REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
03/17/2016	Master's of Military Studies	SEP 2015 - MAR 2016

4. TITLE AND SUBTITLE
Cyber Fluency for US Special Operations Forces: Maximizing Domain Understanding through Cyber Force Protection

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Sarson, Erik J., Major, USA

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
Dr. Matthew Flynn

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT
US Special Operations Forces (USSOF) will increasingly face adversary cyber capabilities that threaten the security of information, operations, and individuals. By training all of its operators in the basics of cyber force protection and allowing them to train their Global SOF Network partners, US Special Operations Command can best develop, apply, and retain cyber skills throughout the organization while maximizing the ability to operate unimpeded in the cyber domain.

15. SUBJECT TERMS
Cyber; Force Protection; Special Operations Forces, SOF; Cyber Fluency; Cyber Force Protection; Cyber Threat; Global SOF Network; Special Operations Command, SOCOM; Special Forces, SF; Security Cooperation; Internet of Things, IoT; Maker Movement

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
					19b. TELEPHONE NUMBER *(Include area code)*
Unclass	Unclass	Unclass	UU	49	(703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

CYBER FLUENCY FOR US SPECIAL OPERATIONS FORCES: MAXIMIZING DOMAIN UNDERSTANDING THROUGH CYBER FORCE PROTECTION

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

MAJOR ERIK SARSON

AY 15-16

Mentor and Oral Defense Committee Member: MATTHEW FLYNN
Approved: 3/16/16
Date: 3/17/16

Oral Defense Committee Member: J.W. Gordon
Approved:
Date: 3/17/16

JAMES M. MIS
COL, SF
3/17/16

Executive Summary

Title: Cyber Fluency for US Special Operations Forces: Maximizing Domain Understanding through Cyber Force Protection

Author: Major Erik Sarson, United States Army

Thesis: US Special Operations Forces (USSOF) will increasingly face adversary cyber capabilities that threaten the security of information, operations, and individuals. By training all of its operators in the basics of cyber force protection and allowing them to train their Global SOF Network partners, US Special Operations Command can best develop, apply, and retain cyber skills throughout the organization while maximizing the ability to operate unimpeded in the cyber domain.

Discussion: Given the growing prevalence of cyber actions in military conflict and international relations, it is evident that special operations forces (SOF) will face increasing threats in the cyber domain. The global ubiquity of networked devices compounds these threats, and the number of such devices continues to multiply exponentially as technology improves, costs decrease, and consumer demand increases. These political, social, and economic developments are shaping the environment in which SOF must operate: an environment that overlaps increasingly with the cyber domain. SOF are also unique within the military due to their persistent engagement in security cooperation missions worldwide. Limited communications support during these missions means that SOF cannot rely upon well-protected, static Department of Defense networks. Rather, they must adapt with ad-hoc setups augmented by commercial, off-the-shelf equipment, which can vary from mission to mission.

US Special Operations Command can best adapt to this changing environment by training all of its SOF in cyber force protection. This training would provide SOF with a foundational understanding of underlying technologies. It would also offer instruction on the technical specifics and best practices related to hardware, software, and social media. Finally, it would explain how hackers conduct basic exploits, and how to avoid these both technically and socially.

Conclusion: Despite growing threats in the cyber domain, USSOF have the ability to respond with resolve. This effort starts with training all SOF in cyber force protection. This will help mitigate cyber threats to tactical special operations teams working to achieve operational or strategic effects. These teams can then train the Global SOF Network to protect itself in the cyber domain, further preventing adversaries across the globe from gaining an upper-hand in operations or intelligence.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Table of Contents

Preface

When I participated in the 2003 NSA/CSS (National Security Agency/Central Security Service) Cyber Defense Exercise as a cadet at West Point, I admit that I did not fully perceive the impact that cyber threats would have on military operations or the civilian sector. It is now abundantly clear just how serious these threats can be thanks to events such as Stuxnet, the Sony hack, and the OPM hack, among many others. With everyone from President Obama through service-level special operations commands calling for cyber capabilities, there is a need for thoughtful discourse on what actions we should take as special operators. As a Special Forces officer with a computer science education and experience in the commercial information technology sector, I am seeking to add new insight to this discussion.

