspirators with the attack although he has thus far avoided prosecution. [14] According to a report on Business Insider, “the NSA recognized the malware from a previous version, built by Russia’s main spy agency. However, this time it was much more dangerous–it had the ability to disrupt the entire network, potentially wiping out Nasdaq altogether.” [15] The Russian methodology of employing hackers, in lieu of sending them to prison, incentivizes their cooperation and affords Moscow a rather unique means of recruitment unavailable, or at least unpursued, to other nations. [16]

Additional reports warn of Russian attempts to hack into the US electric power grid and natural gas pipelines. [17] The impact of these attacks cannot be overstated as they would cause mass power outages or damage the physical infrastructure itself. The threat of and resultant damage from cyber security failures continues to be of national significance with many more high-profile attacks making headlines.

Current U.S. Army Cyber capability and training

The US military has its own cyber units, education and training, although for the purposes of this paper, we will primarily focus upon the Army. The first Army unit formally stood up for this new brand of warfare was the U.S. Army Cyber Warfare Command which was founded in 2010. The Army later designated this unit as an Army Service Component Command in 2016, authorizing it to “gather resources to organize, develop, and employ cyber capabilities in support of the Joint Force.” [18] During testimony before a Subcommittee of the Senate Armed Services Committee (SASC) on emerging threats and capabilities in 2015, then ARCYBER Commanding General LTG Edward Cardon said, “After a detailed study, the Army determined it needs 3,806 military and civilian personnel with core cyber skills.” [19] LTG Cardon further stated the Army would have 41 Cyber Mission Force team, working for the global combatant commanders, in the active component with an additional 21 Cyber Protection Teams in the National Guard or Army Reserves by the end of Fiscal Year 2016. [20] To effectively meet the threats on the cyber battlefield, the Army projects it will need an additional 355 officers, 205 warrant officers and 700 enlisted soldiers in the ranks. This number, combined with the planned 3,000 civilian contractors, will provide the Army with a more robust force both in terms of size and domain knowledge. [21] Recognizing the need for cyber leaders, the Army began commissioning new lieutenants directly into the newly created Cyber Branch. The Army has also issued calls for branch transfers to Cyber Branch of more senior officers, up to the rank of colonel, who already possess the skills, education and training required to meet the demands in this field.

For the bulk of the Army’s non-cyber branch personnel–in other words the rank and file soldiers, non-commissioned officers and officers in the Active Duty, National Guard and

U.S. Army Reserve components–cyber training consists of the online "Cyber Awareness Challenge." Taken annually, the Cyber Awareness Challenge is presented in a chapter format with the goal of "providing enhanced guidance for online conduct and proper use of information technology by DoD personnel, simulates the decisions that Federal government information system users make every day as they perform their work." [22] Test takers are awarded notional digital trophies for properly answering questions posed in a set of scenarios involving common work-related tasks. Although described as "first-person simulations and mini-games that allow the user to practice and review cybersecurity concepts in an interactive manner," the actual training received is limited in scope and value to leaders. [23] However, the Cyber Awareness Challenge provides no information on more advanced enemy cyber capabilities, nor US offensive or defensive cyber capabilities leaders will need in future operations.

Future Army officers enrolled in the Army Reserve Officer Training Corps (ROTC) receive some cyber instruction during their two to four years of military science education prior to earning their commission as lieutenants. There are 275 primary Army ROTC programs at universities and colleges across the US that train approximately 30,000 cadets and commission over 5,000 new officers per year. For most college students, ROTC is also their first encounter with the unique demands of military life and the formative experience beginning their careers as commissioned Army officers. As such, it is the largest source of new Army officers and should be, and indeed must be, the formative step in cyberwarfare training. In addition to taking the same Cyber Awareness Challenge, ROTC cadets also receive one class describing the new cyber branch career field. The authors see this as a prime opportunity to shape the future cyber ability of the force well in advance of their actual entry into military service.

