

AIR WAR COLLEGE

AIR UNIVERSITY

TOP CYBER:
DEVELOPING THE TOP ONE PERCENT TO DEFEAT
THE ADVANCED PERSISTENT THREAT

By

Lance C. DeViney, GS-15, DOD

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. George J. Stein

13 February 2014

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, the Department of Defense, or the Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Mr. Lance C. DeViney, GS-15, is a senior technical leader in the Department of Defense, attending the Air War College, Air University, Maxwell AFB, AL. Mr. DeViney is a career intelligence officer specializing in advanced intelligence, surveillance, reconnaissance, signal exploitation, and cyber security. He earned a Bachelor's degree in Computer Studies from the University of Maryland University College, a Master of Arts degree in National Security Studies with an emphasis on Terrorism from American Military University, and a Master of Professional Studies degree from the Pennsylvania State University in Homeland Security with a focus on Information Security & Forensics. Mr. DeViney also holds graduate-level certificates in Telecommunications Technology from George Washington University and Information Systems Security from the Pennsylvania State University. His diverse career spans assignments as a Naval Cryptologist, a defense industrial sector systems engineer, and as a professional signals analyst with the Department of Defense. Mr. DeViney works as a Senior Cyber Security Manager in the NSA/CSS Threat Operations Center at Fort Gordon, GA.

Abstract

The phenomenal growth of the Internet and the accompanying explosion in online services presents the world with a unique predicament, where the medium that affords citizens a means for peaceful communications also offers malefactors an inroad for theft and destruction. The past five years mark a significant rise in the frequency and severity of online nefarious action from a wide range of actors, and presents a great risk to the security of the United States. U.S Cyber Command is assigned the task of developing and coordinating the online cyber mission of the Department of Defense, and since 2010 is moving aggressively to develop a workforce capable of fighting and winning in cyberspace. Although Cyber Command is making great strides toward this goal, there remains strong risk that nefarious actors presenting an advanced persistent threat will outclass the U.S. military workforce in the most intricate maneuvers of cyberspace. Further, the status quo military staffing, training, and assignment models preclude its personnel from reaching the KSA required for top tier cyber war fighting.

This paper looks at the advanced persistent threat, cites the exemplar of the People's Republic of China as the most obvious adversary, identifies basic shortcomings with the status quo approach, and recommends non-traditional approaches to create a JSOC-like Special Forces class of advanced analyst, drawn from the top one percent of cyber operators. It includes recommendations for re-focusing the bulk of the cyber workforce onto passive defensive duties, while reserving the active attack and the most difficult analytic work for an elite Cyber Corps.

Introduction

“Militaries often take time to adapt. Think world war one and generals using Waterloo tactics.”

John Arquilla, 2012

The U.S. military must be prepared to fight, dominate, and win the next generation battles it will wage by, in, and through, the domain of cyberspace. Thus, it is imperative that its mission focus is on the threat sectors, complexity levels, and work roles that are both *reasonably* and *realistically* achievable within the constraints of the work force. Understanding the knowledge, skills, abilities (KSA) and tradecraft of its adversaries, and the strengths and weaknesses of its own forces, is key to recruiting, training, and fielding a work force suited for the challenges at hand. This paper looks at discrete issues affecting the U.S. military mission in operational cyber warfare, specifically considering the most capable adversary class, herein described as the advanced persistent threat (APT). It considers the capabilities of the U.S. military forces aligned against them, identifies any capability disparity that exists between them, and recommends specific courses of action that may close the gap or alter the paradigm.

This paper argues that the KSA of the most capable state-sponsored APT cyber actors threatening America significantly outclass the U.S. military workforce postured to fight against them. Further, it suggests current cyber force modernization plans will yield forces ready to combat the bulk of the threats, but will fall short in creating *master*-level experts able to defeat the APT. Overcoming this disparity requires a non-traditional approach to career advancement and development of the top one percent (TOP) of U.S. military cyber professionals into true “world class” operators.

Discussing Cyberspace

For the average global citizen, cyberspace and the Internet are nebulous terms for which they have little understanding or concern. Users simply expect to get what they want, when they want it, and how they want it; further, they expect 100% availability of all data types, in great volumes, at high speed, with absolute security. To provide such service, global IT providers juggle myriad challenges crossing the physical, logical, and virtual boundaries, to contend with the paradigm of *volume*, *variety*, *velocity*, and *veracity*, or V4. IT provider International Business Machines (IBM) depicts this domain in a quad chart called *The Big Data & Analytics Hub*,¹ which captures the essence of the problem: *volume* (scale of data) is near incomprehensible; *velocity* (speed of data) must be blindingly fast; *variety* (forms of data) is infinitely diverse; and *veracity* (integrity of data) is essential.

Almost every sector of contemporary society relies to some extent on the collective services of the Internet and its assured availability. The V4 paradigm represents different things to different people: for providers, it is a complex technical challenge; for businesses, it is an incredible income opportunity; for consumers it is a means for getting services; for security officers, it is a source of great risk; and, for hackers, it is the super-highway to a target-rich environment. For the U.S. Government (USG), cyberspace is an important means by which the nation simultaneously conducts business, shares information, provides services, builds wealth, and projects soft power. The Internet is also a medium through which adversaries can *virtually* invade the nation to *actually* steal valuable intellectual property, uncover sensitive proprietary information, deface public web sites, disrupt commercial services, and wreak havoc among USG, commercial and private services. As the nation expands interconnected services, reliance on the Internet rises accordingly, as does risk and danger of compromise. Although the majority uses it

for good, a minority uses it for bad, and defending the former against the latter is important to maintaining good social order worldwide. Ultimately, for all its benefits, the Internet presents an “Achilles’ Heel” in the defense of the nation’s Critical Infrastructure and Key Resources (CIKR).

Characterizing the Cyber Threat

Every second of each day, legions of hackers great and small, foreign and domestic, independent and state-sponsored, probe the Internet’s diverse networks, systems, websites, databases, and accounts. From spear-phishing emails and key loggers to IP spoofing and SQL injection, hackers seek inroads, hoping that system weaknesses and poor user discipline will give way to their malicious software. Writing in *Business Insider*, Stuart Coulson - Director of Hosting at UKFast, describes seven basic computer hacker levels.²

1. Script Kiddies: bored kids looking for a thrill, laying down scripts written by others and manipulating simple operating system weaknesses
2. Hacking Group: loose affiliation of script kiddies collaborating to attack companies and media operations which they tend to dislike
3. Hacktivist: like-minded hackers motivated by political, social, or religious drive, wreaking havoc on targeted governments, agencies, and corporations
4. Black Hat Professionals: experts in network security, software coding, and decryption, throwing their talent at cracking systems advertised as secure
5. Organized Criminal Gangs: online theft, extortion, and globalized command and control of illegal acts, infusing organized crime with new-found wealth
6. Nation States: the top of the heap from the perspective of technical capability, operational prowess, access and funding, and potential risk level

7. The Automated Tool: customized software tool operating independently, often self-reproducing and self-propagating once launched

Broad ranges of perpetrators exist, visualized as a hierarchical pyramid with the highest percentage of lowest skilled forming the base, and the lowest percentage of highest skilled forming the peak. All seven hacking categories represent some threat level to the nation:

- Low = Levels 1-3 (Script Kiddie, Hacking Group, Hacktivist)
- Medium = Levels 4-5 (Black Hat Professionals, Organized Criminal Gangs)
- High = Levels 6-7 (Nation States, Automated Tool)

Major Global Actors

Network security writing is prolific, with new reports regularly detailing significant incidents or modified tactics. Authoritative network security and intrusion detection companies such as Mandiant, RSA, Trend Micro, Project 2049, and Symantec, figure among the most vocal and authoritative sources and their reports help us understand the threats and risks posed by the most advanced cyber actors. The collective body of knowledge identifies the People's Republic of China (PRC) and the Russian Federation at the pinnacle of the state-sponsored threat pyramid, with China blamed for over 95% of the world's cyber spying campaigns, followed by Romania, Russia, and Bulgaria.³ Although other nations also possess advanced capabilities, engagement levels are more benign in terms of expert personnel, aggressive action, and their posture toward the U.S. In Russia, the most active players appear to be sophisticated, prolific, shadowy, and criminal, more financially motivated than ideological or nationalistic.⁴ Public insight to the Russian nation-state is rather sparse; still its cyberspace engagement during its August 2008 rout of Georgian military forces in South Ossetia shows it ready and able to bring cyber skills to bear with strong effect.⁵ Other reports attribute the hacking of U.S. and South Korean sites to the

DPRK, with other analyses pointing to Iran and Syria as emerging actors. Reports cite Iran as the most likely instigator of destructive attacks against Saudi-ARAMCO systems in which the *Shamoon* virus destroyed information stored on tens of thousands of disk drives,⁶ and point to its likely responsibility for distributed denial of service (DDoS) attacks levied on US Banking systems in 2012, as part of *Operation Ababil*.⁷

Advanced Persistent Threats

Although all threat levels present some risk to the U.S., this paper focuses on APT actors representing the most active, prolific, advanced, and serious threats to the nation. Ostensibly, an APT is a nation-state actor, underpinned by the finances and resources of a sovereign country, usually aided by diverse subject matter expert (SME) talent drawn from the best minds of industry, academia, and military, in some cases augmented by high-order Black Hat experts on a “for hire” basis. APTs are able to apply large-scale resources against complex problems, reserving the toughest tasks for their most masterful hackers.

