SMALL WARS JOURNAL

smallwarsjournal.com

Self-Development for Cyber Warriors

by Gregory Conti, James Caroland, Thomas Cook, Howard Taylor

From the battlefields of Iraq and Afghanistan,[1] the inner ring of the Pentagon,[2] and the Defense Industrial Base,[3] to our home computers, mobile devices, and Facebook accounts, cyber warfare permeates virtually every aspect of our personal and professional lives. Once obscure groups like Wikileaks, Anonymous, and LulzSec and rarefied technologies such as the Stuxnet worm are now part of everyday discussions in classified military command centers as well as pubs and living rooms around the world. Rapid technological change, the low-cost asymmetric advantage afforded attackers, and the resultant clear and present danger to critical information systems have not gone unnoticed by military organizations, governments, educational institutions, and kids in the basement, some allied with the United States and some not. As a result, informed experts consider cyberspace an area of prime concern for the United States and a key warfighting domain alongside air, land, sea, and space.[4,5]

As United States Cyber Command enters its second year, the military services are actively seeking to recruit, develop, and retain a world-class cyber workforce. Tailored education, training, and developmental experiences for the cyber domain, as well as an understanding of the knowledge, skills, and abilities required for planning, executing, supporting, and interfacing with cyber warfare operations are now beginning to emerge. However, unlike the mature career paths found in kinetic warfighting, the day when service members will benefit from decades of continuous experience and development in the cyber domain lies far into the future. Even as appropriate training and career paths come to fruition, the rapid rate of technological change demands active self-development and unit-level cyber professional development activities to remain current. Such outside the military classroom self-development must be embraced and encouraged by the military services who have to provide the requisite time and resources. At its core, the cyber warfare ethos must consider self-development a critically important activity, to do otherwise risks less than world class professionals and performance.

Today, most personnel are drawn from career fields with varying degrees of intersection with cyber warfare including: signals intelligence, all source intelligence, and telecommunications, as well as from the larger kinetic warfighting community. While this diversity brings much to the table, every donor group has its own blind spot - gaps in experience, education, and training that must be filled to provide a baseline of common understanding and

[1] Noah Shachtman. "Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack." Wired, Danger Room Blog, 25 August 2010.
[2] Sharon Gaudin. "Hack Attack Forces Pentagon to Take Computers Offline." *Information Week*, 22 June 2007.
[3] Kit Eaton. "How Hackers Stole 24,000 Files From the Pentagon." *Fast Company*, 15 July 2011.
[4] "The National Military Strategy for Cyber Space Operations." United States Department of Defense, December 2006.
[5] "Department of Defense Strategy for Operating in Cyberspace (DSOC)." United States Department of Defense, May 2011.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
10 NOV 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Self-Development for Cyber Warriors	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **United States Military Academy,Cyber Security Research Center,West Point,NY,10996**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**34**	

operate most effectively in the cyberspace domain. This challenge isn't new, military services have frequently faced the challenge of retraining personnel as they transition from one career specialty to another. In many ways, the birth of Cyber Command is as dramatic as the creation of the United States Air Force and similarly brings both the opportunity to create a powerful new culture and the challenge of transitioning many diverse personnel. Our goal with this article is to aid in such a transition by helping readers self-assess their own preparation, identify gaps in expertise, and provide techniques for filling knowledge gaps and facilitating currency through self-development activities. An important part of our discussion is the appropriate trade-off between depth and breadth of expertise across the many facets of cyber warfare. While additional learning resources are available in classified environments, a solid foundation can be built upon on easily accessible and publicly available information and techniques. In addition, while this article is written to help the individual practitioner, many of our recommendations may be used to help create unit professional development programs and inform other more formal education and training activities. There are many important open questions surrounding the cyber workforce, such as the role of Officer, Warrant Officer, and Enlisted personnel as leaders or as technical experts. Other important questions consider the appropriate roles for DoD civilians and contractors. We do not attempt to answer these questions here and instead seek to provide a framework for professional development that can be appropriately tailored to an individual's given circumstances and can adapt to future decisions regarding these and similar questions.

In this article, we use the terms *cyber, cyber warrior* and *cyber workforce*. Widely accepted definitions of these terms have yet to emerge. For purposes of this article, we define *cyber* broadly as Computer Network Attack (CNA), Computer Network Exploitation (CNE), Computer Network Defense (CND) and Global Information Grid (GIG) operations. We define a *cyber warrior* as someone who conducts, plans, or directly supports Computer Network Attack (CNA), Computer Network Exploitation (CNE), or Computer Network Defense (CND) operations.[6] Cyber warriors form the larger *cyber workforce* which staff organizations that conduct CNA, CNE, and CND activities. For additional information on the attributes of a cyber warrior see our previous work.[7]

A culture that respects and supports self-development is critically important to the cyber warfare profession, especially as we transition large numbers of diverse individuals into the cyber workforce. Historically, many military personal have had to develop their cyber warfare expertise *despite* the system, but we are seeing positive change occurring on a daily basis. The most immediate advantages to encouraging professional development are a more capable workforce, more effective operations, and more pleasurable working environments and culture. In addition, for those desiring to work in the cyber warfare domain, perhaps for the first time, working to develop the necessary knowledge, skills, and abilities provides other advantages. For example, by building a resume of experiences, individuals can demonstrate their desire, motivation, and expertise to the leaders, selection boards and human resources personnel that often serve as the gateways to cyber warfare assignments.

---

[6] We acknowledge that there are other facets of cyber warfare that may fall outside this definition, such as Computer Network Operations (CNO), Electronic Warfare (EW), Information Warfare (IW), and Information Assurance (IA) but believe ours to be a reasonable working definition for this paper.

[7] Gregory Conti and David Raymond. "Leadership of Cyber Warriors." Small Wars Journal, 11 July 2011.

Key Categories of Cyber Expertise

Cyber warfare and cyberspace are complex and multi-faceted. While most experts would agree that CNA, CNE, and CND are essential components, there are numerous other areas of expertise that are required of the cyber warfare professional. In this section we propose 20 categories, see Table 1. We acknowledge that there will certainly be debate surrounding the composition of this list, but these categories are based both on the authors' collective expertise in cyberspace operations as well as input from 40 senior and mid-career cyber security professionals taking part in US Cyber Command's Joint Advanced Cyber Warfare Course (JACWC) who assisted in vetting the list. We expect that this list will evolve over time, but believe it to be a reasonable starting point.

Table 1: Categories of Cyber Domain Expertise

Domain	**Brief Definition**
Computer Networks	Theoretical understanding of network technologies and protocols.
Network Ops / GIG Ops	Applied understanding of the design, operation, and management of enterprise networks.
Cyber Community of Interest	The numerous military, government, law enforcement, industry, academic, and hacker community entities who participate in cyber-related activities, both in the United States and internationally.
US Cyber Command	Understanding the organization and operations of US Cyber Command, including subordinate elements and connection to Service Cyber Components.
Signals Intelligence	Understanding of SIGINT tactics, techniques, procedures, and resources, and how to leverage them in support of cyber warfare operations.
All Source Intelligence	Ability to request, analyze, synthesize, and fuse intelligence from Geospatial Intelligence (GEOINT), Human Intelligence (HUMINT), Open Source Intelligence (OSINT), Signals Intelligence (SIGINT) and Measurement and Signature Intelligence (MASINT) sources.
Technology	Understanding of, and facility with, modern technology.
Cyber Policy and Law	Familiarity with major policies and laws surrounding cyberspace

	operations.
Computer Network Defense	Actions taken via computer networks to protect, monitor, analyze, detect and respond to network attacks, intrusions, disruptions or other unauthorized actions that would compromise or cripple defense information systems and networks. (Joint Pub 6-0)
Computer Network Exploitation	Enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks. (Joint Pub 6-0)
Computer Network Attack	Actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves. (Joint Pub 6-0)
Hacker Community	Understand the strengths, weaknesses, opportunities, and resources of the hacker community.
Cyber Training and Exercises	Understanding of major training opportunities as well as experience participating in and planning exercises.
Hacker/Adversary Mindset	Ability to creatively explore technology and push it in directions unintended by its designers and, when necessary, the ability to think like an adversary.
Cyber-Warfighter Integration	How to integrate cyber effects into kinetic operations and vice versa.
Kinetic Warfighting	How military forces conduct kinetic operations.
Cyber Warfare Threats	Understand major threat actors and groups in cyberspace and their tactics, techniques, and procedures.
Intelligence Community Operations	Ability to leverage Intelligence Community (IC) resources in support of cyber operations and objectives.
Emerging Technologies	Awareness of important emerging technologies and their potential impact on cyber operations.