There has been much debate over the role of the military in cyberspace, but little over the role of special operations forces (SOF). In politically and legally sensitive environments, such as limited and proxy wars, SOF have historically been the force of choice. Because of its primarily civilian use, cyberspace similarly qualifies as a sensitive environment, and SOF are likely have an important function therein. Perhaps more importantly, because of their constant work in foreign countries, SOF will encounter evolving cyber threats from various states, non-state actors, and criminals on a continual basis.

Thank you to Dr. Matthew Flynn, Colonel James Mis, and Colonel (retired) Gary Brown for providing relevant guidance and timely feedback. Thank you to Andrea Hamlen from the Leadership Communication Skills Center, and my wife, Christina Sarson, for helping me edit. Finally, I would like to especially thank Colonel Patrick Duggan for helping me narrow my focus to the important but somewhat overlooked topic of cyber force protection.

Introduction

In an increasingly complex geopolitical environment, the United States faces a growing number of adversaries that pose unprecedented threats in the cyber domain. Countries such as China, Russia, North Korea, and Iran have developed and employed cyber capabilities that challenge US interests at home and abroad.[1] These states take advantage of relative cyber anonymity,[2] well-established precedents for international espionage,[3] and a lack of international agreement on laws governing the use of force in cyberspace in order to achieve their objectives through the cyber domain,[4] often without provoking a military confrontation.[5] Non-state actors such as the so-called Islamic State in Iraq and Syria (ISIS) and criminal organizations have also utilized cyber means to adversely influence Western populations and steal valuable information.[6] In response, the United States is working to better secure its networks across government agencies, critical infrastructure, and the civilian sector, as well as developing cooperative cyber security with international partners. The US government has additionally charged the military with developing the ability to conduct both defensive and offensive actions in the cyber domain. The United States Cyber Command (USCYBERCOM/CYBERCOM) has taken the lead in this effort.

At the forefront of irregular, low intensity, and politically sensitive threats to the country's interests, US Special Operations Forces (USSOF) will have to quickly adapt in order to face their adversaries in the cyber domain and maintain an advantage therein. The United States Special Operations Command (USSOCOM/SOCOM) has actively worked with CYBERCOM to integrate cyber capabilities into its formations, and is developing cyber training for its own operators. SOCOM is also working to develop the *Global SOF Network*, which includes US interagency elements and international partners networked worldwide to prevent conflict and

provide rapid response to emerging security threats.[7] With its diverse regional and technical expertise, the Global SOF Network can help give USSOF an edge in the cyber domain.

There are different capabilities that special operations forces (SOF) might pursue in the cyber domain, including cyber intelligence operations, cyber information operations, offensive cyber operations, and cyber force protection. This paper discusses some of the proposals that other authors have put forth for these different categories and further explores the category of cyber force protection. While there are advantages that SOF might gain from developing each of these capabilities, cyber force protection will be the easiest to train, have the broadest application across SOF, and set the foundation for the development of other cyber capabilities.

US Special Operations Forces will increasingly face adversary cyber capabilities that threaten the security of information, operations, and individuals. By training all of its operators in the basics of cyber force protection and allowing them to train their Global SOF Network partners, SOCOM can best develop, apply, and retain cyber skills throughout the organization while maximizing the ability to operate unimpeded in the cyber domain.