Among open public sources, the most direct correlation with a high-order APT goes to the PRC, where online theft of U.S. and Western intellectual property and military technology is massive and continuing. As USG officials denounce the PRC for its aggressive cyber incursions into U.S. networks, companies such as Mandiant are increasingly vocal and detailed about their own cyber sleuthing of nefarious online activity. Mandiant’s groundbreaking M-Trend 2010® report first highlighted this threat and suggested the PRC as the most likely source.⁸ Mandiant followed up in 2013 by specifically naming the PRC General Staff Department (GSD) People’s Liberation Army (PLA) Unit 61398 as the source of APT-1 (one of many APT worldwide), whose operational focus targets U.S. military, technology, industry, and finance sectors.⁹ Other reporting from industry leaders such as Trend Micro, Symantec, RSA, and Project 2049, provide

even more insight into the PRC's vast computer network operations (CNO) enterprise, comprising entities from the PRC's most technologically advanced centers of academia, industry, government, military, and "for hire" private Black Hats. It is clear that the PRC has assembled an epic team, tapping into its impressive collective national intellect.

The following reported findings highlight this diverse and capable force, and provide insight to the complex, deep, and high-end nature of the PRC CNO enterprise.

- Mandiant's editor reports that APT-1 has downloaded "hundreds of terabytes of data from at least 141 organizations" and shown its ability to conduct simultaneous, deep penetration on many targets.¹⁰
- Mandiant's APT-1 report further estimates that "Unit 61398 is staffed by hundreds, and perhaps thousands of people," and that it "requires its personnel to be trained in computer security and computer network operations and also requires its personnel to be proficient in the English language."¹¹
- Symantec's Stephen Doherty reports that a PRC APT called "Hidden Lynx" operated since 2009 and is likely aided by PRC "for hire" Black Hats. The group "is an advanced persistent threat that has been in operation for at least four years and is breaking into some of the best-protected organizations in the world."¹²
- Trend Micro's Forward-Looking Threat Research Team details methodology of an APT campaign targeting India and Japan, masked by use of virtual private servers, which it later attributes to hackers in the Chinese underground.¹³
- Project 2049's Mark Stokes describes the PRC GSD's Beijing North Computing Center as "most capable of cyber reconnaissance architecture design, technology development, systems engineering, and acquisition." Further, "At least 10

subordinate divisions appear responsible for design and development of computer network defense, attack, and exploitation systems.”¹⁴

Civilian and Military Cyber Initiatives

U.S. Army GEN Keith Alexander holds the reins as Commander, USCYBERCOM (USCC), and Director, National Security Agency/Central Security Service (NSA/CSS), a dual-hat role giving him control of a vast network of powerful intelligence systems and skilled professionals comprising federal employees, military service members, and contract civilians.¹⁵ At a 3 June 2010 Cyberspace Policy Debate sponsored by the Center for Strategic and International Studies, GEN Alexander described the USCC’s role:

We at Cyber Command are responsible day to day for directing the operations and defense of the Department of Defense information networks and for the systemic and adaptive planning, integration and synchronization of cyber-activities, and when directed under the authority of the president, the secretary of defense and the commander of U.S. STRATCOM, for conducting full-spectrum military cyberspace operation to ensure U.S. and allied freedom of action in cyberspace.¹⁶

In the three years since, thousands of enlisted and officer personnel joined the ranks of the USCC and SCEs as newly minted “cyber warriors.” Simultaneously, the USG undertook a rapid hiring and training program underpinned by President Obama’s May 2009 plan *The Comprehensive National Cybersecurity Initiative*,¹⁷ a fundament of which is *The National Initiative for Cybersecurity Education (NICE) Strategic Plan*¹⁸ championed by the National Institute of Standards and Technology (NIST). Coincidentally, the rising specter of network attack, hacking, and malicious behavior, has motivated commercial corporations to pursue university

students graduating with degrees in computer science, information technology (IT), and cyber security. Government, military, and commercial employers are therefore all vying for the same critical skills among a very shallow talent pool.¹⁹

Even in federal circles, where the desired number of cybersecurity professionals skyrocketed to 4,900 civilians, agencies are falling short in their ability to attract such personnel, as many perceive the monetary and work-life benefits as substantively better in the commercial sector.²⁰ Further stymieing the ability to attract top talent is the perception of restrictive work conditions, demand for security clearances, lethargic hiring processes, marginal empowerment, and in recent months growing public distrust of government. As the U.S. military has ramped up its own cyber programs, foundational curricula such as the Joint Cyber Analysis Course (JCAC) have arisen as common building blocks, augmented by follow-on training in more advanced studies. Across the board, each service is aggressively building its personnel, systems, tools, and developing tactics, techniques, procedures, policies, rules of engagement, doctrine, and operational authorities.²¹

Identifying the Problem

As several thousand military personnel join the cyber force, a vexing question arises: “What advanced cyber fighting tasks will these troops *actually* be able to perform?” If expected duties comprise network maintenance, account management, operating system patching, antivirus updating, and intrusion detection monitoring, then they are simply describing traditional IT support roles. Conversely, if expected duties include extremely complex network operations using cutting-edge tradecraft against the most concerted APTs, then the question becomes: “What *should* they be doing, and what can they *realistically* accomplish, given the adversary’s very high KSA and the constraints commonly imposed by military recruiting,

training, retention, and assignment practices?” Is the traditional military manning model suited to the unique demands at hand? Many think that it is not, and fear that inexperienced cyber troops will undertake missions they are not realistically capable of performing at the advanced expertise levels demanded. This concern is increasingly relevant in light of the move to reduce contractors as part of deep cuts in defense spending, and a renewed call for limiting intelligence duties to USG and military personnel only, in the wake of the Edward Snowden affair. Yet there is sound reasoning for hiring contractors and civilians, as they routinely have the most extensive education, advanced formal training, diverse industry certification, demonstrated skill and tradecraft mastery, and long-term continuity on the job.²²

Importantly, what contractor and civilian operators have in common is that their operational roles are often their *sole* responsibility, even as they rise through higher pay grades and responsibility levels. They have the ability to focus uncontested, for years on end, on deepening and maturing their KSA, and gaining the mastery level that only comes through sustained development over extended time. The military staffing and assignment model in contrast, limits the period allotted for pure technical focus to a few years, after which organizational leadership and management (OL&M) roles are certain to have priority for building “the leaders of tomorrow.” The singular path of OL&M development sets the course for all personnel to (theoretically) rise to the most senior enlisted or officer ranks (even though most will not), as opposed to defining separate managerial and technical tracks for professional development and career advancement. In practice then, there is a narrow time window of opportunity to harvest competent technical performance prior to OL&M duties taking preeminence. In many cases, the sweet spot is the enlisted grades E4-E5, where troops have completed basic- through intermediate-training, gained work experience, learned tradecraft

skills, remain highly motivated, and are unencumbered by high volumes of OL&M tasks and collateral duties. Although most services consider an E6 to be a senior technical expert, in reality many non-commissioned officers, spend only about half their time working in their technical role, and the other half expanding their leadership competencies. Unfortunately, it is at this precise point where analysts with true world class potential are finally coming into their own and exhibiting the depth and breadth of KSA to defeat the APT.

The U.S. military's foundational, generations-long force development doctrine is successful in training leaders for tomorrow. However, it is questionable whether this approach will suffice in raising up legions of highly skilled cyber masters – experts whose training and KSA maturation requires sustained full-time focus over a many years long growth cycle. Given the extreme KSA of the most advanced cyber adversaries (the enemy's 10%), what counter force is the U.S. military *realistically* able to mount? A critical mind must ask, “Is it *probable*, or even *possible*, that a 20-year-old JCAC graduate is going to battle it out head-to-head and win against so capable an adversary?” A reality check suggests such a vision is not realistic, and the current approach will put its finest yet unequally prepared talent, up against the most hardened cyber force the adversary has to offer. If there is danger this will be the case, then the U.S. military must correct course and adopt a new modus operandi. If it is unwilling to change, APT actors will outclass U.S. military forces, and reliance on contractor and civilian expertise will remain.

How Should We Proceed?