Operational Planning	Ability to plan military operations.

These categories provide a useful framework for assessing both individual and collective expertise in the cyber domain. To assist in this process we've included a survey format version of this table as Appendix A. We've used this survey as part of pre- and post-course assessment for US Cyber Command's Joint Advanced Cyber Warfare Course that we helped develop and found it useful to gage the success of the curriculum. We also recommend the survey as a tool for individuals seeking to identify their personal strengths and weaknesses in the cyber domain, particularly as a way to identify self-development areas that can be addressed via the techniques we present later in this article. As you examine our suggested categories of cyber domain expertise in Table 1 consider your own personal expertise in each area and keep these strengths and weaknesses in mind as we present techniques for improvement in the next section.

Self-Development and Lifetime Learning

Developing cyber warfare expertise is a lifetime journey, not a short-term problem that can be solved with a single training course. Technology marches relentlessly onward at an exponential pace. What was once the state of the art in technology will quickly become dated. We must maintain aggressive personal and organizational development programs in order to remain current and innovate new tools, techniques, tactics, and procedures. The depth and breadth of knowledge sought varies significantly based on one's current duties and existing background, predictions of possible future assignments and projections, as Wayne Gretzky might put it, of where the technological puck will be in the future. This section describes various techniques for learning and sources of information. It isn't complete, but we sought to make the list a solid starting point. This section contains a wide variety of suggested sources of knowledge including books, blogs, magazines, and free videos, even comic strips. When appropriate, we've labeled various sources of information with the most relevant category or categories from the 20 we proposed earlier to assist readers in finding material that will help cover their blinds spots most effectively. This section also provides a great litmus test for those considering transitioning to the cyber warfare field. If you are excited by what you see, ideally find yourself familiar with much of the material, and are intensely interested in learning more, a cyber warfare career is probably for you. However, the opposite is also true.

Professional Reading

Professional reading lists are a mainstay of kinetic warfare professional development. The cyber domain is no different. There are an overwhelming number of cyber warfare related books, many are worth reading, some are not. In this section we've highlighted some essential reading, see Table 2. Due to space we've only included foundational books. Each can point you in the direction of deeper knowledge. For example, after exhausting this list you might study more specialized topics such as web security (*Ajax Security* by Hoffman), Google hacking (*Google Hacking* by Long), Cryptography (*Applied Cryptography* by Schneier), hardware hacking (*Hardware Hacking* by Grand et al), hacking culture (*2600* by Goldstein), information visualization (*The Visual Display of Quantitative Information* by Tufte) and social engineering (*No Tech Hacking* by Long and *The Art of Deception* by Mitnick). A complete list is well beyond

the scope of a single paper, but you will also want to explore wireless security, computer networks, mobile devices, cloud computing, computer forensics, malicious software, secure programming, Voice over Internet Protocol (VoIP), operating systems (Linux, Windows, Mac), and databases, among many other topics. If you are thinking that there is a lot to learn, you are right.

Table 2: Professional Reading (Books)

Title	Author	Category	Description
Counter Hack Reloaded	Edward Skoudis and Tom Liston	CNA, CND, CNE	Exceptional coverage of hacker techniques and countermeasures. Requires intermediate-level technical preparation.
Cuckoo's Egg	Cliff Stoll	Cyber Warfare Threats	Classic account of how a scientist at Lawrence Berkeley Lab tracks down a hacker who broke into his system.
Cyber War	Richard Clarke	Cyber Policy and Law, US Cyber Command, Cyber Community of Interest, Cyber Training and Exercises	The best currently available book on cyber warfare policy.
Defense of Hill 781	James McDonough	Kinetic Warfighting	A classic kinetic warfighting book useful to help understand combined arms warfighting and to understand adversary actions and reactions.
Fatal System Error	Joseph Menn	Cyber Warfare Threats, Cyber Policy and Law	Excellent coverage of online crime and the computer crime underground.
Hacking Exposed	Stuart McClure, Joel Scambray, and George Kurtz.	CNA, CND, CNE	The best selling computer security book in the world. Requires intermediate-level technical preparation.

Inside Cyber Warfare	Jeffrey Carr	Cyber Policy and Law, Cyber Warfare Threats, Cyber-Warfighter Integration	One of the first high-quality books to study modern cyber warfare in depth.
Secrets and Lies	Bruce Schneier	Technology	Introduction to cryptography.
Teach Yourself Networking in 24 Hours	Uyless Black	Computer Networks	Reading this book or something similar will provide you the basics of computer networking.
The Shadow Factory	James Bamford	Intelligence Community Operations	There isn't much publicly available information on the National Security Agency, but Bamford's books are the classic open source texts.
The Singularity is Near	Ray Kurzweil	Emerging Technology	A look into the near future of what continued exponential growth in processing power will mean to mankind.
Victorian Internet	Tom Standage	Technology	Studies the impact of the telegraph on Victorian society. Puts today's technical advances in historical context.

Science fiction will help push your thinking beyond today's technical realities and into the realm of future possibilities. Such out of the box thinking is essential for military and government cyber warfare professionals, because, let's face it, large bureaucratic cultures left to their own devices would have us looking and thinking the same. There are myriad science fiction books appropriate for the cyber professional, but we recommend those in Table 3 as excellent starting points. Each book provides a different and important perspective on technology and the future. In particular, the cyber punk genre is extremely relevant to the cyber professional; book authors such as Neal Stephenson, William Gibson, and Philip K. Dick provide dark, but thought provoking views of the future. A full list of potential books is again beyond the scope of this paper, but when you've exhausted the titles and authors listed below, we recommend considering titles in the Hugo and Nebula award lists.[8]

[8] See http://en.wikipedia.org/wiki/Hugo_Award and http://en.wikipedia.org/wiki/Nebula_Award.

Table 3: Professional Reading (Science Fiction)

Title	Author	Category	Description
Diamond Age	Neal Stephenson	Hacker/Adversary Mindset, Emerging Technologies	Describes many incredible advances in artificial intelligence and nanotechnology that may occur in our lifetimes.
Do Androids Dream of Electric Sheep	Philip K. Dick	Emerging Technologies	Examines a future where androids are all but indistinguishable from humans. Inspired the movie Blade Runner.
Ender's Game	Orson Scott Card	Hacker/Adversary Mindset, Emerging Technologies	Set in a future where a young military genius is essential to the survival of mankind.
The Forever War	Joe Haldeman	Emerging Technologies	A never ending conflict between an alien race and humans, where soldiers fight battles across many centuries.
I, Robot	Isaac Asimov	Emerging Technologies	Studies the future possibilities of robots, and not all of the possibilities are good.
Little Brother X	Cory Doctorow	Hacker/Adversary Mindset, Emerging Technologies	Set in the near future, Little Brother X provides essential reading on electronic civil liberties.
Neuromancer	William Gibson	Hacker/Adversary Mindset, Emerging Technologies	Dark and expansive view of the future. The first book to coin the phrase cyberspace.
Snow Crash	Neal Stephenson	Hacker/Adversary Mindset, Emerging Technologies	Classic cyber punk tale where the hero combats extremely virulent malicious software.
Starship Troopers	Robert Heinlein	Emerging Technologies	Predicts military operations, technologies, and politics in the

			near future.
When Sysadmins Ruled the Earth[9]	Cory Doctorow	Network Operations, Cyber Warfare Threats	Short story describing an apocalyptic series of events and the humans and technology that survive.