Upon commissioning from ROTC, new lieutenants attend further schooling at a Basic Officer Leader Course (BOLC) based upon their respective branch, i.e., Armor, Military Intelligence, etc. While individual BOLC schools provide specialized training pertinent to their chosen fields they all share a common core of education required for any commissioned officer. The authors spoke with several new officers attending BOLC while researching this paper and found none of them had received any cyber training beyond the Cyber Awareness Challenge. This deficit is a glaring gap in officer education given these soldiers will serve as the Army's leadership for the next thirty or more years into the future. Failure to institute an appreciation for operational advantages and dangers of cyberwarfare now will create challenges in cyber application throughout the entirety of their service careers.

Examination of another level of the officer education system (OES) reveals the same problem exists at other levels. The top half of the Army officer corps are centrally selected to attend the Command and General Staff College (CGSC), sometimes called Intermediate Level Education (ILE), usually in their eight to tenth year of military service. This course is approximately ten months in length for those who attend the resident version. CGSC, located at Fort Leavenworth, Kansas, has made some inroads to improving cyber to address the very real threat its graduates will face as they return to the operational force.

Currently, the core curriculum provided to all CGSC students includes a two-hour block on cyberspace with additional cyber instruction as part of the lessons on Command and Control and Fires Integration. Additionally, CGSC includes some cyber play in the various student war game exercises conducted at the end of each major block of instruction. American officers attending CGSC have the option to take a classified cyber elective although class attendance is limited by security clearance requirements and instructor availability. This class, which is double the length of a normal CGSC elective course, includes a mix of classroom instruction, guest speakers and practical exercises. [24] While this nascent initiative is to be applauded, waiting until the midpoint of a military career comes too late for maximum benefit.

The CGSC's approach to cyber education further highlights some of the challenges facing the Army's Training and Doctrine Command (TRADOC) which is responsible for soldier education. First, the pool of available cyber instructors is limited to those with the proper security clearance, education and experience. The CGSC faculty team, for example, is largely made up of civilian instructors who retired from active military service before cyber warfare was a standard consideration. No doubt the instructors are dedicated to their profession and the education of their students, but they will require additional training to bring cyber relevance to the classroom. The pace of change in cyber warfare is rapid and will also require the military's educational platform to quickly develop both courses and instructors. Nor is cyber training a "once and done" type of learning but instead requires dedicated study over a career. The classification of the material itself presents a third challenge. Knowledge of and access to US cyber capabilities must be limited to those with a verified need to know lest it fall into the hands of US competitors.

Improving Army Cyber readiness

We suggest several actions for the U.S. Army to consider improving its current cyber capabilities and training. First, the Army must promote the seriousness of the threat to the entire force and not place the burden to dominate this new domain of warfare on cyber missioned units. The U.S. Marine Corps has a mindset that every Marine is a rifleman first. Given that every Soldier has access to personal and government IT systems, smart phones and the like, the Army must adopt the same mind frame but expand it to include every soldier is a cyber warrior as well.

This new mindset must begin the moment a civilian recruit steps forward and volunteers to serve. The Army must adopt an aggressive national cyber recruiting strategy targeting those citizens with the skill sets demanded by the branch. Similarly, local Army recruiters must identify qualified applicants for cyber branch positions and explain the unique aspects of this military occupational specialty (MOS). A suggestion, not without controversy, is to redirect personnel who are not physically qualified into civilian cyber opportunities that do not have the same operational demands as uniformed soldiers. This would require Army recruiters to place civilian applicants but would also contribute to the Army's overall ability to hire new personnel. Reducing or eliminating the physical requirements for uniformed personnel or the criminal, educational or moral requirements for any Army applicant is categorically rejected by this paper. The Army must further press for more efficient hiring procedures to bring on the required personnel now. During his Senate hearing, LTG Cardon relayed the challenges of hiring personnel "given internal federal employment constraints regarding compensation and a comparatively slow hiring process." [25]

Beginning with their initial training and continuing throughout the entirety of their careers, soldiers must be routinely educated on cyber threats in "hands on classes" taught by experts who are able to demonstrate the dangers of cyber warfare. Instruction should be multifaceted across the entire spectrum of threats including improper use of email, social media accounts, personal cell phones or computers as well as the potential damage of cyberattack during the conduct of actual military operations. Examples of such effective training would include case studies based on real soldier cyber incidents, ruthlessly enforcing operational security (OPSEC) in both garrison duties and field exercises, classes on security classification regulations and drastically reducing the prevalence of personal computing or communication devices at home station or deployed locations.