Background and Literature Review

The United States, the US military, and the US Department of Defense have articulated the need for cyber capabilities. The 2015 US *National Security Strategy* highlights the growing threat of disruptive and potentially destructive cyber espionage and attacks, calling for a coordinated effort to secure cyberspace by investing in capabilities and working cooperatively across sectors of the government and private industry.[8] The 2015 *National Military Strategy* reinforces this guidance and outlines some specific cyber threats from states such as North Korea, and non-state actors such as violent extremist organizations. This document also calls for

greater joint information system interoperability to facilitate cyber security between services, better protection of physical infrastructure tied to cyberspace, the ability to counter enemy cyber attacks, and a focused effort to work with Asian partners to improve their cyber security.[9] The 2015 *DoD Cyber Strategy* further details how the Department of Defense plans to create cyber forces, better defend its networks and homeland infrastructure, develop "cyber options" that it can employ during all stages of conflict, and cooperate with international partners to enhance collective cyber security.[10]

USSOF have also stressed the importance of cyber capabilities. US Special Operations Command's (SOCOM's) strategic vision, *SOCOM 2020*, notes that SOF must take advantage of the cyber domain to help counter growing asymmetric threats.[11] SOCOM's *SOF Operating Concept* further mentions that all SOF elements will have cyber "enablers" at the tactical level by 2020,[12] and that SOF have relied upon, and will increasingly rely upon, the support and integration of national-level cyber capabilities down to the team level.[i] The SOF Operating Concept also recognizes opportunities that cyberspace creates for SOF, such as new ways to communicate with and influence people who might be in areas difficult to access by other means.[13] At the service SOF level, the US Army Special Operations Command (USASOC) published *ARSOF Next*, which states that USASOC is developing multi-level cyber training for SOF, coordinating efforts with US Cyber Command (CYBERCOM), and working toward an overall goal of "normalizing" SOF operations in the cyber domain.[14]

It is clear that guidance and efforts from the national level to the service SOF level point toward a pursuit of cyber capabilities, but what is it that SOF should be doing in cyberspace? Multiple authors have sought to answer this question.

[i] Teams are the smallest tactical formation of SOF, and can vary in size from a few individuals to 12 or more.

Jon Lindsay discusses SOCOM's embrace of technology in recent conflicts, highlighting how SOF have combined both human and technical intelligence to improve counterterrorism operations. Utilizing capabilities such as unmanned aerial vehicles, satellites, and signals intelligence, SOF have been able to locate human targets with unprecedented speed and accuracy.[15] Although Lindsay does not specifically mention cyber capabilities, SOCOM's comfort with leveraging technology suggests that cyber could be a natural addition for the organization.

Jeffry Edgar argues that SOF are "enablers, not cyber warriors" in cyberspace.[16] He says that "information warfare" (sic) should not be a primary SOF mission, but rather a secondary one because it is something that conventional military units also do.[17] Only under certain circumstances would it be preferable for SOF to conduct cyber operations in place of a conventional unit, and even in these circumstances SOF would play a limited technical role. According to Edgar, SOF offer exclusive close access to targets, as well as regional and language expertise that can facilitate cyber operations. But he finds it hard to picture a SOF operator sitting behind a computer for extended periods, and he argues that it would be too difficult to teach SOF to be experts in cyber due to their already expansive training requirements. However, Edgar recognizes that SOF must be knowledgeable of cyber operations because of the unique circumstances of their missions, which they may have to convey to non-SOF cyber elements supporting such missions. He also acknowledges that cyber operations can enhance special operations, using the example of a "computer network attack" (sic) to facilitate SOF operations behind enemy lines by denying an adversary communication and surveillance capabilities.[18]

Matthew Nordmoe takes a more liberal view, arguing that SOF must actively pursue cyber capabilities in order to take advantage of latent enhancements that they can bring to

operations and intelligence. Nordmoe focuses on SOF conducting cyber-augmented unconventional warfare (UW).[ii] He says that SOF may use the cyber domain, and specifically social media, in the *preparation* phase of UW to better understand the population, enemy, resistance movement, and overall environment.[iii] This enhanced understanding will allow the United States to better evaluate the potential for a successful resistance movement. Beyond this, SOF may conduct cyber information operations (IO) to influence target audiences in the operational area, helping to set the conditions for US assistance. In the *initial contact* phase, SOF and resistance movement leadership may conduct their first rendezvous in the cyber domain as opposed to a physical meeting, reducing risk. Nordmoe goes on to describe how cyber operations enable the *organization* and *buildup* phases of UW. His examples include online training videos to improve the capabilities of the resistance movement, social media recruitment and crowd funding to grow the organization, and cyber IO to build popular support. Finally, in the *employment* phase of UW, resistance forces would conduct cyber attacks against enemy targets in cyberspace.[19]