Technology News, Magazines and Blogs

While non-fiction books will provide high quality information on cyber warfare and technology, even the most current books will lag one to two years behind the state of the art. Thus, it is important to augment a cyber warfare professional reading program with more current information. There is good news in this regard, the cyber community has numerous high quality sources of information, including blogs written by experts, websites that provide summaries of the most important news and events, and magazines and journals from industry, academia, government, military, and hacker sources. Table 4 provides a summary of some of the best. While many that we suggest do not focus exclusively on cyber warfare, each is directly related to technology and frequently provides information relevant to cyber operations.

Table 4: Top Technology and Cyber-related Magazines and Blogs

Title	**Location**	**Category**	**Description**
2600	www.2600.com	Hacker Community, Hacker/Adversary Mindset, Cyber Warfare Threats, CNA, CND, CNE	The "Hacker Quarterly," famous for groundbreaking research and insights into the hacker mindset.[10]
Communications of the ACM	cacm.acm.org	Technology, Emerging Technologies, Cyber Policy and Law, Cyber Warfare Threats	Flagship magazine of the world's leading computer and information technology professional society.
Engadget	www.engadget.com	Technology, Emerging Technologies	In depth news and information on the latest gadgets and software.
Gizmodo	gizmodo.com	Technology, Emerging Technologies	In depth news and information on the latest gadgets and

[9] When Sysadmins Ruled the Earth is freely available at http://baens-universe.com/articles/When_Sysadmins_Ruled_the_Earth.
[10] Also see Phrack Magazine, http://www.phrack.org/.

			software.
Hack a Day	hackaday.com	Hacker/Adversary Mindset, Technology, Emerging Technologies	Provides daily updates on the latest developments from the DIY hardware hacker community.
How Stuff Works	www.howstuffworks.com	Technology, Emerging Technologies, Networks, CND	Provides quick overviews of a broad spectrum of technology topics. Often a great starting point.
IEEE Security and Privacy	www.computer.org/security	Emerging Technologies, CNA, CND, CNE, Cyber Policy and Law, Cyber Warfare Threats	Perhaps the best computer security magazine. It provides articles with both a practical and research focus.
Lifehacker	lifehacker.com	Technology, Emerging Technologies	Technology tips and tricks.
Make Magazine	makezine.com	Technology, Emerging Technologies, Hacker/Adversary Mindset	Excellent magazine covering DIY hardware projects.
MIT Technology Review	www.technologyreview.com	Emerging Technologies	An authoritative source on the future of technology.
Schneier on Security	www.schneier.com	Emerging Technologies, Cyber Policy and Law, Cyber Warfare Threats	Bruce Schneier is a security thought leader and his blog contains some of the best topical writing on cyber security.
Slashdot	slashdot.org	Emerging Technologies, Cyber Warfare Threats, Cyber Policy and Law, Cyber Community of Interest	The gold standard in technology news. Slashdot is read by virtually ever member of the technology community on a regular basis.
Small Wars Journal	smallwarsjournal.com	Kinetic Warfighting	The most agile and relevant military journal.

Social-Engineer.Org	www.social-engineer.org	Hacker/Adversary Mindset, Cyber Warfare Threats	Excellent site studying the most vulnerable component of security systems, the human user.
TaoSecurity Blog	taosecurity.blogspot.com	Cyber Warfare Threats, Emerging Technology, Cyber Policy and Law	Blog on digital security, incident response and forensics, by a leading expert, Richard Bejtlich.
Wikipedia	www.wikipedia.org	All Categories.	While you probably won't want to base life and death decisions on the absolute accuracy of Wikipedia, you should consider it a first stop as you learn about a new topic.
Wired Magazine	www.wired.com/magazine	Emerging Technologies	Monthly magazine covering new and developing technology and trends, particularly consumer electronics.
Wired Threat Level Blog	www.wired.com/threatlevel	Cyber Warfare Threats, Cyber Community of Interest, Cyber Policy and Law.	Provides some of the best writing and reporting on online crime, cyber warfare, and security.

Cyber Warfare Journal and Magazine Articles

The magazines and journals discussed above contain a wealth of information, in general. In this section we'd like to highlight some specific articles that we believe merit reading. Many of the articles we include in Table 5 challenge assumptions and are designed to foster discussion and debate.[11]

Table 5: Thought Provoking Journal and Magazine Articles

Title	Publication	Category	Description

[11] Due to space, we do not include a URL for each article because each can be found easily via a simple web search.

Army, Navy, Air Force, Cyber: Is it Time for a Cyberwarfare Branch of the Military	Small Wars Journal	Cyber Community of Interest	Provides a thought provoking study of the need for a fourth Cyber service alongside the Army, Navy, and Air Force.
Defending a New Domain	Foreign Affairs	Cyber Policy and Law, CND, Cyber-Warfighter Integration, Cyber Community of Interest	A seminal article by Deputy Secretary of Defense, William Lynn, which describes key challenges faced when securing cyberspace and important details on the compromise of US Government classified systems.
The Future of Things Cyber	Strategic Studies Quarterly	Cyber Policy and Law, Cyber Community of Interest	Written by retired General Michael Hayden. A former CIA and NSA director, Hayden addresses the right of self defense in cyberspace and many other topical issues.
Leadership of Cyber Warriors: Enduring Principles and New Directions	Small Wars Journal	Cyber Community of Interest, Hacker/Adversary Mindset, Cyber-Warfighter Integration	Leading cyber warriors may require different leadership techniques, this article presents principles for cyber warfare leaders.
Recruiting, Development and Retention of Cyber Warriors Despite an Inhospitable Culture	Small Wars Journal	Cyber Policy and Law, Cyber-Warfighter Integration, Hacker/Adversary Mindset	Recruiting and retaining high-quality cyber warriors is a not an easy task, this article studies the current state of affairs and suggests a way ahead.
Stuxnet: Cyberwar Revolution in Military Affairs	Small Wars Journal	Cyber Warfare Threats	Stuxnet was a seminal event in cyber warfare, this article studies the implications of Stuxnet in depth.
Building Teams of Cyber Warriors	Army Magazine	Cyber Community of Interest, Hacker/Adversary	Studies how teams of cyber warriors can be built and how our

		Mindset, Cyber-Warfighter Integration	adversaries may have a head start in building effective teams.
Winning the Ground Battles but Losing the Information War	Small Wars Journal	Cyber Policy and Law, Cyber-Warfighter Integration	Discusses how our adversaries are effectively using cyberspace to spread their ideology and the challenges the United States faces in working against these efforts.

Doctrine and Policy

Field Manuals (FMs) are authoritative, published doctrine that prescribe how soldiers conduct military operations, missions, and tasks except when, in the judgment of the commander, the situation dictates otherwise. FMs are the "How To" manuals for the Army. Each branch of service has a set of similar publications that describes how they do business. When the services are conducting Joint Operations a set of Joint Publications serve as their guiding manuals.

Doctrine, in general, consists of tried and true tactics, techniques, and procedures that have been battle tested over time. The manner in which an armor battalion conducts an attack, or defends a position has not changed significantly since World War II. Over the years, technology has allowed our armored forces to move faster, shoot farther, and communicate better; but we still fight using the classic hammer and anvil, single, and double envelopment attacks that originated over 80 years ago. Significant upgrades in our tanks have come about every decade since the 1940's. Doctrine and significant technology advancements in the Infantry and Field Artillery branches change in a similar manner. To be clear, US military doctrine has come a very long way going back to WW I and WW II, but change has been methodical, deliberate, and relatively slow. This is simply not the case for publications and doctrine for cyber warriors.

