AIR WAR COLLEGE

AIR UNIVERSITY

CYBERFORCE 2025:

CRAFTING A SELECTION PROGRAM FOR TOMORROW'S CYBER WARRIORS

By

George E. Tromba, Lt Col, USAF

A Research Report Submitted to the Faculty

In the Fulfillment of the Graduation Requirements

Advisor: Robert A. Douglas, Col, USAF

14 February 2013

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the United States government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Colonel George E. Tromba is a U.S. Air Force Space Operations Officer attending the Air War College, Air University, Maxwell AFB, AL. He graduated from Texas State University with a Bachelor's degree in Economics where he was also commissioned through the ROTC program. He received subsequent Masters Degrees in Systems Management, and International Relations and Policy from Golden Gate University, and The Naval War College. He has served in a variety of assignments to include Space Control Squadron Commander, HQ Air Staff A3 Space Control Division Chief, Joint Staff J3 Special Technical Operations Planner, and NRO Squadron Operations Officer.

Abstract

The onset of the present information age, and the national security threats and opportunities posed by the wild-wild west of the cyber domain are as daunting as those ushered in with the birth of the Cold War. Whereas the Cold War yielded a unifying strategy in NSC 68 and groundbreaking forces in the nuclear navy and the US Army Green Berets, to date the underwhelming US response to the pressing cyberspace challenge has consisted of publishing inadequate national, DoD and Service strategies, and the Air Force's adoption of cyberspace as one of its three core missions. Unfortunately, the service's utilization of traditional military accession and training methodologies for its cyber forces neither scientifically nor holistically assess the intelligence, personality, and skills a competent cyber operator requires to execute the technical depth or operational breadth needed to prosecute cyberspace superiority operations. Through examination of the threat, legal/policy, strategy and technology environments that comprise the cyberspace domain, a survey of contemporary intelligence, personality and skill assessment methodologies, and an analysis of nuclear navy and US Army Special Forces selection/accession programs, this paper will develop desired cyberspace warrior attributes and propose a viable and robust selection and accession program for Cyberspace warriors.

Introduction

"Where is the prince who can afford so to cover his country with troops for its defence, so that ten thousand men descending from the clouds might not, in many places, do an infinite deal of mischief before a force could be brought together to repel them?"

Benjamin Franklin 1784

The onset of the cold war ushered in an environment fraught with developing threats, immature and developing security strategy and policy marked by rapid advances in civil and military technology, and rapidly developing tactics, techniques and procedures (TTPs) necessary to employ revolutionary weapon systems. The present information age, and its ever increasing national security threats and opportunities posed by the wild-wild west of the cyber domain is equally demanding, and if the US is to navigate it successfully then our response must prove equally astute. In response to the cold war the US crafted a unifying strategy in NSC 68 and along supporting lines fielded two groundbreaking forces; the nuclear navy, and the US Army Special Forces (SF). In the afterglow of the US' 'winning' the Cold War there were ample post-mortem opinions, facts and myths as to the underlying cause for success, and albeit a varied response these forces played a significant role. In response to the current national security challenge posed by cyberspace the US published elements of a cyber strategy, and for its part the US Air Force (USAF) adopted cyberspace to form its new triumvirate air, space and cyberspace mission set, stood up new officer and enlisted career fields, and training and accession pipelines. The service selects these cyber warriors using traditional assessment and training methods centered on Armed Services Vocational Aptitude Battery (ASVAB) and Air Force Officer Qualifying Test (AFOQT) scores, career field desires of prospective candidates, and performance at Undergraduate Cyber Training courses. Unfortunately, the intelligence, personality, and skills a competent operator requires in order to actively defend, exploit or attack

computer networks are neither scientifically nor effectively assessed using these methods alone.[1] Therefore, given the strategic criticality of the cyber domain to our national security and Joint Operations it is a national imperative that the USAF develop and implement a robust selection program for cyber warriors that scientifically and holistically assesses intelligence, personality and skill; crafting a cyberforce second to none. By examining the threat, legal/policy, strategy and technology environments that comprise the cyberspace domain, surveying existing intelligence, personality and skill assessment methodologies, and analyzing historic selection/accession programs, this paper will develop desired cyberspace warrior attributes and propose a viable selection and accession program for Cyberspace warriors.

Cyberspace Domain

Joint and Air Force doctrines define cyberspace as a man-made global domain comprised of mutually dependent networks of information technology infrastructures with nodes that physically reside in in the air, land, sea and space domains.[2] However, while this definition is sufficient for the un-indoctrinated, it is insufficient as a point of departure in extracting desired/required cyberspace force attributes. Therefore, in order to better identify these cyberspace warrior attributes, this section examines the threat, legal/policy, strategy and technology environments that comprise the cyberspace domain.

Threat Environment

The cyberspace threat environment compels the requirement for robustly capable cyber forces. Upon review, the threats are vast and varied, derived primarily from the all too familiar lexicon of state and non-state challengers.