Patrick Duggan discusses even broader ways in which SOF could potentially utilize cyber capabilities. He compares USSOF to their counterparts in two adversary nations, arguing that Russia and Iran have "successfully employed cyber-enabled special warfare as a strategic tool to accomplish their national objectives,"[20] while the United States has paid insufficient attention to

---

[ii] US Joint Chiefs of Staff, *Special Operations*, Joint Publication 3-05, Washington, D.C.: Joint Staff, July 16, 2014, http://www.dtic.mil/doctrine/new_pubs/jp3_05.pdf, xi. "*Unconventional warfare* consists of operations and activities that are conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerilla force in a denied area."

[iii] Headquarters, Department of the Army, *Unconventional Warfare*, Army Techniques Publication No. 3-05.1, Washington, D.C.: Department of the Army, September 6, 2013. https://armypubs.us.army.mil/doctrine/DR_pubs/dr_c/pdf/atp3_05x1.pdf, 2-8 – 2-16. The *seven phases of unconventional warfare* are preparation, initial contact, infiltration, organization, buildup, employment, and transition.

similar means. He explains that the *Spetsnaz* and *Quds Force* employ cyber capabilities at the tactical level, complementing their nations' strategic-level capabilities, and that Russian and Iranian SOF conduct these cyber operations through proxy forces in order to minimize attribution. Duggan acknowledges the important intelligence, IO, and offensive enhancements that cyber operations can offer in support of special operations. And, he adds that "cyber-enabled special warfare could both deter conflict and be applied throughout the spectrum of conflict."[21]

Duggan presents three specific cyber-related capabilities that USSOF could pursue to their advantage: "cloud-powered foreign internal defense (FID),"[iv] "counternetwork COIN (CNCOIN),"[v] and "cyber UW pilot teams."[vi,22] Cloud-powered FID, while not specifically defined, would consist of information and analysis resources maintained on cloud-based networks and shared between USSOF, US interagency partners, and foreign partners for the purpose of better understanding the factors driving conflict in specific areas. Duggan argues that this concept would "save money, time, and manpower" compared to traditional information gathering and planning in support of FID, and that it would help to build trust between SOF and their partners.[23] CNCOIN would maximize the effectiveness of both IO and intelligence in combatting insurgencies. One CNCOIN method would entail proxy (host-nation government and

---

[iv] US Joint Chiefs of Staff, *Foreign Internal Defense*, Joint Publication 3-22, Washington, D.C.: Joint Staff, July 12, 2010, http://www.dtic.mil/doctrine/new_pubs/jp3_22.pdf , I-1. "*FID* is the participation by civilian and military agencies of a government in any of the action programs taken by another government or other designated organization, to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to their security."

[v] US Joint Chiefs of Staff, *Special Operations*, II-12. "*COIN* [Counterinsurgency] is a comprehensive civilian and military effort designed to simultaneously defeat and contain insurgency and address its root causes."

[vi] Headquarters, Department of the Army, *Unconventional Warfare*, 2-9. "A *pilot team* is a deliberately structured composite organization comprised of Special Forces operational detachment members, with likely augmentation by interagency or other skilled personnel, designed to infiltrate a designated area to conduct sensitive preparation of the environment activities and assess the potential to conduct unconventional warfare in support of U.S. objectives."

ex-guerilla) elements infiltrating insurgent social media and computer networks to gather intelligence for exploitation, "herd" network members to specific virtual locations for easier tracking, and manipulate communications between insurgents to sow confusion and mistrust. A second CNCOIN tactic utilizing social media would be to "crowdsource" intelligence regarding insurgent activity.[24] Third, CNCOIN forces could use social media personas to discredit insurgent leaders and groups. Finally, Duggan's cyber UW pilot teams would accomplish what Matt Nordmoe also outlined in the initial contact phase of cyber-supported UW: a virtual link-up between SOF and resistance leadership that reduces risk while saving time and resources.[25]

Common among most existing literature regarding the relationship between SOF and cyber is a focus on offensive, intelligence, or influence-related cyber operations, but there has been little discussion of defensive or protective cyber measures that might be unique to SOF.[26] This paper seeks to help fill that gap by addressing the intersection of SOF and cyber force protection specifically.