In the cyber world, an attacker's weapons can be developed and deployed in a matter of days, hours, or even minutes. Each weapon is different from the next and hard to defend against, especially if it is the first time defenders have seen a particular attack,[12] if the defender detects the attack at all. Cyber warfare doctrine will inevitably lag technology. Also, cyber warfare doctrine is likely to be significantly different from its kinetic warfare counterpart as the time required to develop new weapons and tactics is several orders of magnitude less than kinetic weapons and tactics, and potential cyber warfare avenues of attack[13] are orders of magnitude more common than in the physical world of kinetic warfare.

Nonetheless, experts have attempted to develop viable doctrine in the face of these and other challenges. As a result, there are Joint and service specific doctrinal publications, National

[12] Novel attacks such as these are call 0-day.
[13] Computer security experts use the term *attack surface* to describe potential avenues of attack.

and DOD Instructions, Directives, and Orders with which cyber professionals should familiarize themselves, see Table 6 below for important examples.

Table 6: Key Cyber Operations Doctrine and Policy Documents

Title	Category	Description
The Comprehensive National Cybersecurity Initiative (2008)	Cyber Policy and Law, CND	Describes "12 mutually reinforcing cybersecurity initiatives with the three goals 1) Establish a front line of defense against today's immediate threats. 2) To defend against the full spectrum of threats and 3) To strengthen the future cybersecurity environment designed to help secure the United States in Cyberspace."
Cyberspace Operations, USAF (2011)	Cyber Policy and Law, US Cyber Command	Serves as "the Air Force's foundational doctrine publication for Air Force operations in, throughout, and from the cyberspace domain."
Cyberspace Policy Review (2009)[14]	Cyber Policy and Law	Comprehensive review to assess U.S. policies and structures for cybersecurity.
Deputy Secretary of Defense Memorandum, The Definition of "Cyberspace" (2008)	Cyber Policy and Law	Official definition of cyberspace.
Department of Defense Strategy for Operating in Cyberspace (DSOC) (May 2011)[15]	Cyber Policy and Law	DoD's first unified strategy for operating in cyberspace. Provides the DoD vision for military, intelligence, and business operations.
International Strategy for Cyberspace (May 2011)[16]	Cyber Policy and Law	The United States' first comprehensive strategy for

[14] This document is available here http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf and a complete set of related documents are here http://www.whitehouse.gov/cyberreview/documents.
[15] DSOC supersedes the 2006 National Military Strategy for Cyberspace Operations. The document is available here http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf

		cyberspace. It describes plans for building prosperity, enhancing security, and safeguarding openness.
JP 3-13 Information Operations (2006)[17]	Cyber-Warfighter Integration, Kinetic Warfighting, Operational Planning	Provides the doctrinal foundation for the conduct of Information Operations in Joint environments.
JP 5-0 Joint Operation Planning (2011)[18]	Cyber-Warfighter Integration, Kinetic Warfighting, Operational Planning	The core of Joint doctrine for Joint operational planning throughout the range of military operations.
Secretary of Defense Memorandum, Command and Control for Military Cyberspace Missions (2008)	Cyber Policy and Law	Describes key policy developments regarding military missions in cyberspace.
US National Strategy to Secure Cyberspace (2003)[19]	Cyber Policy and Law, CND	Outlines an initial framework for "organizing and prioritizing efforts to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact."

Professional Societies and Local Gatherings

Self-development needn't be an isolated activity. There are many groups you can join, both formal and informal, that allow you to interact with like minded individuals. Table 7 provides a list of information security-related groups. As you examine the list, note that many groups may be culturally different from anything you've encountered before. You will get the most out of these groups if you bring an open mind, a humble attitude, and a sincere interest in learning. For more on the value of engaging diverse groups, see our previous work.[20]

[16] This document is available here http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
[17] This document is available here http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf
[18] This document is available here http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf
[19] This document is available here http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf
[20] Gregory Conti. "Why Computer Scientists Should Attend Hacker Conferences." *Communications of the ACM*, March 2005.

Table 7: Professional Societies and Local Gatherings

Title	Location	Category	Description
2600 Meetings	www.2600.com/meetings	Hacker/Adversary Mindset, Hacker Community, Emerging Technology	Informal meetings on computer security and hacking held around the world.
Association for Computing Machinery (ACM)	www.acm.org	Technology, Emerging Technology, Cyber Policy and Law	Professional society dedicated to information technology and computer science researchers and professionals. Membership benefits include access to digital books, training courses, and an excellent magazine.
Defcon Groups	defcon.org/html/defcon-groups/dc-groups-index.html	Hacker/Adversary Mindset, Hacker Community, Emerging Technology	Informal meetings on computer security and hacking held around the world.
Electronic Frontier Foundation (EFF)	www.eff.org	Cyber Policy and Law	Non-profit organization dedicated to electronic privacy and civil liberties.
Electronic Privacy Information Center (EPIC)	www.epic.org	Cyber Policy and Law	Non-profit organization dedicated to electronic privacy and civil liberties.
Hacker Spaces	hackerspaces.org	Hacker/Adversary Mindset, Hacker Community, Emerging Technologies	Community-oriented groups that maintain hacking facilities and collaborate on interesting projects.
Information Systems Security Association (ISSA)	www.issa.org	Cyber Community of Interest, CND, Technology	Professional organization of security practitioners with many local chapters.
InfraGard	www.infragard.net	Cyber Community of Interest, Cyber Policy and Law, CND	Non-profit dedicated to public-private partnership between industry and government, especially

			the FBI.
Institute of Electrical and Electronics Engineers (IEEE)	www.ieee.org	Technology, Emerging Technologies	Highly regarded professional society, similar to the ACM.

Academic, Military, Government, and Hacker Conferences

In addition to regular meetings, some groups also hold large conferences,[21] many with thousands of participants, see Table 8. Each conference has a different culture and include various percentages of security industry, hacker[22] community, government, military, law enforcement, and academic attendees. We'll discuss the online materials these conferences make available in the next section. In addition, academic conferences usually feature print proceedings available in academic digital libraries. We recommend that you review the program of previous conferences before attending a given event to ensure a good fit with your interests and background.

Table 8: Leading Cyber Security Conferences

Title	Location	Category	Description
Black Hat	www.blackhat.com	CNA, CNE, CND, Cyber Warfare Threats, Hacker Community, Cyber Community of Interest, Cyber Policy and Law, Hacker/Adversary Mindset, Emerging Technologies	A leading technical security conference, held in Las Vegas and other locations around the world.
Defcon[23]	www.defcon.org	CNA, CNE, CND, Cyber Warfare Threats, Hacker Community, Cyber Community of Interest, Cyber Policy and Law,	The world's largest hacker convention. Attendees are a mixture of hackers, government, law enforcement, and security

[21] There are too many high quality security conferences to list here, see http://en.wikipedia.org/wiki/Computer_security_conference for a more complete list.
[22] If you have never attended a hacker conference before, we recommend that you read "Why Computer Scientists Should Attend Hacker Conferences," *Communications of the ACM,* March 2005 for an orientation.
[23] Hackers come in many stripes, some are patriots, many are intent on defending the networks and information systems they are trusted to protect, most are into the playful exploration of technology, only a small percentage are up to malicious activities. You would be incorrect to assume Defcon or another hacker conference is a group of cryptoanarchists, attend yourself before passing judgment.