One of the pressingly relevant state actors posing the most seemingly consistent challenge to our national cybersecurity is China, who presents a domain shaping dual-challenge

phenomenology. The first phenomenology is their collective resistance to establishing international cyber "norms of behavior" in accordance with the Law of Armed Conflict (LOAC) framework; a position the US favors.[3] Establishing norms benefits the US and international community by clarifying what constitutes acts of war, espionage, crime and appropriate responses. Their resistance is unsurprising, as China would cede maneuverability within cyberspace under codified norms. For now, they appear more interested in limiting their own citizenry's free exchange of information than protecting critical infrastructure against cyber vulnerabilities.[4]

China's second challenge is their more than anecdotal commitment to exploitive and offensive cyberspace doctrine and actions to shape and achieve favorable strategic outcomes which should inform how we select/access cyber operators. With regards to doctrine, there is precious little within open sources regarding their specified cyberspace doctrine save the curious book "Unrestricted Warfare," written by two People's Liberation Army (PLA) officers in 1999.[5] The authors give significant weight to adversarial computer network operation effects stating "the influence exerted by a nuclear bomb is perhaps less than the influence exerted by a hacker."[6] In execution, China's penchant for state-sponsored hacking has elicited 'knock-it-off' calls from others. In 2007 the PLA's efforts to siphon off mountains of data using a Trojan horse program to rout captured data from government agencies in Germany to Beijing reached such untenable levels that Chancellor Angela Merkel personally broached the subject in meetings with Premier Wen Jiabao.[7] Additionally, in 2003 a PLA hacker's computer network exploitation (CNE) of Florida's power grid unintentionally morphed into an attack as his exploitation went one step too far; darkening much of Florida.[8] China's actions typify the threat US cyber

operators will operate against, and also what happens when selection programs fail to 'weed-out' flawed hacker personality traits.

The topography of rogue and non-state bad actors offers no relief either. Collectively they have demonstrated the ability to conduct a range of offensive operations including DDoS, website defacement, and Trojans and Viruses. Albeit on a limited scale, the impacts are real as Israel experienced first-hand during their operations against Hamas in Operation Cast Lead. Hamas and supportive 'civilian' hackers were the source of at least 10,000 website attacks within just one week of the operation.[10] Thankfully, they have not yet demonstrated the capability to launch crippling infrastructure attacks of the Stuxnet variety levied against Iran's nuclear program, by an as of yet unidentified actor. Unfortunately, the cyber arms market, where these malware and botnets are promulgated, is only warming up and is by no means limited to state actors. The impact and potential of the non-state threat requires cyber warriors who can defend/respond against it; the demonstrated challenge is determining against whom or what to respond. This dilemma illustrates that any cyber forces selection program needs to identify candidates with the forensic and deductive mind of Sherlock Homes.

Legal/Policy Environment

The legal/policy environment provides additional insight into the kind of intelligence and personality traits requiring evaluation in any cyber warrior selection program. The challenge is much of it remains underdeveloped, leaving only current ill-adapted international kinetic-based frameworks and governing bodies such as the LOAC and International Telecommunications Union (ITU), and slow-to-respond domestic law enforcement approaches oriented primarily towards the prevention of child pornography and domestic spying by the US intelligence community. Internationally, the ITU and some nations are working to establish operative and

behavioral norms for cyberspace but as of yet there are no agreed upon frameworks. The ITU also published a "National Cybersecurity Strategy Guide;"[11] however, this is less a proscriptive international cyberspace policy and more a domestic policy guide. Domestically, the only real innovation has come in revamped Foreign Intelligence Surveillance Act Amendments.[12] However, their legality and effectiveness are still up for debate and final resolution. The underdeveloped legal/policy environment coupled with the dispersed and nomadic nature of the cyber threat make it evident that any truly effective response will traverse statutory authorities vested in law enforcement, homeland defense, intelligence, and military operations, either serially or near-simultaneously. Therefore, what makes the underdeveloped legal/policy environment germane to cyber warrior selection is its illustration of the need for a nimble mind that can operate across the spectrum of statutes with the restraint of a law enforcement officer, the protective calculus of a National Guardsman, the stealthiness of an intelligence operative, and the devastating hammer of a bunker buster.

Strategy Environment

The strategy environment compounds the list of potentially required attributes for competent and capable cyber forces. From the national to the Service level, existing cyberspace strategies either lack taskable clarity or are so sufficiently all-encompassing that the inherent tasks for cyber forces are significant enough that again the traditional accession and training methods prove inadequate.

At the national level, the White House released its long awaited US Strategy for Cyberspace in May, 2011. It identifies cyberspace as a "national asset," and sets the goal of network "openness and interoperability," while remaining secure, reliable, trustworthy and resilient.[13] Additionally, the strategy states the nation's cyber policy will preserve foundational

freedoms such as “freedom of expression, privacy,” and the “free flow of information.” The inherent military tasks are to “dissuade and deter malicious actors, and reserve the right to defend…as necessary and appropriate.”[14] It also promulgates the requirement to work with less developed nations to build their own technical capacity as part of its ‘dissuade and deter’ approach to national cyberspace defense.[15]

Within the Joint/DoD construct, the 2011 DoD cyber strategy not only stakes out its responsibility to defend DoD networks it also ties military operations and effectiveness to the US’ critical infrastructure and key elements of economic vitality such as intellectual property.[16] In addition to establishing extensive left and right limits of potential DoD operating space within the cyber domain the strategy establishes core initiatives:

Table-1[17]

DoD Strategy for Operating in Cyberspace		
No.	Initiative	Rationale/Approach
1	Treat cyberspace as an operational domain to organize, train, and equip	Enable DoD to take full advantage of cyberspace’s potential
2	Employ new defense operating concepts	Protect DoD networks and systems
3	Partner with other U.S. government departments and agencies and the private sector	Enable a whole-of-government cybersecurity strategy
4	Build robust relationships with U.S. allies and international partners	Strengthen collective cybersecurity
5	Leverage the nation’s ingenuity	Use an exceptional cyber workforce and rapid technological innovation

Lastly, at the service level, the USAF completed its “Cyber Visions 2025” study in July 2012. It advocates a strategic vision to “Assure cyber advantage across air, space, cyber, C2ISR, and mission support.”[18] The specified/implied cyber tasks include:

Table-2[19]

1.	Conducting mission assurance operations "in congested, competitive, contested, and denied environments in spite of increased dependencies, vulnerabilities, and threats."
2.	Execute defend and exploit operations.
3.	Gain/maintain advantages in agility and resiliency over challengers.
4.	Gain/maintain superiority within and across the cyber domain.