Force Protection, Cyber, and SOF

US joint doctrine defines force protection as "measures taken to prevent or mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information."[27] Measures within force protection include those relating to physical security such as armor, barriers, locks, and guards, as well as those relating to information security such as policies and procedures to prevent the disclosure of sensitive or classified information.[28]

In the cyber domain, force protection must encompass not only infrastructure such as devices and their connecting media, but also the electromagnetic spectrum, content, and the

interactions between users and all of these elements.[29] Thus, cyber force protection may be defined as *measures taken to prevent or mitigate hostile actions against information technology systems and their associated users, data, and communications media, upon which DOD relies*.[vii] The U.S military can enhance cyber force protection by physically securing systems, protecting data, reducing and obfuscating electronic signatures, ensuring that personnel interact properly with systems, and being prepared for contingencies. Some specific means to achieve these goals are the use of strong *authentication*, *access control*, *encryption*, *tunneling*, *proxy servers*, data backups, physical security, and standby, low-technology methods.[viii]

Adversaries can threaten US military forces in the cyber domain in several ways. Any computerized system the US military uses is potentially vulnerable to cyber threats, and an adversary's goals in exploiting a particular system may include gathering intelligence, altering or inserting information for psychological effect, denying a capability, sabotaging a system, or actually causing physical harm.[30] For an adversary to exploit a system, he needs either virtual access via a network or physical access through direct manipulation or inserted media capable of

[vii] Author's definition, italics added for emphasis.

[viii] Matt Walker, *CEH Certified Ethical Hacker All-in-One Exam Guide,* Second Edition, McGraw Hill: New York, 2014, 387. *Authentication* is "the process of determining whether a network entity (user or service) is legitimate–usually accomplished through a user ID and password. Authentication measures are categorized by something you know (user ID and password), something you have (smart card or token), or something you are (biometrics).";

Richard R. Brooks, *Computer and Network Security: Navigating Shades of Gray*, Boca Raton, FL: CRC Press, 2014, 71. *Access control* is a "security attribute for limiting and controlling access to information.";

Walker, *CEH*, 393. *Encryption* is the "conversion of plain text to cipher text through the use of a cryptographic algorithm.";

Ibid, 412. *Tunneling* is "transmitting one protocol encapsulated inside another protocol.";

Ibid, 404. A *proxy server* is "a device set up to send a response on behalf of an end node to the requesting host. Proxies are generally used to obfuscate the host from the Internet."

infecting the system with *malware*.[ix] He also needs the technical abilities, and often malware, that allow him to achieve his desired objectives after gaining access. Hackers overcome the challenge of access by exploiting software or hardware vulnerabilities, human errors in system configuration, human-computer interaction weaknesses, or people's inherent trust of others.[31] The common theme among all of these methods is the fallibility of humans who make, configure, and interact with computer systems. Thus, solutions to deal with cyber threats must start with properly educating and training the people who setup, maintain, and use information systems.

Cyber force protection is a concern for all military forces, but it is especially vital for SOF due to their continuous execution of security cooperation (SC) missions worldwide.[x] SOF must consider force protection in general across a broad range of mission types that includes foreign internal defense (FID) and security force assistance (SFA), along with ten other types.[xi] While cyber force protection can apply to all twelve of these SOF mission types, this paper focuses on SC, which encompasses both FID and SFA.[32] Security cooperation includes training engagements and other interactions to build the capabilities of foreign military forces, as well as

---

[ix] Ibid., 400. *Malware* is "a program or piece of code inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system. Malware consists of viruses, worms, and other malicious code."

[x] US Joint Chiefs of Staff, *Foreign Internal Defense*, I-10. JP 3-22 defines *security cooperation* as "all DOD interactions with foreign defense establishments to build defense relationships that promote specific US security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide US forces with peacetime and contingency access to a host nation."

