Shaping the Army's Cyber Operations Force: the Human Dimension

Todd Arnold, Rob Harrison, David Raymond, and Gregory Conti

1 Introduction

By declaring cyberspace an operational domain, the Department of Defense (DoD) acknowledged the criticality for successfully projecting combat power in the domain,[1] and therefore directed all services to create a component command subordinate to U.S. Cyber Command (USCYBERCOM).[2] Since the declaration of this entirely new operational domain, the Army has faced significant challenges such as determining the force structure requirements, capabilities, and the skills required of its cyberspace operators. In order to build a force capable of operating in cyberspace, the Army must determine how to recruit, assess, train, and retain those with the required talent. However, the Army is not the only organization seeking individuals with the ability to operate in cyberspace and it is widely recognized that there is a small talent pool from which to recruit. According to a recent Rand Institute Report, there already exists a shortage of qualified personnel in general, and that problem is exacerbated within the federal government. Such a dearth of talent potentially undermines the nation's security in cyberspace.[3]

Despite this difficult recruiting environment and the heated competition for such talent, the Army needs to attract enough talented personnel to meet mission requirements. The Army also needs to realign skilled personnel who are already serving in different occupational specialties. Particularly now with the creation of a Cyber branch, the Army must man this branch with the right people in the right roles to achieve operational functionality as quickly as possible. In this article we will explore the fundamental skills needed, roles to be filled, and leadership attributes desirable for the Army's cyber force.

2 Early Transformation Initiatives

While Army Cyber Command (ARCYBER) was still an inchoate organization, structural transformations were underway within two existing branches to support what is now known as the

[1] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011. Available at: `http://www.defense.gov/news/d20110714cyber.pdf`

[2] House Armed Services Committee, "Statement of Major General Rhett Hernandez, USA," September 23, 2010. Available at: `http://cryptome.org/dodi/army-cyber.pdf`

[3] Rand Institute, "Hackers Wanted," Jun 17, 2014. Available at: `http://www.rand.org/pubs/research_reports/RR430.html`

Cyber Mission Force (CMF).[4] In 2011, the Military Intelligence (MI) branch dedicated forces to cyberspace operations by creating the 780th MI Brigade to perform intelligence collection and, when called upon, to perform offensive operations.[5] It also created the Military Occupational Specialty (MOS) 35Q – Cryptologic Network Warfare Specialist for enlisted Soldiers.[6,7] Within the Signal Corps, a unit now called the Cyber Protection Brigade,[8,9] was stood up primarily to focus on defensive activities in cyberspace. Additionally, two MOSs were created: 255S – Cyberspace Defense Technician for warrant officers[10] and 25D – Cyber Network Defender for enlisted Soldiers.[11,12]

To mitigate the issue of tracking and identifying personnel with experience, Human Resources Command (HRC) created the E4 Skill Identifer (SI), awarded by ARCYBER, to identify soldiers who have served a tour in an operational cyber unit or who possess the required skills to conduct cyberspace operations. The biggest leap forward occurred August 21, 2014 (effective September 1, 2014) when the Army created a new branch to support a career path for Soldiers, warrant officers, and officers that would allow them to specialize in cyberspace operations. The first call for applications for active duty officers between the ranks of lieutenant and colonel was released

[4]Andrew Tilgham, "As Cyber Force Grows, Manpower Details Emerge," September 23, 2014. Army Times. Available at: http://www.armytimes.com/article/20140923/NEWS/309230050/As-cyber-force-grows-manpower-details-emerge

[5]Tina Miles, "Army Activates First-of-its-Kind Cyber Brigade," December 9, 2011. 780th MI Brigade. Available at: http://www.army.mil/article/70611/Army_activates_first_of_its_kind_Cyber_Brigade/

[6]Joe Gould, "Be an Army hacker: This top secret cyber unit wants you," April 8, 2013. Army Times. Available at: http://www.armytimes.com/article/20130408/CAREERS/304080008/Be-an-Army-hacker-top-secret-cyber-unit-wants-you. This MOS is open to E3–E7. The initial qualification for being re-classed as a 35Q was to pass the Joint Cyber Attack Course