		Hacker/Adversary Mindset, Emerging Technologies	professionals.
International Conference on Cyber Conflict	www.ccdcoe.org/ICCC/	Cyber Policy and Law, Cyber Warfare Threats, Cyber Community of Interest, Emerging Technologies	International conference, held in Estonia, which brings together cyber security experts from government, academia, and industry.
International Conference on Information Warfare and Security	academic-conferences.org/iciw/iciw2011/iciw11-call-papers.htm	Cyber Policy and Law, Cyber Warfare Threats, Cyber Community of Interest, Emerging Technologies	Academic conference specializing in information warfare, cyber-operations and information security.
USENIX Workshop on Hot Topics in Security	www.usenix.org/event/byname/hotsec.html	CNA, CNE, CND, Cyber Warfare Threats, Hacker/Adversary Mindset, Emerging Technologies	Academic conference focusing on new ideas and problems in security.
Maker Faire	makerfaire.com	Hacker/Adversary Mindset, Emerging Technologies, Technology, Hacker Community	Akin to a science fair, a Maker Faire event hosts many DIY tech projects. Can be enjoyed by children as well.
New Security Paradigms Workshop	www.nspw.org	Cyber Warfare Threats, Hacker/Adversary Mindset, Emerging Technologies	Invitation only workshop that challenges dominant approaches and perspectives in computer security.
NSA Conferences	www.nsa.gov/ia/events/[24]	CND, Cyber Warfare Threats, Emerging Technologies, Cyber Community of Interest, Intelligence	NSA sponsors numerous cyber operations and security

[24] NSA may also advertise conferences in other locations, see www.ncsi.com/nsatc11/ for a recent example.

		Community Operations	conferences.
RSA	www.rsaconference.com	Cyber Community of Interest, Cyber Warfare Threats, CNA, CNE, CND, Cyber Policy and Law, Emerging Technologies	RSA Conferences are leading security events attracting technical managers, senior leaders, and technologists.
Shmoocon	www.shmoocon.org	CNA, CNE, CND, Cyber Warfare Threats, Hacker Community, Cyber Community of Interest, Cyber Policy and Law, Hacker/Adversary Mindset, Emerging Technologies	A leading hacking conference held in Washington, DC each Spring.

Videos and Podcasts

Many of the conferences listed above make their content available for free in iPod friendly video and audio formats as well as on video sharing sites such as YouTube. Similarly, there are numerous podcasts that are freely available. These are tremendous resources that are well worth exploring. We've found the videos useful in the classroom and the audio great to listen to in the car. Table 9 provides a list of great places to start. You may also want to explore Apple's iTunes store and streaming video options using Apple TV or a similar device.

Table 9: Videos and Podcasts

Title	Location	Category	Description
Black Hat Archives	http://www.blackhat.com/html/archives.html	CNA, CNE, CND, Cyber Warfare Threats, Hacker Community, Cyber Community of Interest, Cyber Policy and Law, Hacker/Adversary Mindset, Emerging Technologies	Cutting edge technical security research.

Defcon Archives	https://www.defcon.org/html/links/dc-archives.html	CNA, CNE, CND, Cyber Warfare Threats, Hacker Community, Cyber Community of Interest, Cyber Policy and Law, Hacker/Adversary Mindset, Emerging Technologies	Beginner through advanced hacker community research.
Exotic Liability	www.exoticliability.com	CNA, CNE, CND, Cyber Warfare Threats, Hacker Community, Hacker/Adversary Mindset	Top thinkers in the security community describe important advances and challenges.
HOPE Conference	http://thenexthope.org/talks-list/	Hacker Community, Hacker/Adversary Mindset, Cyber Warfare Threats, CNA, CNE, CND	Beginner through advanced hacker community research.
Paul dot com	www.pauldotcom.com	Cyber Warfare Threats, CNA, CNE, CND, Hacker/Adversary Mindset	Well regarded coverage of information security news, vulnerabilities, hacking, and research.
RSA Conference	https://365.rsaconference.com/community/speakers	Cyber Community of Interest, Cyber Warfare Threats, CNA, CNE, CND, Cyber Policy and Law, Emerging Technologies	Big picture talks by information security professionals on emerging advances and challenges.
Shmoocon	www.shmoocon.org	CNA, CNE, CND, Cyber Warfare Threats, Hacker Community, Cyber Community of Interest, Cyber Policy and Law, Hacker/Adversary Mindset, Emerging	Beginner through advanced hacker community research.

		Technologies	
TED Conference	www.ted.com/talks	Emerging Technologies, Cyber Community of Interest, Cyber Policy and Law	Thought provoking ideas that might change the world.

Movies

Fictional movies are another valuable tool to learn more about the cyber domain. Despite a frequent lack of realism, movies provide insight into both cyber culture and technology as well as provide an important shared experience. In kinetic warfare there is rarely a professional who hasn't seen Top Gun, Apocalypse Now, Patton, The Green Berets, and We Were Soldiers, among many others. The same holds true for cyber. Movies such as those in Table 10 are expected common knowledge.

Table 10: Cyber Domain Movies

Title	**Category**	**Description**
Blade Runner	Emerging Technologies, Cyber Warfare Threats	Bounty hunter Harrison Ford tracks down four rogue androids.
Live Free or Die Hard	Cyber Warfare Threats, Cyber Community of Interest	Terrorist group initiates a series of catastrophic attacks against critical infrastructure.
Enemy of the State	Cyber Community of Interest, Intelligence Community Operations, Emerging Technologies	Rogue NSA agents use electronic surveillance to track down Will Smith and destroy his life in an attempt to cover up a murder.
Ghost in the Shell	Emerging Technologies	Classic Japanese manga, a futuristic police thriller.
Hackers	Hacker Community, Hacker/Adversary Mindset	A much lampooned, but entertaining account of the hacker underground.
Hackers are People Too	Hacker Community, Hacker/Adversary Mindset	Excellent documentary on the hacker community.

The Matrix	Emerging Technologies	Assumption-challenging science fiction film that depicts a future where humans exist in a simulated reality.
Sneakers	Intelligence Community Operations	A tiger team of security experts attempt to recover a black box capable of breaking any encryption algorithm.
Swordfish	Emerging Technologies	Contains perhaps the best account of hacking under pressure.
Tron	Emerging Technologies	Computer programmer Jeff Bridges is trapped in a digital world.
War Games	Hacker/Adversary Mindset	The definitive hacker movie. Hacker Matthew Broderick accidentally causes a nuclear weapons crisis.

Training, Education, Certification and Self Study

There are numerous training, education, certification,[25] and self study programs available to the motivated and interested cyber warfare professional. The costs range from free to $30,000.00 and up for a Masters degree in some aspect of security or security management. Many organizations value these educational programs and may provide some level of financial assistance. Table 11 lists a select few certifications, training programs, and educational organizations that have a solid reputation in the security community.

Table 11: Sources for Training, Education, and Certification

Title	Location	Category	Description
Black Hat Training	http://www.blackhat.com/html/bh-us-11/training/bh-us-11-training_complete.html	CNA, CND, CNE, Emerging Technologies, Cyber Warfare Threats, Computer Networks	Black Hat training provides cutting edge security training taught by industry experts.

[25] We feel obliged to add a caveat to our mention of certifications. Certifications, no matter how hard to obtain, are not an end state. The same is true for a college degree. Human resources personnel love to use certifications and degrees as screening criteria for hiring decisions because it makes their job easier. However, a college degree nor a set of certifications are a guarantee of success, particularly in cyber security where many great people are self-taught. We encourage you to look holistically at each individual before making a hiring decision, otherwise the larger bureaucracy of the US Government may force hiring of the wrong people.