In the commercial world, the majority of computer security professionals are in the business of *providing* services and *defending* them: ensuring network integrity, operating intrusion detection systems, installing vulnerability patches, and keeping core services at a high state of availability. A much smaller subset performs network oversight, reconnaissance,

sleuthing, and penetration testing and hunting for hidden intruders in their networks. An even tinier percentage, comprising the highest educated, trained and proficient SMEs have the prowess and accompanying authority to conduct advanced, and arguably dangerous actions, such as hacking back into an intruder's host machine to disable their system through active defensive means. This industry model should also apply to the U.S. military, whereby the bulk of the cyber workforce conducts *passive defensive* actions at the basic, intermediate, and advanced levels, and a small body of true SMEs conducts *active offensive* actions against the most advanced APT. As Brett T. Williams writes in his article "Ten Propositions Regarding Cyberspace Operations":

Cyber discussions in DOD tend to narrowly focus on computer network attack and computer network exploitation. Not enough attention is given to providing, operating, and defending the networks that define cyberspace. Attack and exploitation get the most attention because they employ some of the most sensitive capabilities and require significant legal and operational considerations. However, it is the ability to provide, operate, and defend cyberspace that should be the JFC's top priority because these activities enable all other cyberspace operations.²³

At USCC, the SCEs, and the USG, programs are on track to field forces to combat the bulk of the global threat (the 90% problem), yet it is the top 10% of APT actors that constitute the *most insidious* danger. If the emerging workforce cannot contend with the most pervasive APT threat, this plan will fail unless something significant is changed. To mitigate this weakness, the U.S. military should consider a re-alignment of forces, and adopt a non-traditional approach that breaks the norms of tradition. If the U.S. military wants its troops to go head-to-

head against the APT, then it must selectively recruit, train, equip, develop, and advance cyber personnel in a manner that creates and retains true *master*-level SMEs.

TOP Cyber Corps

One interesting alternative to consider is the operational model of the Joint Special Operations Command (JSOC), an organization comprising the elite of the elite of unconventional warfare operators. To begin, each service draws raw talent through recruiting and the aid of standardized testing such as the Armed Services Vocational Aptitude Battery (ASVAB). Basic training graduates go on to basic and intermediate schools for their occupational specialty, and then based on performance and conduct, services tap top graduates for advanced training in highly specialized career fields. True standouts in their operational units may volunteer to screen for acceptance into the most rigorous and highly selective programs in their services respective Special Operations Forces (SOF). From these, by-name selection takes place to staff the most elite SOF communities, such as Navy SEALs DevGru and Army DELTA Force. Selected members of these elite SOF units then chop over to operate in JSOC. In practice then, the bulk of the armed forces handle most of the conventional war fighting, individual SOF units handle most of the unconventional operations, and JSOC takes on the most advanced, dangerous, and complex operations, most often focused on counter-terrorism missions. A key factor in the success of JSOC and other SOF units is that personnel focus exclusively on their assigned roles, advancing their KSA, and tackling the most complex challenges on a long-term, sustained, high-intensity basis. Services excuse personnel from traditional OL&M functions and collateral duties so they can focus on their operational roles. Successfully combating the cyber threat of the future will require a similar “mission-first” focus, selectively tasking personnel to combat the most pervasive APT.²⁴

Non-traditional Recruiting

Across the global stage, some of the most capable hackers are well educated and professionally trained, yet others are unschooled in the traditional sense, mastering their trade in the comfort of their bedrooms and the shadowy world of the dark Internet. These homegrown hackers long ago outgrew their peer script kiddies, hackers, activists, and Black Hats, mastered the known tradecraft, and developed new techniques. These hackers take great pride in pushing the envelope of knowledge and advancing their art to find vulnerabilities and compromise the most secure academic, commercial, and government systems on the planet. They are essentially cyber criminals, although many are guilty of rather benign breaches of secure services, defacement of web sites, theft of multimedia, and generic cyber hooliganism. The FBI has imprisoned or sought prosecution of many such hackers, while others remain just a few steps ahead of the law. These unscrupulous hackers are definitively *not* the kind of people the USG or military would want in their work force. Alternatively, *should* they be? Is the U.S. missing a non-traditional source of advanced talent that already lives in its own back yard? If the Chinese and Russians hire domestic hackers to support their own nationalistic missions, should the U.S. consider doing the same in some cases?²⁵ What if the U.S. military selected some U.S. hackers and afforded them an opportunity for a new life, accompanied by rewarding jobs, challenging work, and an ego-boosting chance to put their KSA to the test against the most advanced hackers on the planet? How many bright minds might take the bait, change their behavior, and put their talents to work for the U.S. military? As reported in The Daily Beast, the National Security Agency has already recruited at hacker conferences, telling curious onlookers, “If you have a few, shall we say, indiscretions in your past, don’t be alarmed,” adding in, “By the way, if you think you saw cool things at DEFCON® 20, just wait until you cross the threshold to NSA.”²⁶

While this initially sounds far-fetched, it may represent a non-traditional recruiting ground worth considering on a case-by-case basis.²⁷

Finding Hidden Talent

Although contemporary aptitude testing and career assignment schemes are applicable for the bulk of the cyber workforce, there remains the possibility of unique and undiscovered talent within the ranks. This talent pool may not even know they have “it” (whatever “it” might be), and may have never explored their skills beyond Firefox®, Word®, and Facebook®. Perhaps they grew up in a home with little to no exposure to computers and networks, yet inside them lives an undeveloped, inherent ability to comprehend complex algorithms, intricate codes, nonsensical computer language, and social personas. Like the untrained child virtuoso who arises from obscurity, somewhere in the armed services live these “born hackers.” Finding such people, and helping them develop their raw talents, presents both a difficult challenge and an interesting opportunity. Perhaps a method for such discovery resides in non-traditional testing, tailored to identify natural aptitudes, analytic thought, cognitive reasoning, and ingrained curiosity. Such a workable model might be akin to the approach of the Defense Language Aptitude Battery (DLAB), devised and administered by the Defense Language Institute (DLI). Here the main point is to test for advanced *aptitude*, as opposed to learned *knowledge*; the latter we can teach the former we cannot.²⁸ Personnel entering the services, and those already employed, can be screened through specialized testing to see if they possess the aptitude and attitude required for advanced cyber operations, and those found to match the profile can then be designated for special training and duty assignment, regardless of their original/current military occupational specialty code.

Retaining TOP Cyber Talent

In civilian and military arenas, the most perplexing staffing dilemmas often revolve around the question, “How do we *retain* the most advanced, experienced, high-end talent?” In considering a return on investment calculus within the military, what actions would ensure the continued service of those high-end SMEs who have mastered complex skills, have earned advanced certifications, and for whom private industry is aggressively recruiting? Civil service affords pay options such as annual performance bonuses and work-role premium pay scales, a sense of job security, reasonable work conditions, flexible work schedules, and family-life stability. Contemporary private security industry affords all this, adding higher pay, improved flexibility, better work conditions, excellent benefits, robust education and training, conference and symposia funding, access to state-of-the-art hardware/software, and personal empowerment. Present-day military options are much more restricted however, and few financial incentives tie directly to personal performance, mastery of complex skills, or attainment of advanced certifications and degrees. Appealing to patriotism and promises of military retirement are low-percentage options for retaining TOP Cyber personnel. Although “money isn’t everything,” it is certainly a key factor; but so too is significantly rewarding, intellectually stimulating, technologically challenging, and ego satisfying work. Service pressures to maximize OL&M skills while de-emphasizing technical performance (as a member advances) serve as de-motivators for many, causing some high-end SMEs to opt for civilian employment, not so much for the allure of money, but for the perpetual technical challenge and the ability to continue to advance while remaining technical. Although politically difficult, it remains feasible that the military can create new programs that emphasize career-long technical focus and grade advancement based on mastery of complex skills, accompanied by rewards such as selective

reenlistment bonuses, special performance pay, advanced education opportunities, professional certification, and selected duty assignments. TOP Cyber operators with dozens of companies offering them enormous signing bonuses and job deals *may* choose to remain in military service if they can retain their technical focus throughout their careers. Development of the equivalent of a Cyber Warrant Officer Corps may represent one potential means for achieving the desired outcome. Another may be establishing a separate and unique technical track for cyber professionals comprising *both* enlisted and officer ranks. If America's adversaries can selectively dedicate their nation's best SMEs to advanced cyber work, should not the U.S. be able to do the same? Is not the prize worth breaking the mold of the status quo? Is the risk not worth the price to changing the modus operandi? Reality dictates that the answer is yes.

Recommendations

This paper recommends ten specific courses of action for Cyber Command consideration in recruiting, staffing, training, and retaining its growing cyber forces.

1. Continue the current recruiting and training programs in the USCC, the SCEs, and the USG, with the goal of drastically raising the overall cyber competencies of the baseline workforce.
2. Invest in fundamental training courses such as JCAC and continue to deliver advanced follow-on training on a continual, career-long basis, raising emphasis on attaining and maintaining advanced technical skills.
3. Re-focus emphasis for the mass body of cyber professionals onto cyber intelligence, surveillance, and reconnaissance (ISR) missions focused on *passive defense* (administer, secure, maintain, patch, update, scan, report, and maintain oversight on the DOD Information Network - DODIN).