[7]COL Jake Conway, "Cryptologic Network Warfare Support to Cyber: Recruit, Train, Sustain and Retain," March 27, 2014. Technet Land Forces South. Available at: http://www.afcea.org/events/tnlf/southwest/documents/Tr1S1MIConway.pdf

[8]Siobhan Carlile, "Army recruiting highly qualified Soldiers, DA civilians to serve on new specialized Cyber Protection," October 8, 2013. 7th Signal Command (Theater) Public Affairs, Army.mil. Available at: http://www.army.mil/article/112793/Army_recruiting_highly_qualified_Soldiers__DA_civilians_to_serve_on_new_specialized_Cyber_Protection/

[9]Cyber Protection Brigade. Available at: https://cpb.army.mil

[10]CW5 Todd M. Boudreau, "Cyberspace Defense' Technician (MOS 255S)," 2011. Army Communicator, Volume 36. Available at: http://www.signal.army.mil/armyComArchive/2011/Vol36/No1/2011Vol36No1Sub09.pdf. The Cyberspace Defense Technician is assessed at the senior CW2 level, with feeders coming from the Signal Corps' 250N/255N (Network Management Technician/Cyberspace Network Management Technician), 251A/255A (Information Systems Technician/Cyberspace Content Management Technician), and 254A (Signal Systems Support Technician) warrant officers. A Cyberspace Defense Technician undergoes 25 weeks of training in defensive techniques, with over half the training being provided by the SANS Institute.

[11]Wilson A. Rivera, "Cyberspace warriors graduate with Army's newest military occupational specialty," December 6, 2013. Fort Gordon Public Affairs Office. Available at: http://www.army.mil/article/116564/Cyberspace_warriors_graduate_with_Army_s_newest_military_occupational_specialty/

[12]David Vergun, "Cyber Network Defender MOS now open to NCOs," April 14, 2014. Army Public Affairs. Available at: http://www.army.mil/article/123328/Cyber_Network_Defender_MOS_now_open_to_NCOs/. In order to qualify for the new 25D MOS, a soldier at the rank of staff sergeant must have a minimum of eight years service and pass the 25D In-Service Screening Test (ISST).

October 8, 2014, a Voluntary Transfer Incentive Program (VTIP) panel met in December 2014, and approximately 140 officers were selected to being filling the branch.[13]

While the first call for officers has already begun, this is only one small step in a longer process to bootstrap the nascent Cyber branch. The Army is still defining what fundamental attributes and competencies are common to all members of the Cyber branch, how to align personnel against roles in the branch, and what qualities are needed of leaders in this new domain. In the following sections, we will more clearly define and discuss the demand for technical competence and propose common areas of knowledge required for all members of a Cyber branch, analyze the roles in which Cyber branch Soldiers and officers can serve, and develop the attributes that we believe differentiate the leaders of this branch from the followers.

3 Operating in the Cyberspace Domain

3.1 Nature of the Domain

> Cyberspace is "[a] global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[14]

As reflected in the definition above, cyberspace is a complex and evolving conglomeration of technologies; within which Cyber branch personnel must learn to operate and maneuver. Competent cyberspace operators must be knowledgable in many aspects of cyberspace, regardless of their role (as defined in Section 5). Due to the breadth and depth of the domain, operators will likely become experts in only one or two aspects of cyberspace – it would be a daunting and unrealistic task to expect a cyber operator to be a master of all apsects of cyberspace technology and operations. However, a casual level of familiarity with the remaining aspects is insufficient. A competent cyberspace operator need possess the foundational knowledge in all the aspects of cyberspace and possess the aptitude to quickly become proficient in a new specialty given time and effort.