Additionally, the Army must continue to offer incentives to retain the best cyber personnel in the formation lest we lose them to opportunities elsewhere in the civilian cyber fields. The introduction of competitive bonuses for reenlisting cyber soldiers like those offered to the special operations is but one possible solution. While some special forces bonuses top $150K, the financial and time resources of recruiting and training new cyber personnel would be much greater. [26] Instituting educational partnerships, exchanges or simply sending cyber personnel to undergraduate, graduate or doctoral programs is another method to train and retain the best personnel.

The Army should seek outside expertise and solutions by partnering with industry and educational institutions also combating cyber threats. While hardened infrastructure and new cyber defense technologies will afford some measure of defense against future attacks, these are not sufficiently robust or effective to ignore the human component required to meet the threat. A 2017 Real Clear Defense article neatly sums up this problem stating, "Promising technologies like artificial intelligence – software that autonomously detects and thwarts attacks – are fueling investment and innovation but should not be seen as silver bullets." [27] Simply investing money and energy in the existing paradigms as the quote would suggest is not enough to remedy the situation and put the military on par or beyond that of US near-peer adversaries. Utilizing and working alongside existing academic structures brings in a new non-military perspective from citizens who are in many ways the experts of the cyber field. The University of Dallas, for example, offers undergraduate, graduate, and post-graduate degrees in the various subfields of cyber. A Master of Science in Cyber Security from the University of Dallas teaches students a litany of skills including methods of data protection, legal issues and protections under the law, network security and digital forensics. Proving the connection between cyberattacks and instigator is incredibly difficult and one of the most attractive features of cyberwarfare. Increasing the number of experienced soldiers and civilian contractors armed with the educational background and experience on tracing digital evidence could provide the definitive evidence required for the US to defend against or respond appropriately to future cyberattacks.

More pragmatically, leaders must enforce proper communication procedures and cyber OPSEC in all aspects of a unit's daily duties whether in garrison or in the field. Commanders must hold Soldiers accountable, and they themselves must be held accountable, for violations of standing cyber regulations, rules and laws that threaten the readiness or operational security of their units. Leaders stating, "it's too hard" or "I am assuming risk" and willfully ignoring cyber OPSEC will lead to US casualties or even defeat in warfare against peer or near-peer opponents.

It is equally important the Army continually fund both cyber units and cyber training to ensure all soldiers are prepared for cyber warfare. During the Global War on Terrorism, the Army stood up or expanded numerous capabilities such as counter IED, working dogs, military transition teams (MITT) or agricultural development teams (ADT) to support combat units lacking these enablers in their organic formations. Many of these same enablers were reduced as the Iraq and Afghan theaters drew down. Attempts to expand these programs will long stand up times in any future conflict. Additionally, the Army often failed to promote or select for higher command the personnel assigned to these units, particularly those officers commanding MITTs, all but ensuring the "best and brightest" would seek assignment elsewhere. We cannot afford to make the same mistakes with cyberwarfare.

CONCLUSION

Famed American humorist Mark Twain observed, "history doesn't repeat itself, but it does rhyme." [28] America will go to war again. The cyber domain will play a prominent, if not decisive, role in that war. The only questions which remain unanswered are the opponent, location, and timing of that future conflict. Potential enemies, namely China and Russia, have already shown a willingness and ability to incorporate cyber into their offensive and defensive strategies. The Army must be ready – through education, training and partnership with industry leaders – now to fight and win on the cyber battlefield. This readiness will be found in the education of the next generation of Army leaders.