Collectively, the strategy environment levies significant requirements on the intelligence, personality and skills of today's and tomorrow's cyber warriors. This reaffirms the necessity for a robust selection program that assesses these attributes in order to ensure strategy task accomplishment.

Technology Environment

The last, however certainly not the least, environment within the cyber domain requiring summary assessment is the technological one. This environment sets the relatively hard constraints/restraints and given its requisite impact on cyber operations, and the warriors who must succeed there, requires its inclusion in determining needed traits and abilities in a cyberforce. Due to its very nature, the technological environment is constantly changing; which in and of itself presents an identifiable attribute. Specifically, Antoine Bousquet states, "modern technology is something incomparably different from all earlier technologies because it is based on modern physics as an exact science."[20] However, the reverse is also accurate: "modern physics, as experimental, is dependent upon technical apparatus and upon progress in the building of apparatus."[21] This proves the innate complexity of the technology environment and, as this complexity advances, so too will the need for increasingly specialized expertise and skill.[22] Antoine Bousquet may have captured the nature of it best when he coined the derivative term "chaoplexic" lending from contemporary chaos and complex adaptive system theories to describe it.[23] Aside from the obvious machines, poles and wires that compose it, the ones and

zeroes that traverse it, and apart from the aforementioned more cerebral attempts at defining it, the figure below depicts the constantly moving continuum of readily observable elements of the cyber domain's technology environment.

Figure-1

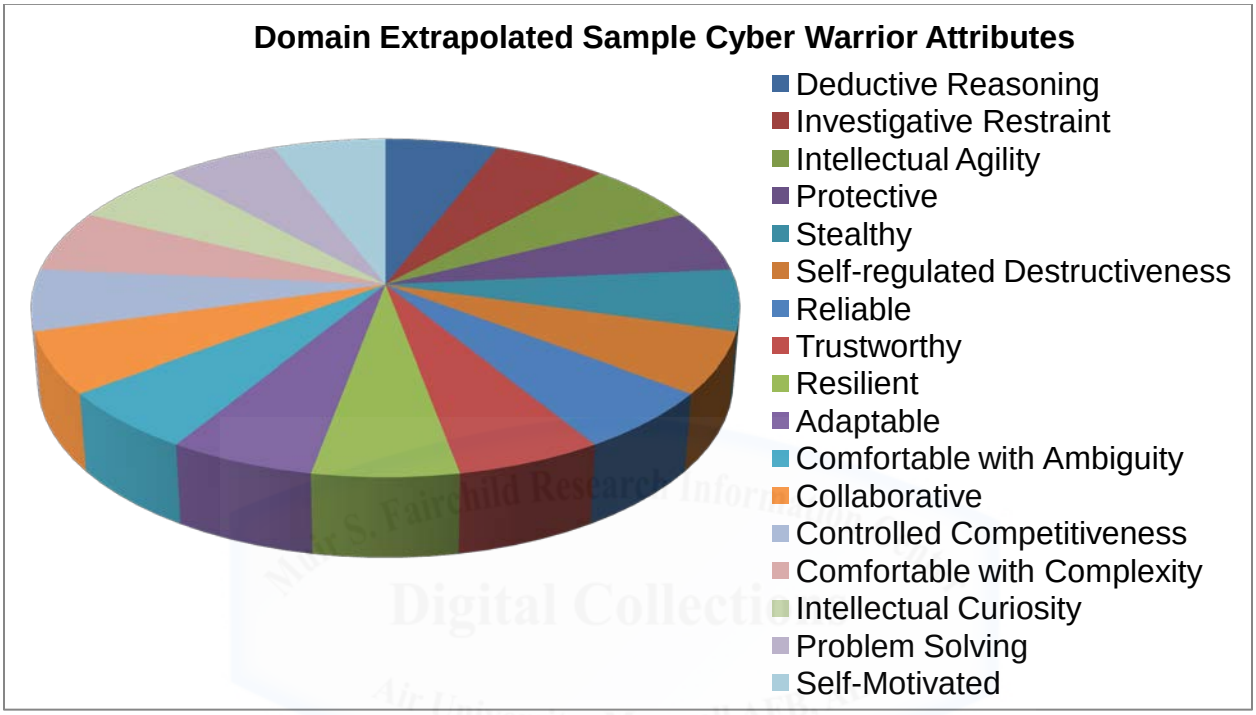
The fact that at any given moment the influence of one, some or all are observable within the cyberspace domain, and some or all may either work in concert together or in diametric opposition to each other is what makes the domain's technological environment, in Bousquet's words, truly chaoplexic.

Assessment Methodologies

Examination of the cyberspace threat, legal/policy, strategy, and technology environments not only provides additional impetus for robust cyber warrior selection but also maps the three categories of potentially desired/required attributes of intelligence, personality and skill such a program should scientifically and holistically assesses. However, as a stand-alone method, while informative, as Figure 2 illustrates, surveying the environmental elements of

the cyber domain is insufficient to fully craft a true selection program. Fortunately there are existing scientific and academic methodologies to adopt with regards to identifying and testing for desired/required intelligence, personality, and skill.