Certified Cisco Network Associate - Security (CCNA Security)	http://www.cisco.com/web/learning/le3/le2/le0/le1/learning_certification_type_home.html	CND, Computer Networks, Cyber Warfare Threats	Intermediate level certification for those charged with building and securing networks.[26]
Certified Ethical Hacker (CEH)	https://www.eccouncil.org/certification/certified_ethical_hacker.aspx	CNA, CND, CNE, Cyber Warfare Threats, Computer Networks, Cyber Policy and Law	A leading technical certification that includes the basics of penetration testing.
Certified Information Systems Security Professional (CISSP)	https://www.isc2.org/cissp/Default.aspx	CNA, CND, CNE, Cyber Warfare Threats, Computer Networks, Cyber Policy and Law	Considered by many to be a premier security certification. CISSP covers a broad swath of the cyber security domain.
Carnegie Mellon University MSIT in Information Security and Assurance	http://www.heinz.cmu.edu/school-of-information-systems-and-management/information-technology-msit/curriculum/information-security-assurance/index.aspx	Varies	Representative of the many high quality degree programs available via distance education.[27]
Edward Tufte's One Day Course on Information Visualization	http://www.edwardtufte.com/tufte/courses	Emerging Technologies	Effective presentation of data is critically important to cyber warfare professionals. Tufte's course provides exceptional training in this area.[28]
Fort Detrick Information Assurance Training Center	https://ia.signal.army.mil/ftdetrick/	Varies	Representative of the many training support programs offered by the military services.
Georgia Tech	http://www.scs.gatech.edu/future/m	Varies	Representative of the

[26] Also consider CISCO's CCNA and CCNP.
[27] See also http://www.scs.gatech.edu/future/msinfosecdistance
[28] For one review of Tufte's course written by a security professional see http://taosecurity.blogspot.com/2008/06/best-single-day-class-ever.html.

MS in Information Security[29]	sinfosec		many full time graduate programs in information security.[30]
MIT Open Courseware	http://ocw.mit.edu/index.htm	Varies	Representative of the free courseware made available by top tier universities.
SANS	http://www.sans.org/	CNA, CND, CNE, Cyber Warfare Threats, Computer Networks, Cyber Policy and Law	SANS provides world class security training taught by industry experts. Training vehicles include classroom, online, and video teleconference courses as well as a Masters degree and rigorous certification programs.
Security+	http://certification.comptia.org/getCertified/certifications/security.aspx	CNA, CND, CNE, Cyber Warfare Threats	A solid certification, Security+ teaches the fundamentals of cyber security.[31]

[29] See also http://www.umuc.edu/grad/gradprograms/csec.cfm
[30] For other high quality schools we recommend reviewing NSA's list of certified Centers of Academic Excellence in Information Security Education, http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml.
[31] Also consider CompTIA's Network+ and A+ certifications.

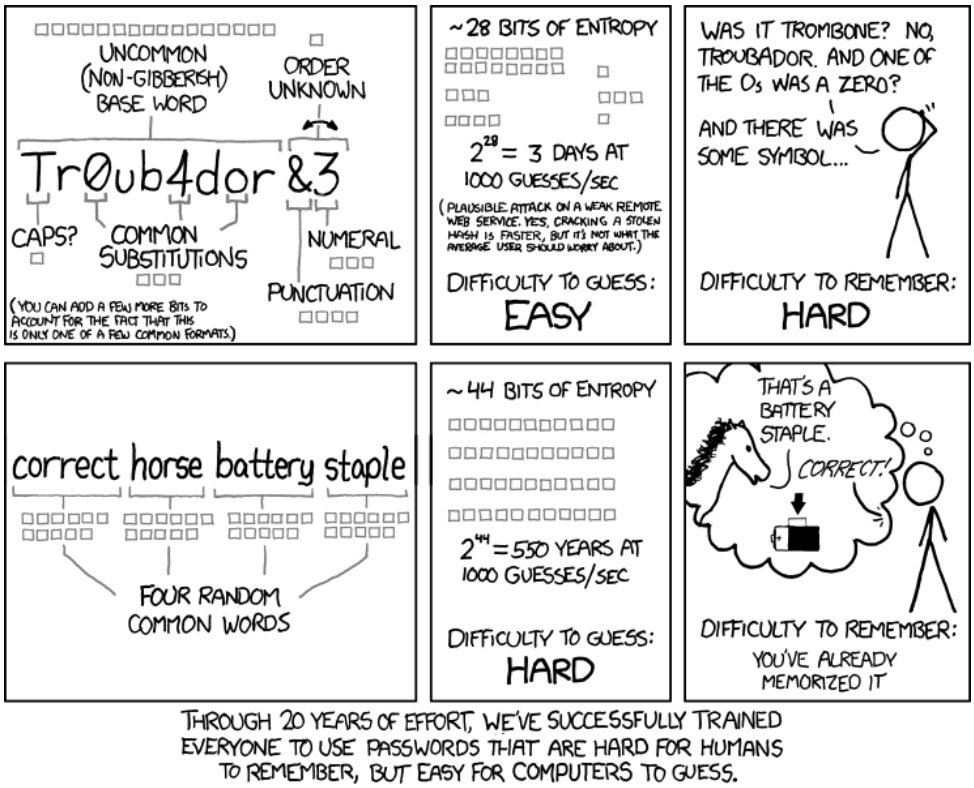

Figure 1: Comics such as xkcd (www.xkcd.com) provide insight into technical issues and technologist culture.[32]

Technology Cartoons

It may seem out of the norm to suggest reading cartoons as a means of professional development, but we aren't crazy. Cartoons are a powerful means of visually conveying technical information to a non-technical audience and can liven up any briefing. *PS - The Preventative Maintenance Monthly* has used a comic book format, and the occasional pin-up girl character, to extol the benefits of preventative maintenance to troops since 1951. There are numerous strips that cover technology and cyber operations topics, but we suggest two as a starting point - *xkcd* and *Dilbert*. xkdc (www.xkcd.com) provides thought provoking illustrations of technical material, see Figure 1, and Dilbert (www.dilbert.com) is especially helpful when leading technologists. Read them. If you or your organization exhibits any behavior that resembles that of the Pointy Haired Boss (PHB), consider changing your leadership style.

[32] Image source: http://xkcd.com/936/. Used with permission.

Other Ideas

There isn't space to include all possibilities, but we'd like to highlight a few other approaches to gaining expertise in the cyber domain. Consider becoming an early adopter of technology. You can be sure that our adversaries are actively studying new technologies and developing innovative ways new technologies can be employed to conduct malicious activities. Whether the technology be microblogging (Twitter), social networking (LinkedIn, Facebook), a smart phone (iPhone, Android), a GPS, or a tablet PC (iPad), by experimenting with technologies before they become widely popular you'll have a head start on their implications regarding cyber warfare. You could also join security related mailing lists or follow appropriate groups on social networking sites. Gaming in various forms can have benefits to your cyber warfare skills. Examples include Go, chess, Dungeons and Dragons, and a wide variety of online games and virtual environments, including World of Warcraft and Second Life. You'll develop problem solving skills and gain insight into important virtual communities. Also, consider picking up cyber related hobbies. These might include building your own computer, running your own website or blog, learning to program, adding automation to your car, building electronics, or becoming an amateur radio operator, among many other possible activities.

Self-Development Roadmaps

The preceding sections of this paper outlined important skills for the cyber warrior, provided tools for performing a self assessment of one's strengths and weaknesses, and suggested a wide variety of techniques for learning about the cyber domain. In this section we bring these ideas together by creating tailored roadmaps for self development.[33] We provide five examples: a signals intelligence Colonel (O6), a field grade army automator (O4), a field grade combat arms officer (O5), a senior enlisted intelligence analyst (E7), and a field grade JAG Corps Attorney (O4). For each example we describe our assumptions about the service member's prior background and experiences. Of course, individual cases will vary significantly from our examples, but the approach we suggest should generalize well and can be tailored to Enlisted, Warrant Officer, and Officer ranks of differing backgrounds and branches of service.