[xi] US Joint Chiefs of Staff, *Special Operations*, II-10 – II-12. While similar, the distinction between FID and SFA lies in their objectives. In FID, the goal is for the partner nation military to be able to prevent and react to extant state-internal threats, while the objective of SFA is a capability to react to both internal and external threats, and to be able to serve as part of an expeditionary multinational force;
US Joint Chiefs of Staff, *Special Operations*, II-3. The remaining SOF missions are direct action (DA), special reconnaissance (SR), countering weapons of mass destruction (CWMD), counterterrorism (CT), unconventional warfare (UW), hostage rescue and recovery, counterinsurgency (COIN), foreign humanitarian assistance, military information support operations (MISO), civil affairs operations (CAO).

interoperability, trust, and enduring relationships between forces. In executing SC, SOF train, advise, and interact with partner nation military forces, usually within the partner nation's borders. These types of missions are especially important when considering cyber force protection because they have greater frequency and continuity than most others, many of which occur only during significant conflict escalation, or are exclusively executed by specific units that do not represent a majority of the SOF community. More SOF units and personnel engage in SC than the other mission types on a consistent basis.[33] Thus, SC will likely be the primary situation in which SOF will encounter cyber threats.

Cyber threats to SOF exist in SC missions, even when the security situation is fully under the control of the host nation government. These threats can come from foreign intelligence entities, active or latent insurgencies, criminal organizations, or terrorist groups.[xii] Threat elements may exploit USSOF systems for a variety of reasons including intelligence, harassment, profit, blackmail, and sabotage. The systems that these elements are likely to target are laptops and other personal electronic devices that SOF rely heavily upon for planning and communication during such missions.[34] For example, a foreign intelligence service may hack into a SOF laptop via a WiFi network, acquire documents describing training for partner nation forces, and provide this information to its government. A criminal organization may exploit a SOF smart phone and steal personal information that it could subsequently sell on the black market or use to blackmail individuals. A terrorist group could gain access to a GPS-enabled tablet and have it report the location of SOF elements in order to facilitate an ambush.

[xii] US Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, Washington, D.C.: Joint Staff, November 8, 2010 (as amended through November 15, 2015), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, 94. *Foreign Intelligence Entities* are "any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire US information, block or impair US intelligence collection, influence US policy, or disrupts US systems and programs. The term includes foreign intelligence and security services and international terrorists."

The Growing Threat

The worldwide trend of states progressively adopting cyber capabilities suggests a growing cyber threat for SOF. Countries such as Russia and China have taken well-publicized strides to advance these capabilities. US officials consider Russia the most advanced potential adversary in cyberspace, and it is the first state to combine cyber attacks with physical ones as it did in both Georgia (2008) and the Ukraine (2014).[35] China has also incorporated cyber operations into its military, with separate departments of the People's Liberation Army dedicated to offensive cyber operations and cyber intelligence.[36] Additionally, both Russia and China have conducted significant cyber espionage against state targets to collect information that might give them political or economic advantages. [37] The most publicized example of this activity is the Office of Personnel Management hack, where the Chinese government allegedly stole the personal information of more than 21 million current and former US federal employees.[38] Iran has also joined the ranks of significantly cyber-capable states, investing billions of dollars in both offensive and defensive cyber capabilities since 2009. Like other malicious cyber actors, Iran particularly sees offensive cyber capabilities as an important asymmetric counter to adversaries with greater relative military strength. Furthermore, Iran has extended its use of proxy forces to the cyber domain by training both the Syrian Electronic Army and elements of Hezbollah. Attacks by these proxies and their Iranian backers have grown increasingly sophisticated and have targeted US and Israeli civilian infrastructure, as well as military networks. [39] With their investment in cyber capabilities, states' militaries, intelligence services, and proxies have gained a relatively inexpensive means to target SOF for intelligence collection, blackmail, or attack. They can do so with a low cost in terms of money, time, physical threat, and attribution.