Figure-2



Intelligence Assessment

Intelligence (IQ) testing is a decades-old science initially born out of a need to identify children entering school who potentially required assistance.[24] Today, IQ tests are used to assess a multitude of attributes and are given to all ages, for everything from determining educational giftedness and learning disabilities of students, to the cognitive intelligence of prospective adult employees. Even the NFL uses an IQ test known as the Wonderlic Cognitive Ability test with its incoming rookies. Most NFL teams have minimum desired/required scores assigned to each football position for any rookies they may potentially draft. One of the more current and commonly used adult IQ tests is the Wechsler Adult Intelligence Scale – fourth edition (WAIS-IV), which currently tests four primary and eleven sub areas.[25]

Table-3

WAIS-IV Test			
Primary Test Area	Sub-test Areas		
Verbal Comprehension	Similarities	Vocabulary	Information
Perceptual Reasoning	Block Design	Matrix Reasoning	Visual Puzzles
Processing Speed	Symbol Search	Coding	
Working Memory	Digit Span	Arithmetic	

Clearly IQ tests are not the end-all-be-all in a cyber forces selection program. However, they can test for and identify key desired/required intelligence attributes that map to one, some or all of the environmental elements of the cyber domain.

Personality Assessment

Although not quite as old as IQ testing, personality testing has a well-established body of scientific work, practitioners and approaches. However, given cyber's highly technical nature some might question the need for personality testing as a component in cyber forces selection. One key attribute identified in surveying cyberspace was the need to operate competently and comfortably in an ambiguous environment. This is a trait not measured in the intellect, but rather the personality, and there are more like it within the cyber domain that are desired/required in building any truly effective cyberforce. Most personality testing is oriented on the "big 5," a personality test built over fifty years ago designed to measure five key personality traits.

Table-4[26]

The Big 5					
Key Trait	Trait Elements				
Extraversion	Excitability	Sociability	Talkativeness	Assertiveness	Emotional Expressiveness
Agreeableness	Trust	Altruism	Kindness	Affection	
Conscientiousness	High-thoughtfulness	Good Impulse Control	Goal-directed	Organized	Detail-oriented
Neuroticism	High-emotional instability	Anxiety	Moodiness	Irritability	Sadness
Openness	Imagination	Insight	High-broad Range of Interests		

Obviously some of these traits are screen-outs while others are requisite screen-ins. The point is, personality testing allows identification of those other whole-person attributes desired/required within a cyber warrior that IQ testing alone won't account for.

Skill Assessment

As established and proven as intelligence and personality testing are, skill assessment is perhaps the oldest form of testing, and is both a science and art. For centuries warriors, craftsman, and academics applied various methodologies to determine skill levels of members desiring entry or progression through their ranks. Knights jousted and matched wits and strength in competitions; craftsman moved from entry-level apprenticeships to skilled journeyman and master craftsman. The USAF enlisted career system is based on the apprentice-journeyman-master-craftsman model, with career specific assessment tests. Initial entry into the service requires a general skill/aptitude test known as the ASVAB for enlisted members and the AFOQT for officers. Lastly, academic and other professional communities have long used tests to assess skill/aptitude for things like university admittance (e.g., SAT) or licensure (e.g., Bar Exam). Clearly, skill testing for potential cyber warriors is well within reach. The question then becomes what skills and aptitudes are required? At a general intuitive level, skills/aptitudes in

programming, networking, and operating systems/languages are minimum requirements for entry. Pulling from two leading university undergraduate programs in computer science and computer criminology the list refines and expands to include:

Table-5[27, 28]

Computing devices	Computing and information internetworks	Computing and intelligence	Computing and media	Computing and modeling-simulation
Computing and people	Computing and systems and architecture	Computing and theory	Programming (generic, concurrent, Unix & Object Oriented)	Computer organization
Discrete mathematics	Computer ethics	Computer security	Network security	Cryptography
Computer and network system administration	Data structures and algorithms	Operating systems	Database theory and structure	Cybercrime detection and forensics

Given both general and more refined skill sets required of potential cyber warriors are not only identifiable but also testable; the USAF should develop and implement a methodology for testing them as part of a robust scientific and holistic selection program.

The Need

Examination of the cyber environments and subsequent survey of existing intelligence, personality, and skill assessment methodologies provides motivation, potentially desired/required cyber warrior attributes, and examples of scientific approaches that could contribute to the construct of a cyber forces selection program. However, just as NFL personnel directors do not rely solely on the Wonderlic in player selection neither should the military use paper testing alone in selecting cyber warriors. While a step-up, even developing and incorporating scientifically based pre-screening intelligence, personality and skill/aptitude tests into existing traditional accession and training models does not provide the scientific *and* holistic accession

and selection program some, including the author and Dr. Ray Bateman of the Human Research Engineering Directorate at the US Army Research Laboratory in Ft. Sam Houston, believes necessary for tomorrow's cyber warriors.[29] What is truly needed is an entirely integrated approach to selecting candidates that accounts for and assesses the intelligence, personality, and skills required by the cyber domain in a scientific and wholistic manner.

Military Selection and Accession Programs

Turning back to the introductory comparison of the contemporary information age to the Cold War era provides a potential model for such a program. The nuclear navy and the US Army Green Berets were two new forces developed and fielded during this timeframe. At first glance, one might surmise the nuclear navy provides the best model given its hi-tech and *strategic* nature and focus. However, as infamously competitive and rigorous as Admiral Hyman Rickover's accession and selection program was, for all intents and purposes it was an amalgam of some scientific pre-screening tests combined with, albeit extremely arduous, traditional methods.[30] Rather, it is the surprisingly scientifically based and integrative whole-person approach of the Green Beret's accession and selection program that offers the best candidate for emulation.

US Army Special Forces Primer

Unfortunately, the hyperbolic John Wayne and Rambo personages betray what the Army's SF troopers are really about and in doing so masks the incredible capability the nation receives thru their selection program. Additionally, some may point to an ill-perceived mismatch between the seemingly kinetic and violent world of SF troopers and the non-kinetic and "benign" world of cyberspace warriors. However, as subsequent discussion will prove, there

is a surprisingly ready corolary between SF missions, organization, pre-screening, a selection program known as the ”Q course,“ and what could and should be for cyberspace warriors.