4. Extend search and discovery (AKA “hunt”) missions to highly competent cyber personnel that master advanced courses and operational tasks, and gain the KSA/experience to distinguish, assess, and analyze APT actor actions.
5. De-emphasize the ideology of ubiquitous active cyber warfare and active defensive measures, setting aside this advanced, complex, and dangerous activity for those selected for TOP Cyber missions.
6. Create, maintain, and perpetually fund, advanced industry-standard certification courses in all aspects of network security, ethical hacking, intrusion detection, and like coursework, ensuring cyber personnel remain up to date with the rapidly changing state-of-the-art.
7. Provide greatly expanded university education for enlisted and officer alike, in computer science, network security, and cyber defense, to include teaching courses through the local education centers on military bases worldwide.
8. Extend opportunities for advanced studies in related sciences to *both* enlisted personnel and officers, to include participation in programs at service-run schools (such as NPS and AFIT), and fellowships at contemporary civilian universities.
9. Create a technical track programs that allows military cyber professionals to continue to advance in pay grade while remaining focused on technical achievement in a perpetual continuum of technical work and associated studies, as opposed to becoming managers at senior enlisted levels.
10. Create the equivalent of a JSOC-like Cyber Corps, where Joint military units will conduct the most advanced, important, “active” cyber war fighting, and the deep analytic reconnaissance, analysis, coding, and modeling needed to underpin it.

Conclusion

The cyber threat facing the U.S. presents a real and present danger to the safety and security of our nation. This is a reality understood at the highest levels of federal civilian leadership, military command, corporate industry, and advanced academia. Significant actions to raise public awareness, to rise up a new model army of cyber warriors, and to prepare to fight, survive, and win in the changing battlefield of cyberspace. Despite best intentions, there is danger and likelihood that the traditional model for military recruitment, education, training, and assignment will prove inadequate to the task of raising up and retaining the extremely high quality, *master*-level talent required to combat and overcome the most advanced persistent threats in cyberspace. Re-focusing the bulk of the cyber workforce toward passive defense, system sustainment, “hunting” and related ISR-related disciplines, accompanied by establishment of a JSOC-like operation comprising the top one percent of the cyber workforce, raises the likelihood of success in the coming battles. The attainment of such a team demands an as-yet unseen willingness to think outside the norm and to consider non-traditional methods for recruiting, training, employing, advancing, and retaining an advanced capability work force. Traditional thinkers need not apply.

Bibliography

- Aitoro, Jill R. "Cyber Talent Pool to Shrink with DOD Workforce Expansion." *Washington Business Journal Fed Biz Daily*, 28 January 2013. http://www.bizjournals.com/washington/blog/fedbiz_daily/2013/01/cyber-talent-pool-to-shrink-with-dod.html?page=all (accessed 3 October 2013).
- Adams, Rebecca. "Will China Stop Cyber Espionage? Absolutely Not." *Huffington Post Blog*, 6 June 2013. http://www.huffingtonpost.com/rebecca-abrahams/will-china-stop-cyber-esp_b_3398271.html (accessed 2 December 2013).
- Akin, Jeff. "How to Create the Best Federal Cybersecurity Workforce." *Federal News Radio 1500 AM*, 11 June 2010. <http://www.federalnewsradio.com/88/1978386/How-to-create-the-best-federal-cybersecurity-workforce> (accessed 21 September 2013).
- Anderson, Mark. "Don't Let Snowden Overshadow the Real Cyber Threat." *The Financial Times. Opinion*. 25 July 2013. <http://www.ft.com/cms/s/0/d18f1e6a-ef97-11e2-a237-00144feabdc0.html#axzz2kZOH9Qln> (accessed 15 November 2013).
- Apps, Peter, and Brenda Goh. "Cyber Warrior Shortage Hits Anti-Hacker Fightback." *Reuters*, 13 October 2013. <http://www.reuters.com/article/2013/10/13/net-us-security-internet-idUSBRE99C03F20131013> (accessed 10 December 2013).
- Armerding, Taylor. "DHS Aims to Hire 600 Cybersecurity Pros - If it Can Find Them." *CSO Security Leadership*, 13 November 2012. <http://www.csoonline.com/article/721444/dhs-aims-to-hire-600-cybersecurity-pros-if-it-can-find-them> (accessed 3 October 2013).
- Ball, Desmond. "China's Cyber Warfare Capabilities." *Security Challenges AU*, Winter 2011. <http://www.securitychallenges.org.au/ArticlePDFs/vol7no2Ball.pdf> (accessed 8 December 2013).
- Ballenstedt, Brittany. "Building Cyber Warriors." *Government Executive*. 15 August 2011. <http://www.govexec.com/magazine/features/2011/08/building-cyber-warriors/34656/> (accessed 16 November 2013).
- Barboza, David. "Hacking Inquiry Puts China's Elite in New Light." *The New York Times*, 21 February 2010. <http://www.nytimes.com/2010/02/22/technology/22cyber.html> (accessed 12 November 2013).
- Beidel, Eric, and Stew Magnuson. "Government, Military Face Severe Shortage of Cybersecurity Experts." *National Defense*, August 2011. <http://www.nationaldefensemagazine.org/archive/2011/August/Pages/Government,MilitaryFaceSevereShortageOfCybersecurityExperts.aspx> (accessed 17 September 2013).
- Belani, Rohyt. "APT Mitigation: The Human Way." *Mandiant Blog*, 5 December 2013. https://www.mandiant.com/blog/apt-mitigation-the-human-way/?utm_source=rss&utm_medium=rss&utm_campaign=apt-mitigation-the-human-way (accessed 10 December 2013).
- Bennett, Dashiell. "Did Iran Hack The World's Biggest Oil Company?" *The Wire: Technology*, 24 October 2012. <http://www.thewire.com/technology/2012/10/did-iran-hack-worlds-biggest-oil-company/58284/> (accessed 3 December 2013).

- Blau, John. "Russia – a Happy Haven for Hackers." *Computer Weekly*, May 2004.
<http://www.computerweekly.com/feature/Russia-a-happy-haven-for-hackers> (accessed 17 November 2013), 1-4.
- Brown, Gary D. "Why Iran Didn't Admit Stuxnet Was an Attack." *Joint Forces Quarterly*, Issue 63, 4th Quarter 2011. <http://www.dtic.mil/doctrine/jfq/jfq-63.pdf> (accessed 13 October 2013) p. 70-73.
- Bumiller, Elisabeth. "Pentagon Expanding Cybersecurity Force to Protect Networks Against Attacks." *The New York Times*, 27 January 2013.
http://www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html?_r=1&#h (accessed 2 October 2013).
- Buxbaum, Peter A. "Building a Better Cyber Range." *ISN/ETH Zurich International Relations and Security Network*, 21 March 2012. <http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=127714> (accessed 16 November 2013).
- Carroll, Rory. "US Urged to Recruit Master Hackers to Wage Cyber War on America's foes." *The Guardian*, 10 July 2012. <http://www.theguardian.com/technology/2012/jul/10/us-master-hackers-al-qaida> (accessed 12 December 2013).
- Chabrow, Eric. "7 Levels of Hackers. Applying An Ancient Chinese Lesson: Know Your Enemies." *The Public Eye*, 25 February 2012. <http://www.bankinfosecurity.com/blogs/7-levels-hackers-p-1206> (accessed 1 December 2013).
- Chen, Thomas. "An Assessment of the DoD Strategy for Operating in Cyberspace." *U. S. Army Strategic Studies Institute*, 23 September 2013.
<http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=1170> (accessed 11 December 2013).
- Claburn, Thomas. "China Closes Hacker Training Site." *Information Week*, 8 February 2010.
<http://www.informationweek.com/security/vulnerabilities-and-threats/china-closes-hacker-training-site/d/d-id/1086734> (accessed 3 December 2013).
- Cornish, Paul. "On Cyber Warfare." *A Chatham House Report*, 3 November 2010.
https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf (accessed 11 November 2013).
- Corrin, Amber. "Navy's Cyber Unit Scans Horizon for New Challenges." *Defense Systems*, 21 July 2011. <http://defensesystems.com/articles/2011/06/08/cyber-defense-navy-cyber-programs.aspx> (accessed 3 October 2013).
- Corrin, Amber. "Air Force Expects to Hire Cyber Pros." *FCW: The Business of Federal Technology*, 22 January 2013. <http://fcw.com/articles/2013/01/22/cyber-command-hires.aspx> (accessed 3 October 2013).
- Coulson, Stuart. "The Seven Levels of Cyber Security Hacking Explained." *Business Insider*, 24 February 2012. <http://www.business7.co.uk/business-news/business-view-and-comment/2012/02/24/explaining-the-seven-levels-of-cyber-security-106408-23763473/> (accessed 12 December 2013).
- Cox, Alex, Chris Elisan, Will Gregido, Chris Harrington, and John McNeill. "The VOHO Campaign: An In Depth Analysis." *RSA FirstWatch Team Whitepaper*, 2012.