3.2 Technical and Tactical Competence

Regardless of an individual's rank or position, we argue every individual in the Cyber branch must be capable of operating within the cyberspace domain. This is especially true for officers; leaders must be able to maneuver as effectively as their Soldiers in any domain, thereby demonstrating their technical and tactical proficiency – a fundamental tenet of Officership. Such officers would have little difficulty leading and maneuvering in cyberspace, or providing advice on the integration of cyberspace effects to complement kinetic operations.

The Cyber branch has been recognized as an operational branch and placed within the Operations functional category. Therefore, its leaders will be expected to be experts within their specific

[13] Jim Tice, "Officers Can Apply to go Cyber in Voluntary Transfer Program," October 8, 2014. Army Times. Available at: `http://www.armytimes.com/article/20141008/CAREERS03/310080059/Officers-can-apply-go-cyber-voluntary-transfer-program`

[14] Joint Chiefs of Staff, "Joint Publication 3-0: Joint Operations," August 11, 2011. Available at: `http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf`

and unique warfighting functions, similar to officers in the other operational branches. Officers, especially junior company grade officers, are expected to maneuver alongside their Soldiers while leading and conducting operations within their specific warfighting functions. Conceptually, the Cyber branch should be no different with the exception that instead of maneuvering on land, officers of the Cyber branch will operate in cyberspace. Therefore, we assert that officers, especially at the company grade level, *should be as hands-on as possible*. This will give them the operational experience, technical competence, and perspective needed to serve in positions of increasing responsibility.

With such a high bar of technical and tactical competence set, the Army can ill-afford to rush and "fill the ranks" of the Cyber branch immediately. Exigence should not be a subtitute for excellence; the Army should recruit and assess only capable and qualified individuals in this early bootstrapping of the Cyber branch.[15] The skills required to effectively maneuver in cyberspace are separate and distinct from those required of system administrators, compliance auditors, or help-desk personnel.[16] The skills required of the Army's cyberspace operators are more complex, require an in-depth knowledge of multiple topics and an agility within the cyberspace domain. We propose these foundational skills and attributes in the following sections.

3.3 Foundational Aspects of Cyberspace

Starting with the above definition of cyberspace, we may begin to enumerate all of the individual knowledge areas the cyberspace domain encompasses. Such a list quickly becomes unmanageably long so we use the following broad categories to group areas by technology. We believe the following seven areas are essential to an operator's ability to successfully maneuver in the cyber domain. These areas (for a more detailed list of the sub-topics within each of these areas, please see Table 3 in the Appendix, in no particular order, are:

- Computer architecture
- Operating systems
- Electricity and electromagnetic radiation/propagation
- Programming language(s)/algorithms
- Computer Networking and Telecommunications
- Cryptography
- Data storage and information retrieval

[15] Don Dodge, "How to get a Job at Google, Interview Questions, Hiring Process," September 14, 2010. Available at: `http://dondodge.typepad.com/the_next_big_thing/2010/09/how-to-get-a-job-at-google-interview-questions-hiring-process.html`. Other organizations which rely on technical competence would rather leave a position unfilled than fill the position with an unqualified individual. The Cyber branch should be no different.

[16] Rand Institute, page 47.