Missions

US Army SF have four primary missions: Direct Action (DA), Special Reconnaissance (SR), Unconventional Warfare (UW), and Foreign Internal Defense (FID).[31] DAs are the high-visibility media events like raids and strikes, and high-value leadership capture/kill missions.[32,33] Cyber equivalents are computer network attack (CNA) and computer-network-enabled high-value data exfiltration/destruction. SRs are the see-but-don't-be-seen and hear-but-don't-be-heard missions of covert or clandestine intelligence collection, pre-strike reconnaissance.[34,35] CNE is a comparable activity within the tasked cyber mission set. The UW mission is best typified by a scenario where foreign anti-government fighters (guerillas) are trained and advised by SF troopers as they attempt to defeat the government in power.[36,37] A perfect example of this was SF troops advising the Northern Alliance in Afghanistan as they attempted to defeat the Taliban government. As of yet, this is not a well-defined or mature mission set for cyber warriors. However, given the universally increasing governmental reliance on cyberspace, developing doctrine, forces and TTPs to conduct cyberspace UW would prove an immensely valuable plus-up in military capability/capacity, and provides another arrow in the national security quiver. Lastly, FID, the other side of the UW coin, entails training and advising a government in power to either build additional military capability/capacity or conduct counterinsurgency (COIN) operations.[38,39] As is the case for cyberspace UW, cyberspace FID is an underdeveloped military capability/capacity. However, given that building partnership cyberspace capability/capacity is specifically spelled out within current national cyberspace strategy as part of collective defense, it seems compelling that the services organize, train and

equip for such a mission set. In summary then, the SF mission set is readily translatable into not only existing, but future cyberspace missions.

Organization

The focused yet expansive SF mission set in and of itself deserves consideration as a template for cyberforce operations, but equally impressive and also deserving of consideration, especially in increasingly resource-constrained times, is the substantial capability relatively small SF units provide. The foundational SF organization is the 12-man Operational Detachment Alpha (ODA) team.[40] As any past adversary will attest, although small, these teams pack an uncanny cognitive, stealthy, and lethal wallop. Each consists of an Officer in Charge, Warrant Officer (assistant team leader), two heavy/light weapons specialists, two engineers, two medics, two communicators, and one each intelligence and operations NCOs.[41] These ODAs coalesce into larger regionally trained/focused SF Groups. It is the construct of these ODAs and SF Groups that deserve consideration as emulatable models. It is both unrealistic and potentially capability-draining to build cyber warriors as equally interchangeable carbon copies of each other given the aforementioned complex breadth and depth of the cyber domain's technical and intellectual landscape. Georgia Tech's College of Computing, and other well regarded programs minting computer scientists, recognize this fact and have their students focus on no more than one or two "threads" within the computer sciences in order to "add value" to the field.[42] In light of the domain's complexity and the increasingly required specialization needed to successfully operate within it, application of the ODA construct provides a readily adaptable model for organizing cyberspace forces. Each SF Group's regional focus also bears replication as it mandates and cultivates cultural and regional continuity and expertise. Accordingly, SF troopers are required to gain/maintain language proficiencies for their assigned area. This paradigm also

dictates which Group is primarily responsible for conducting tasked missions in specified areas of the world. Given the global nature of the cyber domain is still affected by regional and cultural languages and issues, a cyberforce organized along such lines would facilitate development of a greater depth of expertise in-turn enabling more effective operations.

US Army Special Forces Selection and Accession Applied to Cyber

The SF model is very compelling for a scientific and holistic cyber forces selection program. It consists of three blocks: Special Operations Preparation Course, Special Forces Assessment and Selection (SFAS), and the Special Forces Qualification Course (Q-Course).[43] As part of the overall selection program candidates take three psychological and aptitude tests: the Wonderlic, the Test for Adult Basic Education which tests candidate's relative grade levels in reading and math, and the Minnesota Multiphasic Personality Inventory which evaluates thoughts, emotions, attitudes, behaviors and even mental disorders.[44] The tests are proctored by psychologists, with specific results understandably sensitive and close-hold. However, they *are* used to assess key make-or-break intelligence and personality attributes.[45] From an intelligence and aptitude standpoint, these tests have consistently and successfully predicted whether a given candidate has a 40, 70 or 95 percent chance of successfully completing the academic component of specialty training.[46] It has also proven very effective in assessing/predicting personality traits and disorders. For example, an active duty soldier attempting entry into the SF selection program, Timothy McVeigh, took these tests, and based on the results was subsequently removed from candidacy in the program.[47,48] Although low-profile and non-kinetic, cyberspace operations *can* have potentially disastrous kinetic effects; therefore, just as the low-profile SF community incorporates scientific tests within its selection program so too should any cyberforce equivalent.

Special Operations Preparation Course (SOPC)

The SOPC provides 30-days of training to prepare both off-the-street and within-service candidates for the SFAS block known as phase-I. It is designed to elevate both physical fitness and land navigation skills, the hallmarks of an SF trooper. The caveat for this block and all others is that successful completion does not guarantee passage of the subsequent block. At the end of each block or phase candidates are either invited to continue in the selection program, or return to their home unit and work on skills and re-attempt selection at another time, and in the worst case scenario candidates are told respectfully, but honestly, they are not particularly well suited to the SF profession and should pursue other soldiering options. These selection program continuance/dismissal decisions are made by review board evaluation using the whole-person approach including records reviews and both cadre observations and peer reviews of a candidate's performance, as well as the aforementioned battery of IQ and personality tests.[49] The applicability of the SOPC framework to cyber is twofold. First, the Army recognizes there are ready, willing and suitably skilled candidates to pull from both off-the-street and from within the service, and has an established program to baseline both pools physically and skill set-wise. Given the demand for cyber-skilled individuals across commercial, civil, and military spectrums, any cyberforce selection program must adopt a similar approach in order to recruit sufficient numbers of candidates. Second, the program recognizes some key skills are at nuanced different levels among the candidates, or may have atrophied; so the SOPC compensates for that potentiality. Cyber skills are no different so to establish a relatively level playing field for candidates, a cyberforce selection program should accomplish similar ends as the SOPC does for SF candidates.