- http://blogs.rsa.com/wp-content/uploads/VOHO_WP_FINAL_READY-FOR-Publication-09242012_AC.pdf (accessed 12 October 2013).
- Davis, Joshua L. Georgia Tech. "Building Cyber Warriors." *GA Tech Technical briefing*, undated. http://www.itea.org/~iteaorg/images/pdf/Events/2012_Proceedings/2012_Cyber/track_3_davis_cyberwarriorbrief.pdf (accessed 16 November 2013).
- Demchak, Chris C., and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly*, Spring 2011. <http://www.au.af.mil/au/ssq/2011/spring/demchak-dombrowski.pdf> (accessed 1 December 2013).
- Demick, Barbara. "China Says it Shut Down Online Academy for Hackers." *Los Angeles Times*, 9 February 2010. <http://articles.latimes.com/2010/feb/09/world/la-fg-china-hackers9-2010feb09> (accessed 16 November 2013).
- Doherty, Stephen. "Hidden Lynx – Professional Hackers for Hire." *Symantec: Security Response*, 17 February 2013. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf (accessed 19 November 2013).
- Donelly, Harrison. "US 24th Air Force. Maj Gen. Vautrinot's interview with MIT Magazine." *Air Force News*, 7 February 2013. <http://www.24af.af.mil/news/story.asp?id=123289111> (accessed 1 October 2013).
- Doty, Joseph, and T. J. O'Connor. "Building Teams of Cyber Warriors." *Army Magazine*. January 2010. http://www.ausa.org/publications/armymagazine/archive/2010/1/Documents/FC_Doty_0110.pdf (accessed 13 November 2013).
- Drummond, David. "A New Approach to China." *Google Official Blog*, 12 January 2010. <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html> (accessed 19 November 2013).
- Eddy, Max. "The Chinese Hacking Empire: Don't Believe the hype." *ITProPortal*, 29 May 2013. <http://www.itproportal.com/2013/05/29/the-chinese-hacking-empire-dont-believe-the-hype/> (accessed 17 November 2013).
- Editor. "Hydraq - An Attack of Mythical Proportions." *Symantec Official Blog*, 15 January 2010. <http://www.symantec.com/products-solutions/training/> (accessed 9 November 2013).
- Editor. "Luckycat Redux: Inside an APT Campaign with Multiple Targets in India and Japan." *Trend Micro Research Paper*, 2012. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf (accessed 22 November 2013).
- Editor. "M-Trends 2010: The Advanced Persistent Threat." *Mandiant M-Trends Report, 2010*. https://dl.mandiant.com/EE/assets/PDF_MTrends_2010.pdf?elq=afb700e5cd22471184f20d7f447def11&elqCampaignId= (accessed 1 December 2013).
- Editor. "M-Trends 2011: When Prevention Fails." *Mandiant M-Trends Report 2011*. https://dl.mandiant.com/EE/assets/PDF_MTrends_2011.pdf?elq=4515fa49a05e485096d796b919c8173b&elqCampaignId= (accessed 1 December 2013).

Editor. "M-Trends 2012: An Evolving Threat." *Mandiant M-Trends Report 2012*.
https://dl.mandiant.com/EE/assets/PDF_MTrends_2012.pdf?elq=9cda0e3308934c76a6aa59c1fb0b1ba3&elqCampaignId= (accessed 2 December 2013).

Editor. "M-Trends 2013: Attack the Security Gap." *Mandiant M-Trends Report 2013*.
https://dl.mandiant.com/EE/library/M-Trends_2013.pdf?elq=26f1d1e457634ee3a2a6ea238fb89de9&elqCampaignId= (accessed 4 December 2013).

Editor. "APT1 – Exposing One of China’s Cyber Espionage Units." *Mandiant Technical Report*, 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (accessed 8 November 2013).

Editor. "China Large Hacker Training Web Site Shut Down." *CNN Tech*, 8 February 2010.
<http://www.cnn.com/2010/TECH/02/08/china.hackers/> (accessed 13 September 2013).

Editor. "The Four V’s of Big Data." *International Business Machines* quad-chart.
<http://www.ibmbigdatahub.com/enlarge-infographic/1642> (accessed 10 December 2013).

Editor, Reuters. "The Training Ground for China’s Digital Army." *Business Tech*, 19 July 2013.
<http://businesstech.co.za/news/international/42360/the-training-ground-for-chinas-digital-army/> (accessed 20 November 2013).

El-Harmeel, Muhammad. "Humans - The Overlooked Asset." *SANS Cyber Defense Whitepapers*, 1 November 2009. <http://cyber-defense.sans.org/resources/papers/gsec/humans-overlooked-asset-116347> (accessed 22 September 2013).

Estes, Adam Clarke. "To Combat China's Hacker Army, the U.S. Is Copying Its Methods." *Motherboard: Hackers*, 2 April 2013. <http://motherboard.vice.com/blog/the-government-burgeoning-hacker-army-is-inspired-china> (accessed 7 December 2013).

Evans, Karen, and Franklin Reeder. "A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters." *A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. 15 November 2010. <http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity> (accessed 30 September 2013).

Finkle, Jim. "Hacker Group in China Linked to Big Cyber Attacks: Symantec." *Reuters*, 17 September 2013. <http://www.reuters.com/article/2013/09/17/us-cyberattacks-china-idUSBRE98G0M720130917> (accessed 17 October 2013).

Finkle, Jim. "U.S. Seeks Patriotic Computer Geeks for Help in Cyber Crisis." *NBC News.Com Technology*, 31 October 2012. <http://www.nbcnews.com/technology/technolog/u-s-seeks-patriotic-computer-geeks-help-cyber-crisis-1C6782914> (accessed 2 October 2013).

Fisher, Max. "South Korea Under Cyber Attack: Is North Korea Secretly Awesome at Hacking?" *The Washington Post*, 20 March 2013. <http://www.washingtonpost.com/blogs/worldviews/wp/2013/03/20/south-korea-under-cyber-attack-is-north-korea-secretly-awesome-at-hacking/> (accessed 19 November 2013).

Fryer-Briggs, Zachary. "U. S. Military Goes on Cyber Offensive." *Defense News*, 24 March 2012. <http://www.defensenews.com/article/20120324/DEFREG02/303240001/> (accessed 22 November 2013).

- Garamone, Jim. "Questions Abound in Cyber Theater of Operations, Vice Chairman Says." *U.S. Department of Defense News*, 9 June 2009. <http://www.defense.gov/news/newsarticle.aspx?id=54709> (accessed 29 September 2013).
- Gertz, Bill. "White House Hack Attack." *Washington Free Beacon*, 30 September 2012. <http://freebeacon.com/white-house-hack-attack/> (accessed 27 November 2013).
- Gewirtz, David. "For China, Hacking May be all About Sun Tzu and World War III." *ZDNet Government*, 29 May 2013. <http://www.zdnet.com/for-china-hacking-may-be-all-about-sun-tzu-and-world-war-iii-7000015988/> (accessed 29 November 2013).
- Goodlin, Dan. "Meet Hidden Lynx: The Most Elite Hacker Crew You've Never Heard Of." *Ars Technica*, 17 September 2013. <http://arstechnica.com/security/2013/09/meet-hidden-lynx-the-most-elite-hacker-crew-youve-never-heard-of/> (accessed 22 September 2013).
- Goldsmith, Jack. "The NSA's Growing Role in Domestic Cybersecurity." *Lawfare: Hard National Security Choices*, 21 October 2010. <http://www.lawfareblog.com/2010/10/the-nsa%E2%80%99s-growing-role-in-domestic-cybersecurity/> (accessed 3 October 2013).
- Glenny, Misha. "Hire the Hackers!" *TED Global 2011/TED Talk*, July 2011. Audio/video presentation. http://www.ted.com/talks/misha_glenny_hire_the_hackers.html (accessed 13 November 2013).
- Gray, Colin S. "Making Strategic Sense of Cyber Power Why The Sky is not Falling." U. S. Army Strategic Studies Institute, April 2013. <http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1147> (accessed 28 November 2013).
- Hadnagy, Christopher. *Social Engineering: The Art of Human Hacking*. Indianapolis, IN: Wiley Publishing, 2011.
- Harris, Shane. "How Did Syria's Hackers Suddenly Get so Good?" *The Seattle Times*, 4 September 2013. http://seattletimes.com/html/nationworld/2021756024_syriahackxml.html (accessed 28 September 2013).
- Harwood, Matthew. "China: Hacker Schools Become Big Business." *Security Management*, 5 August 2009. <http://www.securitymanagement.com/print/6017> (accessed 13 September 2013).
- Haynie, Devon. "U.S. Sees Record Number of International College Students." *U.S. News*, 11 November 2013. <http://www.usnews.com/education/best-colleges/articles/2013/11/11/us-sees-record-number-of-international-college-students> (accessed 30 November 2013).
- Henderson, Scott. "Chinese Hacker Schools Growing Bolder." *The Dark Visitor*, 17 August 2009. <http://www.thedarkvisitor.com/2009/08/chinese-hackers-schools-growing-bolder/> (accessed 19 November 2013).
- Henderson, Scott. "The Dark Visitor - Inside the World of Chinese Hackers." *The Dark Visitor*, October 2007. http://www.lulu.com/items/volume_62/2048000/2048958/4/print/2048958.pdf (accessed 10 December 2013).
- Hoover, J. Nicholas. "Closing the Cybersecurity Gap In Government." *Information Week: Government*, 30 August 2010. <http://www.informationweek.com/government/security/closing-the-cybersecurity-gap-in-governm/227100067> (accessed 29 September 2013).