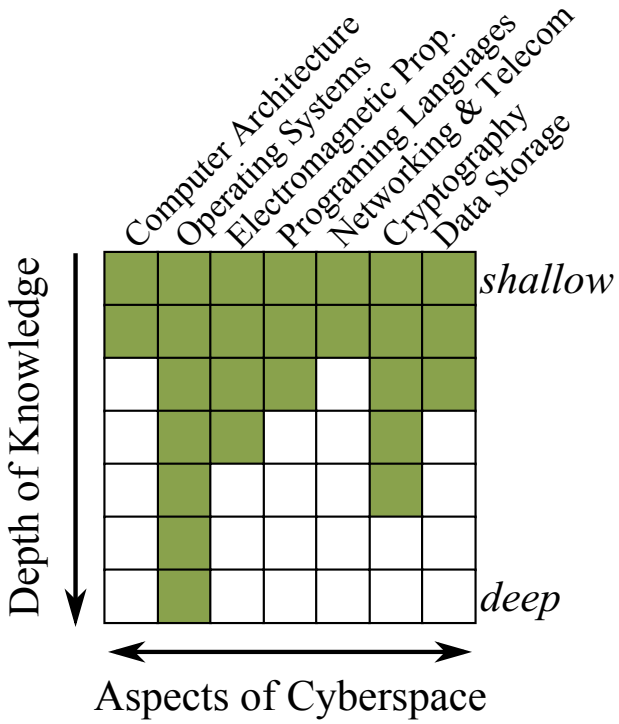

Figure 1: In this figure, we can see an example of the different levels of mastery an individual in cyberspace operations may achieve. While the fictional individual may be considered a subject matter expert in Operating Systems, they are also extremely knowledgable in Electicity and Electromagnetic Radiation/Propagation and Cryptography. This combination of skillsets could indicate someone who possesses a strong skillset for working on mobile devices. Also of note is they have more than a cursory familiarity with the other four areas.

While these categories may seem like a broad and disconnected set of technologies, they are what we believe encompass the fundamental aspects of understanding the cyberspace domain defined above.[17] There will be a need for the Cyber branch to have personnel who are experts in a single area (or sub-area) listed above, but all operators must have a solid foundation in the other aspects of the domain (see Figure 1 for a visual representation of a typical Cyber branch personnel's distribution of knowledge). Such a strong foundation is not achieved overnight; it will require time, education, and experience. Once a basic foundation is established, individuals can begin to master multiple areas which would result in more advanced skillsets. For instance, a strong understanding of operating systems, architecture, and programming would allow someone to easily take on reverse engineering; similarly, one interested in forensics might first build a foundation in operating systems, data storage, and cryptography.

While it is desirable for some operators to become highly specialized, to the point of mastery, it is not desirable for all personnel to do so. The Cyber branch will need to rely not only on personnel with deep knowledge who enable specific capabilities but also those with broad knowledge who plan, approve, and execute full-spectrum operations in this domain.

[17]The degree to which this list can be considered an exhaustive list of technologies encompassing the cyberspace domain is debatable and not meant to be the final authoritative answer.

4 Attributes of Leaders in the Cyber Branch

The Cyber branch needs leaders who are unquestionably technically competent, but at the same time are able to *lead* the Soldiers and organizations within the branch. If leaders were selected based solely on technical competence, the Cyber branch would be managed by technicians. Conversely, if leaders were selected solely on generalist leadership attributes, the branch would be managed by those lacking an understanding of its most basic tactics. Surely, fissure would result along technical comptence and managerial lines. Only by fostering the development of *technical leaders* will the Cyber branch find success and legitimize its existence among other operational branches. Most of these leadership characteristics are difficult to quantify, but must be considered when evaluating and screening candidates for leadership positions in the Cyber branch.

Solid Ethical Foundation: One of the most critical aspects of all personnel within the Cyber branch is an ethical foundation. Personnel who receive the specialized and extensive training as a member of the Cyber branch will undoubtedly possess the ability to create and employ sophisticated and devastating effects in cyberspace. The Army must have the utmost confidence that Cyber branch operators will not engage in vigilantism and will only employ their skills within the carefully defined limits of professional conduct. This point may seem trivially obvious – we expect that our stewards of land combat power abide by the laws of land warfare and will not intentionally target innocents. However, similar employment of combat power in cyberspace is often less perceptible and attribution is difficult,[18] making ethical transgressions both easier to commit and less likely to be caught.

Creativity: As mentioned previously, the cyberspace domain evolves rapidly and the change in a couple lines of code change could render a technique or a piece of software ineffective or even useless.[19] Cyber branch officers must possess the ability to adapt to this perpetually dynamic environment and to solve ill-defined problems.

Passion: Leaders must possess a passion for executing operations and an eagerness for understanding the cyberspace domain. No conventional maneuver leader would sneer at difficult road marches or challenging field problems. Similarly, no leader at any level in the cyberspace domain should discount topics as "too nerdy" or beyond their ability to comprehend. Rather, a passionate leader would not allow themself to be placed in such a position.