NOTES

1. Federal Bureau of Investigation, RSA Cyber Security Conference remarks, https://archives.fbi.gov/archives/news/speeches/working-together-to-defeat-cyber-threats.
2. *The Daily Telegraph,* Iraq and Syria: How many foreign fighters are fighting for ISIL?, http://www.telegraph.co.uk/news/2016/03/29/iraq-and-syria-how-many-foreign-fighters-are-fighting-for-isil/.
3. *The Washington Post*, Businessman admits heling Chinese military hackers target U.S. contractors, https://www.washingtonpost.com/world/national-security/businessman-admits-helping-chinese-military-hackers-target-us-contractors/2016/03/23/3e74e4a4-f136-11e5-85a6-2132cf446d0a_story.html?utm_term=.106972b16120.
4. *The New York Times*, Chinese Army Unit Is Seen as Tied to Hacking Against U.S, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?emc=na&_r=1&.
5. Ibid.
6. *The Daily Beast,* China Reveals Its Cyberwar Secrets, http://www.thedailybeast.com/china-reveals-its-cyberwar-secrets.
7. *Foreign Policy*, China's Hacker Army, https://foreignpolicy.com/2010/03/03/chinas-hacker-army/.
8. *The Washington Free Beacon,* Report: Chinese Spies Stole Pentagon Secrets, http://freebeacon.com/national-security/report-chinese-spies-stole-pentagon-secrets/.
9. *The Christian Science Monitor,* How Russia and others use cybercriminals as proxies, https://www.csmonitor.com/USA/2017/0628/How-Russia-and-others-use-cybercriminals-as-proxies.
10. *The New York Times,* Before the Gunfire, Cyberattacks, http://www.nytimes.com/2008/08/13/technology/13cyber.html.
11. *Business Insider,* The Massive Hack of the Nasdaq That Has Wall Street Terrified of Cyber Attacks, http://www.businessinsider.com/nasdaq-attacked-by-hackers-2014-7.
12. CNN, Russian hackers placed 'digital bomb' in Nasdaq – report, http://money.cnn.com/2014/07/17/technology/security/nasdaq-hack/index.html.
13. The United States Department of Justice, Russian National Charged in Largest Known Data Breach Prosecution Extradited to United States, https://www.justice.gov/opa/pr/russian-national-charged-largest-known-data-breach-prosecution-extradited-united-states.
14. NJ Advance Media, Russian hackers plead guilty in N.J. in worldwide $300M credit card scheme, http://www.nj.com/news/index.ssf/2015/09/russian_hackers_plead_guilty_in_nj_in_worldwide_30.html.
15. *Business Insider,* The Massive Hack of the Nasdaq That Has Wall Street Terrified of Cyber Attacks, http://www.businessinsider.com/nasdaq-attacked-by-hackers-2014-7?IR=T.
16. NJ Advance Media, Russian hackers plead guilty in N.J. in worldwide $300M credit card scheme, http://www.nj.com/news/index.ssf/2015/09/russian_hackers_plead_guilty_in_nj_in_worldwide_30.html.
17. CNN, Russia attacks U.S. oil and gas companies in massive hack, http://money.cnn.com/2014/07/02/technology/security/russian-hackers/index.html.
18. The United States Army, Army Announces ARCYBER as an ASCC, https://www.army.mil/article/171513/army_announces_arcyber_as_an_ascc.
19. The United States Army, Army may create cyber career field for civilians, https://www.army.mil/article/146485/Army_may_create_cyber_career_field_for_civilians/.
20. Ibid.

NOTES

21. The Army Times, Staffing goal for Cyber branch totals nearly 1,300 officers, enlisted soldiers, http://www.armytimes.com/news/your-army/2015/06/15/staffing-goal-for-cyber-branch-totals-nearly-1300-officers-enlisted-soldiers.
22. The Center for Development of Security Excellence, CyberAwareness Challenge 2019 for Department of Defense (DoD) DS-IA106.06, http://www.cdse.edu/catalog/elearning/DS-IA106.html.
23. Ibid.
24. Kurt Vandersteen, email to author, August 8, 2017.
25. The United States Army, Army may create cyber career field for civilians, https://www.army.mil/article/146485/Army_may_create_cyber_career_field_for_civilians/.
26. *The Stars and Stripes*, $150,000 bonus offered for some Special Forces, https://www.stripes.com/news/150-000-bonus-offered-for-some-special-forces-1.75636#.Wa0oEbpuLIU.
27. *Real Clear Defense*, Will U.S. Cyberwarriors Be Ready for the Next Big Hack?, http://www.realcleardefense.com/articles/2017/08/17/will_us_cyberwarriors_be_ready_for_the_next_big_hack_112066.html.
28. Good Reads, Mark Twain Quotes, https://www.goodreads.com/quotes/5382-history-doesn-t-repeat-itself-but-it-does-rhyme.