- Hsu, Francis. "Principles of (Information?) War." *Joint Forces Quarterly*, Issue 61, 2nd Quarter 2011. <http://www.ndu.edu/press/lib/images/jfq-60/jfq-61/JFQ61.pdf> (accessed 17 November 2013), p. 27-31.
- Jinghua, Lu. "China's Cyber Threat: Real or Imaginary?" *China US Focus*, 7 July 2013. <http://www.chinausfocus.com/peace-security/chinas-cyber-threat-real-or-imaginary/> (accessed 16 November 2013).
- Jullien, Francois. *The Propensity of Things: Toward a History of Efficacy in China*. Cambridge, MA: Zone Books, 1999.
- Kopstein, Joshua. "How the NSA Recruits in a Post-Snowden World." *The Daily Beast*, 17 January 2014. <http://www.thedailybeast.com/articles/2014/01/17/how-the-nsa-recruits-in-a-post-snowden-world.html> (accessed 21 January 2014).
- Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyber Power and National Security*. Washington, DC: NDU Press, 2012.
- Lai, David. "Learning from the Stones: A Go Approach to Mastering China's Strategic Concept, Shi." *U. S. Army Strategic Studies Institute*, 1 May 2004. <http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=378> (accessed 10 December 2013).
- Langevin, Jim. "Column: Cyber Dominance Meaningless Without Skilled Workforce." *Federal News Radio 1500 AM*, 24 October 2012. <http://www.federalnewsradio.com/1049/3089868/Column-Cyber-dominance-meaningless-without-skilled-workforce> (accessed 29 September 2013).
- Lavigna, et al. "Cyber IN-Security: Strengthening the Federal Cybersecurity Workforce." *Booz \ Allen \ Hamilton: Partnership for Public Service*, July 2009. <http://ourpublicservice.org/OPS/publications/download.php?id=135> (accessed 1 October 2013).
- Lawson, David. "Iran Accused of Hacking into US Navy Computers." *CIO Magazine*, 27 September 2013. http://www.cio.com.au/article/527753/iran_accused_hacking_into_us_navy_computers/ (accessed 30 November 2013).
- Lever, Rob. "US Scholarships Aim to Close Cybersecurity Gap." *Phys.Org.*, 29 September 2012. <http://phys.org/news/2012-09-scholarships-aim-cybersecurity-gap.html> (accessed 24 September 2013).
- Levine, Mike. "Outgoing DHS Secretary Janet Napolitano Warns of 'Serious' Cyber Attack, Unprecedented Natural Disaster." *ABC News: Politics*, 27 April 2013. <http://abcnews.go.com/blogs/politics/2013/08/outgoing-dhs-secretary-janet-napolitano-warns-of-serious-cyber-attackunprecedented-natural-disaster/> (accessed 21 September 2013).
- Lewis, James (Moderator). "U.S. Cyber Security Policy and the Role of USCYBERCOM." CSIS Cybersecurity Policy Debate Series, 3 June 2010. http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf (accessed 10 December 2013).
- Liebelson, Dana. "Why Iran's Hackers Might Be Scarier Than China's." *Mother Jones*, 30 May 2013. <http://www.motherjones.com/politics/2013/05/who-has-scarier-hackers-china-or-iran> (accessed 26 September 2013).

- Littell, Charles. "AFIT's Cyber Warriors Develop New Cyber Career Field Training." *Air Force Print News Today*, 11 December 2009. http://www.wpafb.af.mil/news/story_print.asp?id=123181838 (accessed 11 December 2013).
- Lonsdale, David J. *The Nature of War in the Information Age*. New York, NY: Frank Cass, 2004.
- Mick, Jack. "Federal Reserve Hacked, WSJ Still Under Heavy Fire From Chinese Hackers." *Daily Tech*, 6 February 2013. <http://www.dailytech.com/Federal+Reserve+Hacked+WSJ+Still+Under+Heavy+Fire+From+Chinese+Hackers/article29841.htm> (accessed 9 December 2013).
- Miles, Donna. "DOD, Homeland Security Collaborate in Cyber Realm." *Defense.gov News*, 3 June 2011. <http://www.defense.gov/news/newsarticle.aspx?id=64186> (accessed 19 September 2013).
- Milevski, Lukas. "Stuxnet and Strategy - A Special Operation in Cyberspace?." *Joint Forces Quarterly*, Issue 63, 4th Quarter 2011. <http://www.dtic.mil/doctrine/jfq/jfq-63.pdf> (accessed 15 October 2013) p. 64-69.
- Miller, Robert. Daniel Kuehl, and Irving Iachow. "Cyber War: Issues in Attack and Defense." *Joint Forces Quarterly*, Issue 61, 2nd Quarter 2011. <http://www.ndu.edu/press/lib/images/jfq-60/jfq-61/JFQ61.pdf> (accessed 17 November 2013), p. 18-23.
- Minnick, Wendell. Experts: "Chinese Cyber Threat to US Is Growing." *Defense News*. 9 July 2013. <http://www.defensenews.com/article/20130709/DEFREG03/307090009/> (accessed 16 November 2013).
- Morozov, Evgeny. *The Net Delusion: The Darker Side of Internet Freedom*. New York, NY: Public Affairs, 2011.
- Nakashima, Ellen. "China Proves to be an Aggressive Foe in Cyberspace ." *The Washington Post*, 11 November 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/11/10/AR2009111017588_pf.html (accessed 20 September 2013).
- Nakashima, Ellen. "Cyber Command's Growth Plan Raises a Lot of Questions." *The Washington Post: National Security*, 27 January 2013. http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/19/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html (accessed 22 September 2013).
- Osinga, Frans P.B. *Science, Strategy and War: The Strategic Theory of John Boyd*. New York, NY: Routledge, 2007.
- Pellerin, Cheryl. "Cybercom Builds Teams for Offense, Defense in Cyberspace." *U.S. Department of Defense News*, 12 March 2013. <http://www.defense.gov/news/newsarticle.aspx?id=119506> (accessed 1 October 2013).
- Perlroth, Nicole, and Quentin Hardy. "Bank Hacking Was the Work of Iranians, Officials Say." *The New York Times*, 8 January 2013. http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0 (accessed 10 December 2013).
- Plafke, James. "Single Chinese Hacking Unit Responsible for Stealing Terabytes of Data From Hundreds of Organizations, Says US Security Firm." *Extreme Tech*, 20 February 2013. <http://www.extremetech.com/computing/148800-single-chinese-hacking-unit-responsible-for->