Special Forces Assessment and Selection

Following successful completion of SOPC, candidates progress to SFAS for 24 days of immensely challenging training designed to assess their survivability/resiliency, intelligence, agility and resourcefulness. The cornerstone element of the block is quite possibly the mother-of-all combined intellectual, physical, and emotional problem sets known as the "Star course;" an 18-kilometer land navigation test with tough terrain and multiple obstacles. Candidates are not allowed to use roads or flashlights, and must navigate through the night with a 30-lb rucksack, regardless of the weather. They have three opportunities to successfully complete the course. Even with the baselining and freshening-up of physical fitness and critical navigation skills in SOPC, an estimated 50 percent of candidates still wash-out of this block.[50] Candidates are told by the cadre that as their "evaluators, and…future teammates" they are being assessed for "a balance of the physical, mental and emotional."[51] Regarding fitting parallels to cyberforce selection, obviously land navigation with a 30-lb ruck in the dark, rain or shine, and in challenging terrain are not needed intelligence and personality attributes, and skills. But, the parallels with cyber exist. Specifically, cyberspace terrain is comprised of networks-of-networks requiring intelligence, skill and sometimes even endurance to successfully navigate. Depending on the mission, the rules of engagement may require avoidance of main cyber thoroughfares (i.e., roads), and may require actions to mitigate any chance of tracking or attribution of the mission (i.e., flashlights and noise). Given this scenario, a cyber warrior will invariably get intellectually, emotionally and potentially physically tired, and if they are not especially thorough and disciplined they could quite possibly fail to make one or more objectives. Incorporation of a "Cyber Star" course on a cyber range within a cyber forces selection program provides an excellent vehicle for cadre evaluation and assessment for a balance of intellectual, emotional and

physical attributes. So clearly, albeit a wholly physical domain and terrain, the SFAS and its Star course are fitting block-II model elements for a cyber forces selection program.

Special Forces Qualification Course

The Q-course is the next SF selection program block; consisting of five phases (II thru VI) encompassing small unit tactics, specialty training, capstone course, language training, and Survival Escape Resistance and Evasion training. Phase-II is oriented on training and assessing candidate skills in the basic SF trade craft of small unit tactics such as individual and patrol movement, patrol movement formations, recce, ambush and raid patrols, mission planning, and troop leadership. Granted phase-II is decidedly kinetic, but its focus on foundational tradecraft is mirrorable within the cyber domain. Cyber warriors must posess some common and basic tradecraft skills in order to successfully patrol their domain individually or as a team, or mission plan for and conduct cyber recce, ambush or raid sorties, and lead themselves or others while doing it. So a cyber selection phase equivalent is emulatable and desireable. In phase-III SF candidates are broken out into their intended specialties and undergo extensive training. While the specialties are not exact matches within cyber forces, the approach is nonetheless viable for cyber warrior selection. The candidates rejoin for the phase-IV "Robin Sage" capstone exercise.[52] Here candidates are organized into ODA teams and placed on a simulated range environment where they are given a scenario and orders, and are assessed in their performance of all standard SF mission sets. They must demonstrate their ability to put everything they've learned to use. Failure to do so results in dismissal from the selection program. Successful completion leads to selection and follow-on assignment to an ODA team and SF Group. The capstone exercise is an ideal method for conducting one final, holistic assessment of the candidate's potential performance as an operator, as key intelligence and personality attributes,

and skills are observed and evaluated within an environment as proximate to real operating conditions as possible. It is for this very reason any future cyberforce selection program must include an equivalently realistic capstone exercise if it is to truly craft cyber warriors second to none.

Conclusion

The onset of the present information age, and the national security threats and opportunities posed by the wild-wild west of the cyber domain are no less daunting than those ushered in with the birth of the Cold War. Whereas the Cold War yielded a unifying strategy in NSC 68 and groundbreaking forces in the nuclear navy and the US Army Green Berets, to date the underwhelming US response to the pressing cyberspace challenge has consisted of the publishing of inadequate national, DoD and Service strategies, and the Air Force's adoption of cyberspace as one of its three core missions. Unfortunately, the service's utilization of traditional military accession and training methodologies for its cyber forces neither scientifically nor holistically assess the intelligence, personality, and skills a competent cyber operator requires to execute the technical depth or operational breadth needed to prosecute cyberspace superiority operations. Therefore, given the strategic criticality of the cyber domain to national security and Joint Operations it is a national imperative that the USAF develop and implement a robust selection program for cyber warriors that scientifically and holistically assesses intelligence, personality and skill; crafting a cyberforce second to none. The US Army Special Forces selection and assessment program provides a fitting model for crafting a cyber forces equivalent. In spite of the illperceived mismatch between the seemingly kinetic and violent world of SF troopers with the non-kinetic and surface benignity of cyberspace, the comparative analysis demonstrates a surprising corolary between the two; making the SF model

a well-suited candidate for developing a scientific and holistic cyberforce selection program that assesses intelligence, personality and skill; fielding a cyberforce second to none.