Non-state actors, including terrorist groups and criminal organizations, have also increasingly relied upon cyber means to achieve their goals, and will challenge SOF operations through the cyber domain. For its part, ISIS has been steadily improving its ability to conduct cyber attacks, performing a denial-of-service attack on a French TV news station, hacking social media accounts of the US Central Command, and conducting other cyber attacks against both organizations and individuals.[40] In the future, terrorist organizations may effectively target SOF in the cyber domain, even within the relative security of places like Western Europe, in order to gather intelligence or conduct surveillance that supports high-visibility physical attack. Such an act could provide the group with a media win that sows fear in Western society, attracts more terrorist recruits, and perhaps causes international partners to question the value of their relationship with USSOF. The rise of international cyber crime will also affect SOF.[41] The links between criminal organizations and other adversaries are cause for concern, as adversaries may draw upon cyber criminals' experience in order to exploit SOF cyber weaknesses.[42] Even where this link is not present, opportunist criminals may target SOF just as they would any other group or individual, especially if they perceive a potential market for whatever unique information they are able to capture.

Broader technological, social, and economic trends are also increasing the cyber threat to SOF. As broadband and mobile Internet connectivity continues to spread to more places, and more people connect more devices, opportunities for hackers grow.[43] These opportunities are also taking new forms as people increasingly connect different types of devices that have not traditionally been on the Internet.[44] This is the *Internet of Things* (IoT), where cars, surveillance cameras, climate control systems, and just about any other device that a person might want to monitor, access, or control is connected. Smart phones are an example of the utility gained in

connecting a non-traditional computing device to the Internet. The average American cell phone user in 1995 would not have predicted that his 2016 counterpart would be using a cell phone for emailing, searching the Internet, and instantly connecting with vast social networks. Beyond this, connected cars now allow drivers to monitor and control their automobiles over the Internet via mobile applications, while allowing manufacturers to track real-time performance and maintenance data.[45] Connected surveillance cameras also allow home and business owners to monitor the security of their premises from anywhere in the world.

While potentially useful in many ways, the IoT also presents a threat for SOF because of its inherent lack of security, and because of its various possibilities for surveillance.[46] Manufacturers in many different industries are rushing to build and market products that will live on the IoT, but in order to get products to market quickly and make a profit, most manufacturers have paid little attention to the network security of their new devices. Where companies have included security features, they are often rudimentary and not difficult to crack.[47] Ease of monitoring from anywhere in the world, mixed with a lack of security, also means that there are new opportunities for adversaries to conduct surveillance of SOF. As these devices proliferate throughout the world, SOF will inevitably encounter them when deployed, and possibly even bring IoT devices themselves. Threat elements can focus on the weak security of these devices and take advantage of them to break into a network, redirect cyber attacks through an IoT device, monitor SOF, or steal information.

A related trend that could negatively affect the cyber security of SOF is what is known as the *Maker Movement*. In various communities of interest throughout the world, people are increasingly making physical items and devices themselves rather than relying upon manufacturers.[48] Disruptive technological innovations such as three-dimensional printers, a wide

variety of advanced sensors, and inexpensive microcontrollers that users can program through open-source software have made this possible.[49] *Makerspaces*, or places with the requisite equipment where people can gather to make things, such as public universities and private organizations like *TechShop*, have made it economically feasible.[50] International corporations have stretched their supply chains to drastic scales, making it harder for them to provide meaningful variety or add value to products. Meanwhile, the ways that people are able to work in an increasingly digital and networked age have broadened. Under these conditions, and with access to the technology and the tools, individuals will increasingly add aftermarket value to products or create their own. A 2013 study by Deloitte goes as far as predicting that this will lead to drastic changes in the production economy and the way people are employed: where individuals and small manufacturing operations play a much bigger role in a market with growing diversity, while larger companies limit themselves to economies of scale enabled by robotics.[51]