- stealing-terabytes-of-data-from-hundreds-of-organizations-says-us-security-firm (accessed 2 December 2013).
- Ramo, Joshua Cooper. "Talking Cyber Threat With China." *The New York Times. The Opinion Pages*. 9 July 2013. http://www.nytimes.com/2013/07/10/opinion/global/talking-cyberthreat-with-china.html?_r=0 (accessed 16 November 2013).
- Reed, John. "Inside one of U.S. Cyber Command's Offensive Units." *FP National Security: Killerapps*. http://killerapps.foreignpolicy.com/posts/2012/10/24/inside_one_of_us_cyber_commands_offensive_units_0 (accessed 29 September 2013).
- Riley, Michael. "Snowden's Leaks Cloud U.S. Plan to Curb Chinese Hacking." *Bloomberg*, 30 January 2013. <http://www.bloomberg.com/news/print/2013-07-01/snowden-s-leaks-cloud-u-s-plan-to-curb-chinese-hacking.html> (accessed 13 November 2013).
- Riley, Michael. "Hackers Linked to China's Army Seen From EU to D.C." *Bloomberg*, 26 June 2012. <http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html> (accessed 22 November 2013).
- Rohozinski, Rafal. "Tracking GhostNet: Investigating a Cyber Espionage Network." *Information Warfare Monitor*, 29 March 2009. <http://www.nartv.org/mirror/ghostnet.pdf> (accessed 18 November 2013).
- Sahadi, Michael K. Keeping JSOC a Secret: The Exposure of Special Warfare and its Adverse Effects on National Security and Defense to the United States. 2013 Military Legitimacy Review. <http://militarylegitimacyreview.com/wp-content/uploads/2013/05/KEEPING-JSOC-A-SECRET.pdf> (accessed 12 January 2014).
- Sanger, David, David Barboza, and Nicole Perlroth. "Chinese Army Unit is Seen Tied to Hacking Against U.S." *The New York Times*, 18 February 2013. http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?_r=1& (accessed 2 December 2013).
- Schanz, Mark V. "Building Better Cyber Warriors." *Air Force Magazine*. September 2010. <http://www.airforcemag.com/MagazineArchive/Pages/2010/September%202010/0910cyber.aspx> (accessed 13 November 2013).
- Schreier, Fred. "On Cyberwarfare." *DCAF Horizon Paper 2015 Working Paper No. 7*, 2012. <http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf> (accessed 22 November 2013).
- Sheldon, John B. "Deciphering Cyberpower Strategic Purpose in Peace and War." *Strategic Studies Quarterly*, Summer 2011. www.au.af.mil/au/ssq/2011/summer/sheldon.pdf (accessed 20 September 2013).
- Serbu, Jared. "DoD Building Cyber Workforce of the Future." *In Federal News Radio*. 19 September 2012. <http://www.federalnewsradio.com/885/3021032/DoD-building-cyber-workforce-of-the-future> (accessed 15 November 2013).
- Small, Prescott E. "Defense in Depth: An Impractical Strategy for a Cyber World." *SANS Cyber Defense Whitepapers*, 14 November 2011. <http://cyber-defense.sans.org/resources/papers/gsec/defense-depth-impractical-strategy-cyber-world-114659> (accessed 15 September 2013).

- Smith, Dirk A.D. "NSA: Looking for a Few Good Cybersecurity Professionals." *Network World*, 13 November 2012, <http://www.networkworld.com/news/2012/111312-nsa-cybersecurity-264223.html> (accessed 2 October 2013).
- Smith, Tiffany S. "In Pursuit of an Aptitude Test for Potential Cyberspace Warriors." *AFIT/GIR/ENG/07-01*, Student Thesis. <http://www.hsdl.org/?view&did=479420> (accessed 19 November 2013).
- Stevenson, Alastair. "China Responsible for 96 percent of World's Cyber Spying Campaigns." *V3-CO-UK*, 23 April 2013. <http://www.v3.co.uk/v3-uk/news/2263187/china-responsible-for-96-percent-of-worlds-cyber-spying-campaigns> (8 November 2013).
- Stevenson, Alastair. "Chinese Military Unit Accused of Cyber Attacks on 141 Companies." *V3-CO-UK*, 19 February 2013. <http://www.v3.co.uk/v3-uk/news/2244837/chinese-military-unit-accused-of-cyber-attacks-on-141-companies> (accessed 10 November 2013).
- Stevenson, Alastair. "US Government: Chinese Hackers Have the Skills to Take Down Critical Infrastructure." *V3-CO-UK*, 7 May 2013. <http://www.v3.co.uk/v3-uk/news/2266397/us-government-chinese-hackers-have-the-skills-to-take-down-critical-infrastructure> (accessed 10 December 2013).
- Stewart, Joshua. "Navy Wants 1,000 More Cyber Warriors." *Navy Times*, 2013. <http://www.navytimes.com/article/20130423/NEWS/304230016/Navy-wants-1-000-more-cyber-warriors> (accessed 30 September 2013).
- Stokes, Mark. "Countering Chinese Cyber Operations Opportunities and Challenges for U.S. Interests Opportunities and Challenges for U.S. Interests." *Project 2049 Institute*, 29 October 2012. http://project2049.net/documents/countering_chinese_cyber_operations_stokes_hsiao.pdf (accessed 17 November 2013).
- Stokes, Mark. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure." *Project 2049 Institute*, 11 November 2011. http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf (accessed 1 December 2013).
- Tapscott, Don. *Grown up Digital: How the Net Generation is Changing Your World*. New York, NY: McGraw-Hill, 2009.
- The Cybersecurity Act of 2012*. S. 3414. 112th Cong., 2nd sess., 19 July 2012. <http://www.gpo.gov/fdsys/pkg/BILLS-112s3414pcs/pdf/BILLS-112s3414pcs.pdf> (accessed 27 September 2013).
- The Cyber Warrior Act of 2013*. Senate Bill S658, 22 March 2013. <http://beta.congress.gov/bill/113th/senate-bill/658/text> (accessed 10 December 2013).
- The Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011* (the PRECISE Act). H.R. 3674. 112th Cong., 1st sess., 15 December 2011. <http://www.gpo.gov/fdsys/pkg/BILLS-112hr3674ih/pdf/BILLS-112hr3674ih.pdf> (accessed 1 October 2013).
- The Whitehouse. "The Comprehensive National Cybersecurity Initiative." The White House: National Security Council, 20 January 2008. <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative> (accessed 23 September 2013).

- Tonelson, Alan. "Chinese Hacking Is Made in the U.S.A." *Bloomberg*, 28 May 2013. <http://www.bloomberg.com/news/2013-03-28/chinese-hacking-is-made-in-the-u-s-a-.html> (accessed 20 September 2013).
- Tromba, George. "Crafting a Selection Program for Tomorrow's Cyber Warriors." Air War College, 14 February 2013. A Student Professional Study Paper for 2013.
- U.S. - China Economic and Security Review Commission. "The National Security Implications of Investments and Products from the People's Republic of China in the Telecommunications Sector." *USCC Staff Report*, January 2011. http://origin.www.uscc.gov/sites/default/files/Research/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf (accessed 30 November 2013).
- U.S. Department of Defense. *Cyber Operations Personnel Report*. Department of Defense Report to the Congressional Defense Committees, April 2011. <http://www.nscivva.org/CyberReferenceLib/2011-04-Cyber%20Ops%20Personnel.pdf> (accessed 15 September 2013).
- U.S. Department of Defense. *Military and Security Developments Involving the People's Republic of China 2013*. Annual Report to Congress, 2013. http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf (accessed 17 November 2013).
- U.S. Department of Defense. *Information Operations*. Joint Publication 3-13. 27 November 2012. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (accessed 16 November 2013).
- U.S. Department of Homeland Security. *Cybersecurity Education and Training Assistance Program (CETAP)*. Catalog of Federal Domestic Assistance, 2009. <https://www.cfda.gov/index?s=program&mode=form&tab=step1&id=15671b2374af0679e2a40baf6e3203bb> (accessed 29 September 2013).
- U.S. Department of Homeland Security. *ICS-CERT Cyber Threat Source Descriptions*, 2009. <http://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions> (accessed 27 September 2013).
- U.S. Department of the Navy. OPNAVINST 5450.345 *Mission, Functions, and Tasks of Commander, U.S. Fleet Cyber Command and Commander, U.S. Tenth Fleet*. 2013. <http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-400%20Organization%20and%20Functional%20Support%20Services/5450.345.pdf> (accessed 1 October 2013).
- U.S. Department of the Navy. "Navy Cyber Power 2020." *Navy Public Affairs*, November 2012. http://www.public.navy.mil/fcc-c10f/Strategies/Navy_Cyber_Power_2020.pdf (accessed 1 October 2013).
- U.S. Department of the Navy. *U.S. Navy Information Dominance Roadmap 2013-2028*. IDC Self-synchronization. <http://www.idcsync.org/documents/20130326%20Navy%20Information%20Dominance%20Roadmap%202013-2028.pdf> (accessed 3 October 2013).
- U.S. Director of National Intelligence. "Foreign Spies Stealing US Economic Secrets in Cyber Space." Counterintelligence Security, October 2011. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (accessed 19 November 2013).