Endnotes

1. Bateman, Raymond, interview by Lt Col George Tromba. *Dr.* (9 6, 2012).
2. US Air Force. *Air Force Doctrine Document 3-12: Cyberspace Operations.* Maxwell AFB AL: LeMay Center, 2011, p. 1-2.
3. Reed, John. "Napolitano: US and allies must improve info sharing on cyber threats." *Killer Apps Foreign Policy*, October 25, 2012: p. 15-17.
4. Ibid, p. 15-17.
5. Qiao Liang, Wang Xiangsui. *Unrestricted Warfare.* Beijing: PLA Literature and Arts Publishing House, 1999.
6. Ibid, p. 47.
7. Ibid, p. 119.
8. Spiegel Staff. "Merkel's China Visit Marred by Hacking Allegations." *Spiegel International*, August 27, 2007.
9. Harris, Shane. "China's Cyber-Militia." *National Journal*, January 31, 2011.
10. Carr, Jeffrey. *Inside Cyber Warfare.* Sebastopol: O'Reilly, 2012, pg. 19.
11. Dr. Frederick Wamala (Ph.D.), CISSP. *ITU National Cybersecurity Strategy Guide.* Geneva: ITU , 2012.
12. Times, The New York. *Foreign Intelligence Surveillance Act (FISA).* New York, September 13, 2012.
13. *International Strategy for Cyberspace; Prosperity, Security, and Openness in a Networked World.* Washington, D.C.: The White House, 2011.
14. Ibid, p. 12-13.
15. Ibid, p. 12-14.
16. *Department of Defense Strategy for Operating in Cyberspace.* Washington, D.C.: Department of Defense, 2011, p. 4.
17. Ibid, p. 1.
18. Scientist, United States Air Force Chief. *Cyber Vision 2025.* Washington, D.C.: USAF/PA, 2012, p. 2.
19. Ibid, p. 2.
20. Bousquet, Antoine. *The Scientific Way of Warfare.* New York: Columbia University Press, 2009, p. 17.
21. Ibid, p. 17.
22. Ibid, p. 18.
23. Ibid, p. 34.
24. Cherry, Kendra. "History of Intelligence Testing." *About.com.* 2012. http://psychology.about.com/od/psychologicaltesting/a/int-history.htm (accessed 12 01, 2012).
25. Pearson Education. *Introducing the WAIS–IV.* Pearson Education, 2008, p. 12.
26. 123 Test. *The Big Five Personality Theory.* 123 Test, 2012.
27. Technology, Georgia Institute of. "Bachelor of Science in Computer Science Threads." *College of Computing Course Catalog.* Atlanta: Georgia Institute of Technology, 2012.
28. University, Florida State. "Computer Criminology Degree Program." *Florida State University College of Criminal Justice Course Catalog.* Tallahassee: Florida State University, 2012.
29. Bateman, Raymond, interview by Lt Col George Tromba. *Ph.D., US Army Research Laboratory; Human Research Engineering Directorate* (9 6, 2012).

30. Beaver, William. "Tenacious Visionary, Admiral Rickover: Lessons for Business Leaders." *Business Forum*, Vol 23: Nos. 3, 4.
31. Couch, Dick. *Chosen Soldier: The Making of a Special Forces Warrior.* New York: Crown Publishing Group, 2007, p. 24-42.
32. Ibid, p. 24.
33. Bateman, Raymond, interview by Lt Col George Tromba. *Ph.D., US Army Research Laboratory; Human Research Engineering Directorate* (9 6, 2012).
34. Ibid.
35. Couch, Dick. *Chosen Soldier: The Making of a Special Forces Warrior.* New York: Crown Publishing Group, 2007, p. 25.
36. Ibid, p. 25-26.
37. Bateman, Raymond, interview by Lt Col George Tromba. *Ph.D., US Army Research Laboratory; Human Research Engineering Directorate* (9 6, 2012).
38. Ibid.
39. Couch, Dick. *Chosen Soldier: The Making of a Special Forces Warrior.* New York: Crown Publishing Group, 2007, p. 26.
40. Ibid, p. 18.
41. Ibid, p. 49-51.
42. Georgia Institute of Technology. "Bachelor of Science in Computer Science Threads." *College of Computing Course Catalog.* Atlanta: Georgia Institute of Technology, 2012.
43. Bateman, Raymond, interview by Lt Col George Tromba. *Ph.D., US Army Research Laboratory; Human Research Engineering Directorate* (9 6, 2012).
44. Couch, Dick. *Chosen Soldier: The Making of a Special Forces Warrior.* New York: Crown Publishing Group, 2007, p. 140-141.
45. Ibid, p. 142.
46. Ibid, p. 143.
47. Ibid, p. 143.
48. Bateman, Raymond, interview by Lt Col George Tromba. *Ph.D., US Army Research Laboratory; Human Research Engineering Directorate* (9 6, 2012).
49. Couch, Dick. *Chosen Soldier: The Making of a Special Forces Warrior.* New York: Crown Publishing Group, 2007, p. 118.
50. Ibid, p. 131.
51. Ibid, p 266-267.
52. Ibid, p. 313.

Bibliography

123 Test. *The Big Five Personality Theory.* 123 Test, 2012.

Adams, Chris. *Inside the Cold War: A Cold Warrior's Reflections.* Maxwell AFB, AL: Air University Press, 1999.

Air Force Doctrine Document 3-14: Space Operations. Maxwell AFB AL: LeMay Center, 2012.

Alexander, GEN Keith B. "Building a New Command in Cyberspace." *Strategic Studies Quarterly 5, no.2*, Summer 2011: 3-12.

Associated Press. "Why It Matters: Cyber Security." *AP Wire*, October 10, 2012: 1.

Bateman, Raymond, interview by Lt Col George Tromba. *Ph.D., US Army Research Laboratory; Human Research Engineering Directorate* (9 6, 2012).