Team Player: The lone hacker is not able to accomplish what a cohesive and competent team of cyberspace operators is able to achieve.[20] Leaders should be capable of building a team of diverse

[18]David D. Clark and Susan Landau, "Untangling Attribtion," 2011. Harvard National Security Journal. Available at: `http://cs.brown.edu/courses/csci1950-p/sources/lec12/ClarkandLandau.pdf`. This is known as the *Attribution Problem* and is a known challenge within the cyberspace domain.

[19]For an example of a simple fix for a critical flaw in a piece of software, an explanation on the fix for the Heartbleed vulnerability can be found at `http://www.theregister.co.uk/2014/04/09/heartbleed_explained/`.

[20]David Fulghum, "Solitary Genius Trumped by the Socially Adept," July 30, 2012. Aviation Week and Space Technology. Available at: `http://aviationweek.com/awin/solitary-genius-trumped-socially-adept`

individuals, with myriad skillsets, to accomplish a mission. Not only must they be capable of building a cohesive team, they must also be able to *operate* as a member of a team or to recognize who has more expertise or experience to achieve mission success.

Self Education and Development: As already mentioned, the cyberspace domain evolves very rapidly, so leaders will need to be very adaptable. If leaders are not constantly engaged in self-development, they may quickly find their skills languishing or becoming irrelevant. A high degree of self-development is also an indicator for passion, and the following three attributes indicate one's capacity for engaging in self-development.

Intellectual Curiosity: Accumulating a large body of knowledge can help someone achieve a level of success, but such a body of knowledg can quickly become stale in cyberspace. A competent leader in the Cyber branch must possess an "innate driving interest to understand what goes on within computer applications."[21] Such a drive compels one to seek out new problems and decompose unknown systems because nothing can be left to mystery and happenstance. This process is self-reinforcing; by constantly engaging in decomposition and discovery, new problems present themselves while others become understood. This curiosity becomes intellectual when it is transformed into an interest in *problems* provoked by the observation of things and the accumulation of material.[22] Individuals possess the proper amount of intellectual curiosity when they want and are able to tackle problems on their own with minimal guidance and direction. Rather than quickly capitulating to a difficult problem, they instead resolutely dig in and achieve success.

Inference: In many cases, all of the facts relevant to a problem or technology may not be apparent when a leader is faced with a challenge. To solve such challenges requires the ability to analyze and determine that present facts suggest other facts (or truths) in such a way as to induce belief in the latter. The exercise of inference involves a jump, a leap, a going beyond what is surely known to something else accepted on its warrant.[23] Inference is enhanced by intellectual curiousity, and is a building block towards the next characteristic.

Critical Thinking: Building upon intellectual curiosity and inference, Cyber branch officers must be able to think critically in order to make sound and rapid decisions to accomplish their mission. "The essence of critical thinking is suspended judgment; and the essence of this suspense is inquiry to determine the nature of the problem before proceeding to attempts at its solution. This, more than any other thing, transforms mere inference into tested inference, suggested conclusions into proof."[24]

Operational Mindset: The combination of the previous few traits (self development, intellectual curiosity, critical thinking, and inference) must be applied in the proper direction. Personnel who possess "personality characteristics that correlate well with cybersecurity requirements, notably an

[21] Rand Institute, pg. 33
[22] John Dewey, "How We Think," 1910, page 32-33
[23] Ibid., page 26.
[24] Ibid., page 74

intense curiosity with how things work (and can be made to fail)"[25] will not think only in terms of defensive maneuvers or traditional methods of security. Rather, they must possess an operational mindset allowing them to approach a scenario from both offensive and defensive perspectives. They can harden a piece of software because they can determine how to break it.

We believe the combination of these attributes will result in leaders who are confident, capable, and competent leaders within the cyberspace domain who are proficient at conducting both Defensive and Offensive Cyberspace Operations (DCO/OCO).