Colonel/O6, 35G (Signals Intelligence): This officer began her career as an Intelligence Officer for a Field Artillery Battalion and later a Field Artillery Brigade, and then participated in the Junior Officer Career Cryptologic Program (JOCCP).[34] After graduating from JOCCP she served in a variety of cryptologic assignments, which included a tour of duty at the National Security Agency, command of a Signals Intelligence Battalion, and a deployment on an expeditionary SIGINT support team. She holds a BS in Civil Engineering and an MS in Management Information Systems. Given this officer's strong technical and SIGINT background, we'd recommend the following as a bridge to cyber.

[33] Note that our roadmaps are designed as starting points for self-development, not as an exhaustive listing of all activities one should pursue over many years.

[34] JOCCP is the US Military's premier developmental program for SIGINT Officers. Over the three year period of JOCCP the student receives extensive training and significant professional growth via tailored workplace assignments.

- Pursue CISSP certification via self-study, or a week long bootcamp training course, to increase depth and breadth of cyber security knowledge.
- Read *Little Brother X* to gain a fresh perspective on civil liberties.
- Visit Slashdot daily to keep abreast of current events.
- Take SANS 512 Security Leadership Essentials For Managers course to increase depth and breath of security knowledge.
- Read *Secrets and Lies* to learn more about cryptography.
- Attend an RSA Conference to network with senior leaders from industry and learn about their challenges.
- Take Edward Tufte's one-day Information Visualization course to better understand how to convey information and help avoid a PowerPoint-centric mindset.
- Buy a domain name and web hosting service to learn by hands-on experience how a website works.

Major/O4, FA53 (Signal Corps / Information Systems Management): This officer began his service as a Signal Corps Officer responsible for providing reliable data and voice communications to Armor units. As a junior Captain he specialized as an Information Systems Manager (FA53) and helped engineer distributed information systems and networks, both in the United States and in Afghanistan. He holds a BS and MS in Computer Science. He has also earned the Certified Information Systems Security Professional (CISSP) and the Cisco Certified Network Associate (CCNA) certifications. For this officer we'd recommend the following.

- Read *Hacking Exposed* or *Counter Hack Reloaded* to increase depth of security-related technical expertise.
- Attend a hacker conference to network and learn about emerging technologies.
- Read *The Shadow Factory* to learn about the National Security Agency.
- Pursue Certified Ethical Hacker (CEH) certification to keep hands-on technical skills fresh.
- Join the Association for Computing Machinery to keep abreast of technical and policy developments.
- Read Joint Operations Planning (JP-5) to gain a greater understanding of Joint planning.
- Take SANS 504 Hacker Techniques, Exploits and Incident Handling course to learn new technical skills.

Lieutenant Colonel/O5, 11B (Infantry)***:*** This officer has led infantry soldiers at the platoon and company levels, and served on battalion level staff as an operations officer. He holds a BS in Military History and an MS in Military Arts and Sciences. He is also a graduate of the United States Army's School of Advanced Military Studies (SAMS),[35] is an expert kinetic warfare planner, has extensive deployed experience in Iraq and Afghanistan, and is considered a strong leader by his, all male, infantry soldiers.

[35] The School of Advanced Military Studies is the US Army's premier school for training and educating military planners.

- Read *Cyber War* to gain a big picture understanding of cyber warfare.
- Take the SANS 512 Security Leadership Essentials For Managers course to gain overview of cyber security domain.
- Read *Cuckoo's Egg* as a case study in tracking down an attacker.
- Visit How Stuff Works to learn about key technologies such as web servers and networks.
- Subscribe to Wired Magazine to keep abreast of current events.
- Read *When Sysadmins Ruled the Earth* to learn about providing network services despite an emergency.
- Watch Hackers are People Too documentary to better understand the hacker community.
- Attend a Maker Faire to help appreciate the hacker mindset.
- Watch Live Free or Die Hard to gain a perspective on attacks against critical infrastructure.
- Buy an iPad and learn to use it at the expert level to better understand emerging technologies.
- Read "Leadership of Cyber Warriors: Enduring Principles and New Directions" to learn how to adapt his leadership style to cyber professionals.

Sergeant First Class/E7, 35F (Intelligence Analyst): This soldier has extensive tactical experience analyzing and synthesizing HUMINT, SIGINT, and IMINT data, and requesting intelligence collection via tactical, operational, and strategic assets in order to provide the best possible battlefield situational awareness for his commander. He is a graduate of several Non-Commissioned Officer development courses as well as the Army's Airborne and Jumpmaster schools. He has completed a BA in Business Administration and is currently working on an MBA part-time.

- Read *Cyber Warfare* to gain a big picture understanding of cyber warfare.
- Read *The Victorian Internet* to understand the implications of new technologies on society.
- Read *Teach Yourself Networking in 24 Hours* to understand the basics of how a network works.
- Pursue the Network+ certification to solidify understanding of how networks work.
- Pursue the Security+ certification to develop foundation of cyber security skills.
- Follow Social-Engineer.org to understand potential attacks against human users.
- Read "Stuxnet: Cyberwar Revolution in Military Affairs" to understand the implications of cyber warfare weapons.
- Read JP 5-0 to gain a greater understanding of Joint planning.
- Attend the Shmoocon hacker conference to learn about the hacker community.

Major/04, 27Z (JAG Corps Attorney): This officer is a mid-career military attorney. She has prosecuted criminal cases under the Uniform Code of Military Justice, provided legal assistance (wills, powers of attorney, etc.) to soldiers and their families, provided legal and

ethical reviews of military actions, and advised her commanders on legal issues.[36] Her undergraduate degree was in pre-law, and her JD is from a top university. She is a member of the bar in her home state. She is interested in technology and is frequently an early adopter of new technologies such as electronic book readers and tablet PCs.

- Read *Inside Cyber Warfare* for an overview of cyber warfare operations.
- Read *Fatal System Error* for a case study on tracking down online criminals.
- Follow Wired's Threat Level Blog to stay abreast of current events.
- Take SANS 523 - Law of Data Security and Investigations course
- Visit the Electronic Frontier Foundation (EFF) and Electronic Privacy Information Center (EPIC) websites to learn about current legal issues.
- Attend an InfraGard meeting to network and learn about challenges faced by law enforcement.
- Attend a Black Hat conference to network, learn about emerging technologies, and better understand current policy and legal issues.
- Begin long-term study toward the CISSP certification to gain a fundamental understanding of cyber security technology.

Table 12 helps us take a broader look at the strengths and weakness of the major donor career fields to the cyber workforce. Of course, this is one assessment and by necessity overly generalized, but we suggest that such side-by-side comparisons are helpful when trying to create the right balance of backgrounds and expertise in cyber warfare units. As you examine the table note that we've added an idealized cyber warrior. This cyber warrior serves as a benchmark for comparison. We've chosen what we believe to be reasonable standards for this cyber warrior who rates "High" levels of expertise across 18 of the twenty domains. We've chosen to rate our cyber warrior as "Medium" in two categories, Kinetic Warfighting and All Source Intelligence because while expertise is helpful in these domains a high level of expertise most likely isn't necessary. There is significant work currently being conducted to better define specialties within the cyber workforce. For example, Timothy Franz suggests four major roles: Operators, Technicians, Analysts and Developers.[37] Whether the ultimate solution are the roles suggested by Franz, or another categorization, we believe that better and more precise definitions of cyber work roles and requisite knowledge, skills, and abilities will soon emerge. These insights can then be used to perform better analyses of where an individual's expertise is now and where it should be in the future.

[36] These attributes are drawn extensively from http://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/legal-and-law-enforcement/jag-corps-attorney.html.
[37] Timothy Franz. "The Cyber Warfare Professional." *Air and Space Power Journal*, Vol. 26, No. 2.