Beaver, William. "Tenacious Visionary, Admiral Rickover: Lessons for Business Leaders." *Business Forum*, Vol 23: Nos. 3, 4.

Benson, Etienne. "Intelligent intelligence testing." *APA Monitor*, February 2003: 48.

Bousquet, Antoine. *The Scientific Way of Warfare.* New York: Columbia University Press, 2009.

Bush, George W. *The National Strategy to Secure Cyberspace.* Washington, D.C.: The White House, 2003.

Carr, Jeffrey. *Inside Cyber Warfare.* Sebastopol: O'Reilly, 2012.

Cherry, Kendra. "History of Intelligence Testing." *About.com.* 2012. http://psychology.about.com/od/psychologicaltesting/a/int-history.htm (accessed 12 01, 2012).

Couch, Dick. *Chosen Soldier: The Making of a Special Forces Warrior.* New York: Crown Publishing Group, 2007.

Cyberspace Operations: AFDD 3-12. Maxwell Air Force Base: Curtis E. LeMay Center for Doctrine Development and Education, 2011.

David J. Kay, Terry J. Pudas, and Brett Young. *Preparing the Pipeline: The U.S. Cyber Workforce for the Future.* Institute for National Strategic Studies: National Defense University Press, 2012.

Defense, US Department of. *Cyber Operation Personnel Report.* Washington D.C.: US Department of Defense, 2011.

Dempsey, General Martin E. *Mission Command White Paper.* Pentagon, Washington D.C.: CJCS, 2012.

Department of Defense Strategy for Operating in Cyberspace. Washington, D.C.: Department of Defense, 2011.

DeYoung, Colin G. *Intelligence and Personality.* MN: University of Minnesota, 2011.

Dr. Frederick Wamala (Ph.D.), CISSP. *ITU National Cybersecurity Strategy Guide.* Geneva: ITU , 2012.

Evans, Colonel Gerald D. "Hyman Rickover: Excellence, Greatness, Heroism." *Military Review*, January-February 2005: 85-87.

Fish, Christi. "College students gather for cyber defense competition nationals April 8-10." *UTSA*, April 7, 2011.

Fitzgerald, Sandy. "Air Force Steps Up Cyber Warfare Defenses." *Mobile Media*, July 12, 2012: 1-3.

Force, US Air. *Air Force Doctrine Document 3-12: Cyberspace Operations.* Maxwell AFB AL: LeMay Center, 2011.

Griggs, Susan. "New Officer Course Boosts Cyberspace Transformation." *Air Force Print News*, June 15, 2010: 1-2.

Harris, Shane. "China's Cyber-Militia." *National Journal*, January 31, 2011.

International Strategy for Cyberspace; Prosperity, Security, and Openness in a Networked World. Washington, D.C.: The White House, 2011.

Kastenberg, Stephen W. Korns and Joshua E. "Georgia's Cyber Left Hook." *Parameters*, Winter 2008-09: 60-73.

Lynn M. Scott, Raymond E. Conley, Richard Mesic. *Human Capital Management for the USAF Cyber Force.* Stanta Monica CA: Rand Corporation, 2010.

Major General Werner Widder, German Army. "Auftragstaktik and Innere Furung: Trademarks of German Leadership." *Military Review*, September - October 2002: 3-9.

Osinga, Frans P.B. *Science, Strategy and War: The Strategic Theory of John Boyd.* New York: Routledge, 2007.

Pearson Education. *Introducing the WAIS–IV.* Pearson Education, 2008.

Pomper, Stephen D. "A Smarter Force for Less Time and Money." *Joint Force Quarterly*, 2011: 53-55.

Qiao Liang, Wang Xiangsui. *Unrestricted Warfare.* Beijing: PLA Literature and Arts Publishing House, 1999.

Reed, John. "Napolitano: US and allies must improve info sharing on cyber threats." *Killer Apps Foreign Policy*, October 25, 2012: 15-17.

Robert A. Miller, Daniel T. Kuhl, and Irving Lachow. "Cyber War: Issues in Attack and Defense." *Joint Forces Quarterly*, 2011: 18-23.

Roger J. Spiller. *Combined Arms Since 1939.* Fort Leavenworth KS: US Army Command and General Staff College Press, 1992.

Scientist, United States Air Force Chief. *Cyber Vision 2025.* Washington, D.C.: USAF/PA, 2012.

"Sheriffs of Cyberspace: Enlisted course next step in cyber transformation." *Air Force Print News Today*, 1 19, 2011: 1.

Singer, P.W. "The Future of National Security, By the Numbers." *Joint Force Quarterly*, 2011: 64-71.

Spiegel Staff. "Merkel's China Visit Marred by Hacking Allegations." *Spiegel International*, August 27, 2007.

Technology, Georgia Institute of. "Bachelor of Science in Computer Science Threads." *College of Computing Course Catalog.* Atlanta: Georgia Institute of Technology, 2012.

The Saturday Evening Post. "The Patriots for Whom the Polaris Submarines Were Named." May/June 1973: 30-34.

Times, The New York. *Foreign Intelligence Surveillance Act (FISA).* New York, September 13, 2012.

Trollman, Capt David. "Drop Night Sets Path to Future for Cyber Officers." *Air Force Print News Today*, 10 13, 2010: 1.

University, Florida State. "Computer Criminology Degree Program." *Florida State University College of Criminal Justice Course Catalog.* Tallahassee: Florida State University, 2012.

Westermeyer, Lt Col Roger H. *Recruiting and Retaining Cyberwarriors.* Carlisle Barracks, PA: United States Army War College, 2008.

Williams, Brett T. "Ten Propositions Regarding Cyberspace Operations." *Joint Forces Quarterly*, 2011: 11-17.