5 Roles Within the Cyberspace Misson Force

We assert that these previously discussed core competencies (Section 3.3) apply for all cyberspace operators and that leaders in this domain must also display certain attributes (see Section 4). From this corps of people, the CMF must be manned.

In the CMF there are five main roles that will need to be filled: operator, planner, analyst, developer, and leader. Traditionally Soldiers perform job-specific tasks, Non-Commissioned Officers (NCOs) train Soldiers and small units on tasks, warrant officers perform deeply technical functions, and officers provide planning and leadership. While this paradigm is *generally* applicable, the deeply technical nature of the cyber domain precludes the drawing of lines as clearly as in other branches. In Table 1, we propose one feasible mapping of the traditional rank structure onto the roles in the CMF.

Rank	Role	Description
Enlisted Soldier	Cyber Operator, Analyst/Collecter	Employs tools, conducts operations, etc. Is the primary operator for operations in cyberspace.
NCO	Cyber Operations, Technology Leadership	May employ tools and conduct operations, also responsible for training Soldiers on the use of tools, and Tactics, Techniques, and Procedures (TTPs). May be in charge of small teams, such as a development team within a project or an operational team responsible for deploying a specific type of toolset.
Warrant Officers	Senior Operator, Senior Analyst	Technical expertise on use and employment of tools, and create training programs for the employment of tools. May be team member within a project or the project lead.
Officers	Leadership	Serve as operational team leads, commanders, project team leads.

Table 1: Roles of cyber Soldiers broken down by traditional rank.

The traditional roles as defined by rank should be a guideline for the Army's structure in cy-

[25] Rand Institute, pg. XI.

berspace, but it should not be the definitive requirement. Table 2 provides a look at the roles unique to cyberspace operations which we believe should not have a specific rank assigned to them. Rather, these roles should be filled based on matching the specific talents required of the positions to those of the individuals selected to fill them.

Role	Description
Developer/Technical Expert	Programmer, tool development, and other advanced topics in cyberspace operations (we define this broadly to include topics such as reverse engineering). Regardless of rank, there will be individuals whose skills and abilities at coding (a.k.a. super coder) or other areas of expertise within the Cyber Domain dictate they should only serve in development positions. Roles outside of their area of expertise will greatly diminish their skillset and ability to contribute. For example, someone who is adept at reverse engineering Linux binaries should not be assigned to work on Windows driver development.
Cyberspace Operational Planner	These are the individuals who are able to integrate the desired effects and outcomes, the tools required, and the tactical, operational, and strategic planning. Planning and execution of these plans may take an extended period of time to complete, as the planning for a successive operation may not be possible prior to completion of the current mission. Additionally, based on their intimate knowledge of the battlespace and current operations, planners (along with cyberspace operators) should generate requirements for tool developers based on operational requirements.
Technical Lead/Integrater	Technically proficient in more than one area but not as specialized as a developer or technical expert. These individuals should serve as the technical adviser/lead/director on a project, within a division or planning cell, or to commanders.
Adviser	Serve as top technical adviser to a commander. Individuals who fill these roles are most able to communicate cyber capabilities and how to intregrate their employment with traditional kinetic operations. Commanders at all levels would need to be educated that an adviser's rank does not diminish their knowledge or expertise.

Table 2: Roles within cyber operations that fall outside of traditional rank structure, which we contend makes them rank immaterial. These roles should be filled based on technical ability and competency rather than purely on rank or MOS.

6 Conclusions

Winning in cyberspace is a national security imperative. A clear argument for a cyber service has been made.[26,27] Until our nation commits to such a grand reorganization, the onus is on *all* of the services to operate and man the CMF. While our Army is second to none in projecting land combat power, it is rapidly working towards projecting power in cyberspace and to create a corps of professional cyberspace operators. The competencies and attributes we described could be used as a guide for the Army to start actively recruiting and building and premier force that will win in cyberspace.