Table 12: Analysis of Primary Cyber Workforce Donor Career Fields

	Signals Intelligence	All Source Intelligence	Comms / Technologist	Warfighter	Policy and Law	Cyber Warrior
Computer Networks	Medium	Low	High	Low	Low	High
Network Ops / GIG Ops	Medium	Low	High	Low	Low	High
Cyber Community of Interest	Medium	Low	Low	Low	Low	High
US Cyber Command	Medium	Low	Low-Medium	Low	Low	High
Signals Intelligence	High	Medium	Low	Low	Low	High
All Source Intelligence	Medium	High	Low	Medium	Low	Medium
Technology	Medium	Low	High	Low	Low	High
Cyber Policy and Law	Low-Medium	Low	Low-Medium	Low	Medium	High
Computer Network Defense	Low-Medium	Low	Medium-High	Low	Low	High
Computer Network Exploitation	Medium	Low	Low	Low	Low	High
Computer Network Attack	Medium	Low	Low-Medium	Low	Low	High
Hacker Community	Low	Low	Low-Medium	Low	Low	HIgh
Cyber Training and Exercises	Low-Medium	Low	Low-Medium	Low	Low	High
Hacker/Adversary Mindset	Low-Medium	Low	Low	Low	Low	High

Cyber-Warfighter Integration	Medium	Medium	Low	Medium	Low	High
Kinetic Warfighting	Medium	Medium	Low	High	Low	Medium
Cyber Warfare Threats	Low-Medium	Low	Medium	Low	Low	HIgh
IC Operations	High	Low-Medium	Low	Low	Low	High
Emerging Technologies	Medium	Low	High	Low	Low	High
Operational Planning	Low	Medium	Low	Medium	Low	High

Conclusions

Aggressive self-development is a critical task for the cyber warfare professional. No matter the quality, formal training and education programs age poorly when facing the relentless advance of technology and agile adversaries. Self-development serves as a continuous complement to formal training and fosters the currency and depth of expertise a world class cyber workforce demands.

In addition, as many have yet to receive significant formal training, self-development can serve as a powerful tool for those transitioning into the cyber warfare career field for the first time. While the backgrounds of those joining the cyber workforce bring important diversity, each individual has important gaps in their expertise. We should not succumb to the belief that we can drop in any individual, no matter how competent in other areas, into the cyber arena and believe that success will follow. We must each, humbly acknowledge our shortcomings, work to address them in both ourselves and the units we may be charged to lead. We must also foster an ethos supportive of self-development. Self-development must not be done in spite of workplace culture, it demands proper command support.

Our purpose with this paper was to help each of us, beginner or expert, identify our own personal strengths and weaknesses, and employ time-tested ways for filling the gap between what we know and what we should know. We must regularly take a step back and reevaluate our knowledge, skills, and abilities, and actively map out our short-term and long term strategies for learning. The techniques we present in this paper are necessarily not complete, it is up to each individual and organization to further refine improved strategies to achieve mastery. Such mastery requires more than passively absorbing information, it requires application, failure, success, contribution, teaching, mentoring and leading, as well as speaking and writing both in public and in the workplace. This article also serves as a litmus test, if you are excited by what you see in this article, then the cyber warfare workforce is the place for you. If you were turned off, then perhaps a career as a cyber warfare professional is not for you.

The future bears great promise. Appropriate cyber career fields and high quality cyber workforce education, training, and professional programs are emerging now. On the horizon, we can see the day when the cyber workforce will consist of mature tools, techniques, tactics, and procedures, similar to our kinetic warfighting brothers and sisters. As great tank battalion commanders were once great tank company commanders and tank platoon leaders, we will enjoy a workforce that uniformly, throughout the ranks, is professional and battle tested in cyber warfare operations.

In conclusion, we proffer one challenge. Seek to be the world expert in what you do. This goal may sound pretentious, but it is not. Striving for a lesser goal will only place our Nation unnecessarily at risk and increase our chances of failure, and we must not fail, as we are only going to get one chance at getting this right.

Appendix A: Self-Assessment of Cyber Domain Expertise

Domain	**Brief Definition**	**Expertise** **(Low)** **(High)**
Computer Networks	Theoretical understanding of network technologies and protocols.	1 2 3 4 5 6
Network Ops / GIG Ops	Applied understanding of the design, operation, and management of enterprise networks.	1 2 3 4 5 6
Cyber Community of Interest	The numerous military, government, law enforcement, industry, academic, and hacker community entities who participate in cyber-related activities, both in the United States and internationally.	1 2 3 4 5 6
US Cyber Command	Understanding the organization and operations of US Cyber Command, including subordinate elements and connection to service cyber commands.	1 2 3 4 5 6
Signals Intelligence	Understanding of SIGINT tactics, techniques, procedures, and resources, and how to leverage them in support of cyber warfare operations.	1 2 3 4 5 6
All Source Intelligence	Ability to request, analyze, synthesize, and fuse intelligence from imagery intelligence, human intelligence, and other sources.	1 2 3 4 5 6

Technology	Understanding of, and facility with, modern technology.	1 2 3 4 5 6
Cyber Policy and Law	Familiarity with major policies and laws surrounding cyberspace operations.	1 2 3 4 5 6
Computer Network Defense	Actions taken via computer networks to protect, monitor, analyze, detect and respond to network attacks, intrusions, disruptions or other unauthorized actions that would compromise or cripple defense information systems and networks. (Joint Pub 6-0)	1 2 3 4 5 6
Computer Network Exploitation	Enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks. (Joint Pub 6-0)	1 2 3 4 5 6
Computer Network Attack	Actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves. (Joint Pub 6-0)	1 2 3 4 5 6
Hacker Community	Understand the strengths, weaknesses, opportunities, and resources of the hacker community.	1 2 3 4 5 6
Cyber Training and Exercises	Understanding of major training opportunities as well as experience participating in and planning exercises.	1 2 3 4 5 6
Hacker/Adversary Mindset	Ability to creatively explore technology and push it in directions unintended by its designers and, when necessary, the ability to think like an adversary.	1 2 3 4 5 6
Cyber-Warfighter Integration	How to integrate cyber effects into kinetic operations and vice versa.	1 2 3 4 5 6
Kinetic Warfighting	How military forces conduct kinetic operations.	1 2 3 4 5 6
Cyber Warfare Threats	Understand major threat actors and groups in cyberspace.	1 2 3 4 5 6
Intelligence Community Operations	Ability to leverage Intelligence Community (IC) resources in support of cyber operations and	1 2 3 4 5 6

	objectives.	
Emerging Technologies	Awareness of important emerging technologies and their potential impact on cyber operations.	1 2 3 4 5 6
Operational Planning	Ability to plan military operations.	1 2 3 4 5 6

LTC Gregory Conti is a Military Intelligence Officer and Director of West Point's Cyber Security Research Center. He holds a BS from West Point, an MS from Johns Hopkins University and a PhD from the Georgia Institute of Technology, all in Computer Science. He has served as an advisor in US Cyber Command Commander's Action Group (CAG), as Officer in Charge of US Cyber Command's Expeditionary Cyber Support Element in support of Operation Iraqi Freedom, and co-developed US Cyber Command's Joint Advanced Cyber Warfare Course with CDR Caroland.

CDR James Caroland is a Navy Information Warfare Officer, member of the US Cyber Command Commander's Action Group, and an adjunct Associate Professor in University of Maryland University College's Cybersecurity Program. He co-developed US Cyber Command's Joint Advanced Cyber Warfare Course with LTC Conti.

COL Thomas Cook is an Armor Officer, Assistant Professor, and Senior Research Scientist 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.

Mr. Howard Taylor is West Point's National Security Agency Fellow. He holds a BS from Brigham Young University and an MS from the Naval Postgraduate School. He spent 28 years on active duty in the US Navy, advancing through the ranks from Seaman Recruit to Commander. He then continued as a career NSA civilian where he managed complex interagency projects and systems for the US Intelligence Community.

The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Military Academy, Department of the Army, Department of the Navy, National Security Agency, US Cyber Command, Department of Defense, or United States Government.