- U.S. National Criminal Intelligence Resource Center. "An Overview of the United States Intelligence Community for the 111th Congress." *NCIRC National Strategies*, 2009. http://www.ncirc.gov/documents/public/ODNI_Overview_of_US_Intell_Community.pdf (accessed 22 September 2013).
- U.S. National Institute of Standards and Technology. "The National Initiative for Cybersecurity Education Strategic Plan." http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf (accessed 22 September 2013).
- U.S. National Institute of Standards and Technology. "The National Cybersecurity Workforce Framework." National Initiative for Cybersecurity Education. http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_v1_1_august2012_for_printing.pdf (accessed 15 September 2013).
- U.S. National Security Agency. "Defense in depth." *National Security Agency Central Security Service Publications*, 2012. http://www.nsa.gov/ia/_files/support/defenseindepth.pdf (accessed 17 September 2013).
- U.S. Secretary of Defense. *Resilient Military Systems and the Advanced Cyber Threat*. Defense Science Board, January 2013. <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf> (accessed 8 December 2013).
- U.S. Senate. *Cyber Threats and Ongoing Efforts to Protect the Nation: Hearings before the House Senate Select Committee on Intelligence*, prepared remarks by Mike Rodgers, 4 October 2011. <http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/100411CyberHearingRodgers.pdf> (accessed 19 November 2013).
- Van Creveld, Martin. *The Transformation of Wars*. New York, NY: The Free Press, 1991.
- Villanova. "Combat Threats with Cyber Security Training." *Villanova University: Cyber Security Training*, 2013. <http://www.villanovau.com/cyber-security-training/> (accessed 26 September 2013).
- White, Gary. "China the World's 'Most Sophisticated' Hacker, says Google's Eric Schmidt." *The Telegraph*, 2 February 2013. <http://www.telegraph.co.uk/finance/9843886/China-the-worlds-most-sophisticated-hacker-says-Google-Eric-Schmidt.html> (accessed 13 November 2013).
- Williams, Brett T. "Ten Propositions Regarding Cyberspace Operations." *Joint Forces Quarterly*, Issue 61, 2nd Quarter 2011. <http://www.ndu.edu/press/lib/images/jfq-60/jfq-61/JFQ61.pdf> (accessed 17 November 2013), p. 11-17.
- Winter, Jana. "Washington Confirms Chinese Hack Attack on White House Computer." *Fox News*, 1 October 2012. <http://www.foxnews.com/tech/2012/10/01/washington-confirms-chinese-hack-attack-on-white-house-computer/> (accessed 12 September 2013).
- Wong, Edward. "Hackers Find China Is Land of Opportunity." *The New York Times*, 22 May 2013. http://www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html?_r=1& (accessed 1 December 2013).
- Zakaria, Fareed. "How Big is China's Cyber Threat?" *CNN World*. 19 February 2013. <http://globalpublicsquare.blogs.cnn.com/2013/02/19/how-big-is-chinas-cyber-threat/> (accessed 16 November 2013).

Notes

1. Editor, "The Four V's of Big Data." *International Business Machines* quad-chart. <http://www.ibmbigdatahub.com/enlarge-infographic/1642> (accessed 10 December 2013), 1.
2. Stuart Coulson. "The Seven Levels of Cyber Security Hacking Explained." *Business Insider*, 24 February 2012. <http://www.business7.co.uk/business-news/business-view-and-comment/2012/02/24/explaining-the-seven-levels-of-cyber-security-106408-23763473/> (accessed 10 December 2013), 1-3.
3. Alastair Stevenson. "China Responsible for 96 percent of World's Cyber Spying Campaigns." *V3-CO-UK*, 23 April 2013. <http://www.v3.co.uk/v3-uk/news/2263187/china-responsible-for-96-percent-of-worlds-cyber-spying-campaigns> (8 November 2013), 1-2.
4. John Blau. "Russia – a Happy Haven for Hackers." *Computer Weekly*, May 2004. <http://www.computerweekly.com/feature/Russia-a-happy-haven-for-hackers> (accessed 17 November 2013), 1-4.
5. Fred Schreier. "On Cyberwarfare." *DCAF Horizon Paper 2015 Working Paper* No. 7, 2012. <http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf> (accessed 22 November 2013), 112-113.
6. Dashiell Bennett. "Did Iran Hack The World's Biggest Oil Company?" *The Wire: Technology*, 24 October 2012. <http://www.thewire.com/technology/2012/10/did-iran-hack-worlds-biggest-oil-company/58284/> (accessed 3 December 2013), 1-3.
7. Nicole Perlroth and Quentin Hardy. "Bank Hacking Was the Work of Iranians, Officials Say." *The New York Times*, 8 January 2013. http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0 (accessed 10 December 2013), 1-2.
8. Editor. "M-Trends 2010: The Advanced Persistent Threat." *Mandiant M-Trends Report, 2010*. https://dl.mandiant.com/EE/assets/PDF_MTrends_2010.pdf?elq=afb700e5cd22471184f20d7f447def11&elqCampaignId= (accessed 1 December 2013), 1-32.
9. Editor. "APT1 – Exposing One of China's Cyber Espionage Units." *Mandiant Technical Report*, 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (accessed 8 November 2013), 1-76.
10. Ibid, 3.
11. Ibid.
12. Stephen Doherty. "Hidden Lynx – Professional Hackers for Hire." *Symantec: Security Response*, 17 February 2013. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf (accessed 19 November 2013), 5.
13. Editor. "Luckycat Redux: Inside an APT Campaign with Multiple Targets in India and Japan." *Trend Micro Research Paper*, 2012. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf (accessed 22 November 2013), 4.

14. Mark Stokes. "Countering Chinese Cyber Operations Opportunities and Challenges for U.S. Interests Opportunities and Challenges for U.S. Interests." *Project 2049 Institute*, 29 October 2012. http://project2049.net/documents/countering_chinese_cyber_operations_stokes_hsiao.pdf (accessed 17 November 2013), 7.
15. Jack Goldsmith. "The NSA's Growing Role in Domestic Cybersecurity." *Lawfare: Hard National Security Choices*, 21 October 2010. <http://www.lawfareblog.com/2010/10/the-nsa%E2%80%99s-growing-role-in-domestic-cybersecurity/> (accessed 3 October 2013).
16. GEN Keith B. Alexander. "U.S. Cybersecurity Policy and the Role of USCYBERCOM." *Cybersecurity Policy Debate Series*, 3 June 2010, Washington, D.C. http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf (accessed 10 December 2013), 4.
17. The Whitehouse. "The Comprehensive National Cybersecurity Initiative." *The White House: National Security Council*, 20 January 2008. <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative> (accessed 23 September 2013), 1-5.
18. U.S. National Institute of Standards and Technology. "The National Initiative for Cybersecurity Education Strategic Plan." http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf (accessed 22 September 2013).
19. Peter Apps and Brenda Goh. "Cyber Warrior Shortage Hits Anti-Hacker Fightback." *Reuters*, 13 October 2013. <http://www.reuters.com/article/2013/10/13/net-us-security-internet-idUSBRE99C03F20131013> (accessed 10 December 2013), 1-4.
20. Jill Aitoro, "Cyber Talent Pool to Shrink with DOD Workforce Expansion." *Washington Business Journal Fed Biz Daily*, 28 January 2013. http://www.bizjournals.com/washington/blog/fedbiz_daily/2013/01/cyber-talent-pool-to-shrink-with-dod.html?page=all (accessed 3 October 2013), 1.
21. Jared Serbu. "DoD Building Cyber Workforce of the Future." *In Federal News Radio*. 19 September 2012. <http://www.federalnewsradio.com/885/3021032/DoD-building-cyber-workforce-of-the-future> (accessed 15 November 2013), 2-4.
22. Eric Beidel and Stew Magnuson. "Government, Military Face Severe Shortage of Cybersecurity Experts." *National Defense*, August 2011. <http://www.nationaldefensemagazine.org/archive/2011/August/Pages/Government,MilitaryFaceSevereShortageOfCybersecurityExperts.aspx> (accessed 17 September 2013), 2-3.
23. Brett T. Williams. "Ten Propositions Regarding Cyberspace Operations." *Joint Forces Quarterly*, Issue 61, 2nd Quarter 2011. <http://www.ndu.edu/press/lib/images/jfq-60/jfq-61/JFQ61.pdf> (accessed 17 November 2013), 1.
24. Michael K. Sahadi Keeping JSOC a Secret: The Exposure of Special Warfare and its Adverse Effects on National Security and Defense to the United States. 2013 Military Legitimacy Review. <http://militarylegitimacyreview.com/wp-content/uploads/2013/05/KEEPING-JSOC-A-SECRET.pdf> (accessed 12 January 2014), 1-36.

25. Edward Wong. "Hackers Find China Is Land of Opportunity." *The New York Times*, 22 May 2013. http://www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html?_r=1& (accessed 1 December 2013), 1-4.

26. Joshua Kopstein. "How the NSA Recruits in a Post-Snowden World." *The Daily Beast*, 17 January 2014. <http://www.thedailybeast.com/articles/2014/01/17/how-the-nsa-recruits-in-a-post-snowden-world.html> (accessed 21 January 2014), 2.

27. Misha Glenny. "Hire the Hackers!" *TED Global 2011/TED Talk*, July 2011. Audio/video presentation. http://www.ted.com/talks/misha_glenny_hire_the_hackers.html (accessed 13 November 2013).

28. Tiffany Smith. "In Pursuit of an Aptitude Test for Potential Cyberspace Warriors." *AFIT/GIR/ENG/07-01*, Student Thesis. <http://www.hsdl.org/?view&did=479420> (accessed 19 November 2013).