About the Authors

Major Todd Arnold is an FA24 and former Signal Corps officer, currently assigned to the Advanced Concepts and Technologies Division of ARCYBER. He holds an M.S. from the Pennsylvania State University and a B.S. from the United States Military Academy (USMA) at West Point, both in Computer Science. His previous assignments include two tours in Operation Iraqi Freedom (OIF) with the 22d Signal Brigade, developing, testing, and analyzing CNO capabilities in support of current and future contingency operations for NSA and USCYBERCOM, and as an Assistant Professor in the Department of Electrical Engineering and Computer Science (EE&CS) at USMA.

Major Rob Harrison is an FA24 and currently assigned to the Advanced Concepts and Technologies Division of ARCYBER. He holds an M.S.E. and B.S. from Princeton University and the United States Military Academy, respectively, both in Computer Science. Rob has completed three combat tours in support of OIF with both conventional Signal Corps and Special Operations units in a variety of capacities, and served as an Assistant Professor in the Department of EE&CS at USMA.

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

Colonel Gregory Conti is a Military Intelligence Officer and Director of the Army Cyber Institute at West Point. He holds a Ph.D. from the Georgia Institute of Technology, an M.S. from Johns Hopkins University and a B.S. from West Point, all in computer science. He has served as a senior adviser in USCYBERCOM Commander's Action Group (CAG), as Officer in Charge of a

[26]Gregory Conti and John "Buck" Surdu, "Army, Navy, Air Force, Cyber: Is it Time for a Cyberwarfare Branch of the Military," 2009. Information Assurance Newsletter, Vol. 12, No. 1, Spring 2009, pp. 14-18. Available at: `http://www.rumint.org/gregconti/publications/2009_IAN_12-1_conti-surdu.pdf`

[27]James Stavridis and David Weinstein, "Time for a U.S. Cyber Force," January 2014. U.S. Naval Institute, Proceedings Magazine Vol. 140/1/1,331. Available at: `http://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force`

deployed USCYBERCOM Expeditionary Cyber Support Element, and co-developed USCYBERCOM's Joint Advanced Cyber Warfare Course. He served in the Persian Gulf War and in Operation Iraqi Freedom.

Disclaimer

The views expressed in this article are those of the authors and do not reflect the official policy or position of West Point, Army Cyber Command, the Department of the Army, US Cyber Command, the Department of Defense, or the US Government.

Appendix

Areas of Competency Sub-topics

The following table is intended to expand on the seven areas of competency as defined in Section 3.3. This list is not meant to be all-inclusive, but lists specific examples of topics within each of the broad categories previously identified.

Area	Example Topics
Computer architecture	Memory hierarchy, instruction set, multiprocessing, distributed processing, multithreading, digital logic, assembly language, bus technologies, HDD, SSD
Operating systems	Resource management, security concepts/security rings, user authentication and roles, scheduling, synchronization, kernel vs user level, device drivers, program execution, interrupts, processes, threads, virtual memory, Executable and Linkable Format (ELF), Portable Executable (PE), virtualization, hypervisors (type 1 and type 2)
Electricity and electromagnetic radiation/propagation	Digital logic, wireless technologies, radio wave propagation, electromagnetic spectrum, cellular technologies
Programming language(s)/algorithms	Recursion, functions, data structures, syntax, compilers, abstraction, linking, efficiency, optimization, Assembly, C, C++, Python, Java, Javascript, scripting, procedural/object oriented/functional programming
Networking and data communications	OSI Model, networking protocols (TCP, UDP, IP, IPv6, etc.), routing protocols, layer 2 protocols, Software Defined Networking (SDN), cellular technologies, 802.11, 802.16, Access Control Lists/firewalls, queuing theory, service applications (HTTP/HTTPS, DNS, etc.)

Cryptography	Data at rest, securing communications, Cellular Message Encryption Algorithm (CMEA), public/private key encryption, hashing algorithms,
Data storage and information retrieval	File systems, HDDs, SSDs, databases, SQL, forensically sound data transfer/recovery

Table 3: Detailed breakdown of knowledge required within each of the areas which encompass cyberspace.