The Maker Movement presents the possibility of an infinite number of unique and potentially vulnerable devices on the IoT, as well as new ways for adversaries to conduct discreet technical surveillance of SOF. Of the people actively making things, or *makers*, more than half of them are creating hardware with integrated microcontrollers like *Arduino* that are available for less than $50 and programmable with open-source software.[52] These microcontrollers have the ability to connect to the Internet, drastically increasing the diversity and number of devices that could potentially live on the IoT. An example of this is a homemade, networked security camera using Arduino, a USB webcam, and a basic motion detector, which streams captured video live to the Internet via YouTube.[53] Makers have also created various radio spectrum analyzers using Arduino.[54] Although an average person creating a computing device and networking it to the

Internet is remarkable, the average person does not possess the skills or concern necessary to ensure that this device is adequately secure in the cyber domain. Thus, just as the possibilities for creation are limitless, so are the possibilities for exploitation. The Maker Movement also allows new and innovative ways to develop technical surveillance devices that may be hidden in or amongst other innocuous-looking objects. One can imagine a networked spectrum analyzer that reports cell phone, WiFi, or other radio signal activity across the Internet, allowing a hacker to track specific devices and their associated users in a certain area. State-run intelligence organizations have historically created discreet technical surveillance devices, but as the Maker Movement grows, both state and non-state adversaries may be able to outsource such work to greater effect. Such a development might follow patterns similar to insurgents' use of homemade explosives (HME) and improvised explosive devices (IEDs) in recent conflicts.[55]

SOF will encounter cyber threats in a growing number of locations and situations when conducting SC. Potential US state adversaries, especially China and Russia, have placed a high value on continually shaping the conditions necessary for diplomatic, informational, military, and economic success before a significant conflict arises. This leads them to conduct persistent and broad intelligence gathering in the cyber domain in order to understand their adversaries' (United States' and US partners') capabilities, intentions, and bargaining positions.[56] Because of the inherent political and operational sensitivity of their missions, USSOF in a foreign country present adversary states with a unique opportunity for intelligence gathering. Thus, heightened threats will exist in countries where cyber aggressor states have specific interests and have employed cyber capabilities in support of those interests, or are likely to do so. This is particularly true for countries where cyber aggressor states have expansionist political goals, such as the Ukraine (vis-à-vis Russia); in countries that harbor perceived threats to cyber

aggressors, such as the Baltic States (Russia), India and Japan (China), and Israel (Iran); and countries that have portions of the population sympathetic to aggressor state interests, such as Pakistan (China), as well as Yemen and Lebanon (Iran).

Terrorist organizations may see SOF conducting SC as potential high-payoff targets. If terrorist hackers can effectively track SOF in the cyber domain and guide operatives to conduct a physical ambush, then they can utilize a successful attack as a recruiting tool while also challenging the integrity of international SOF partnerships. Therefore, SOF may face an increased cyber threat in countries where terrorist organizations operate, including many Middle Eastern, North African, Central Asian, South Asian, and Southeast Asian states.

Criminal organizations, acting alone or in collusion with other adversaries such as states, may also target SOF for information theft or other exploitation. Thus, countries with robust criminal organizations, such as many of those already listed as presenting potential terrorist threats, as well as some Eastern European states, will be higher cyber risk areas for SOF.

Finally, the proliferation of unsecure devices on the IoT, many of which are capable of surveillance, will also present a threat to SOF conducting SC. These devices may be either commercial or homemade, increasing the difficulty in keeping track of specific threats. When working in areas that are more technologically advanced (Europe and East Asia), and in areas that are especially dependent on wireless communication (parts of Africa and South Asia), SOF will face an increased cyber threat due to the presence of such devices.

Importance of the SOF-Cyber Link

USSOF are uniquely capable of learning and teaching cyber force protection skills due to their exceptional experience, intelligence, and adaptability. Most SOF positions require a service member to have several years of military experience prior to entry. Furthermore, most SOF positions have a selection process that thoroughly tests an individual's physical, mental, and social (leadership/followership/teamwork) capabilities, as well as their psychological suitability. These factors, paired with the limited number of SOF positions in the US military, ensure that membership is highly competitive, and that members are above the military average in most favorable traits. Once they become members of the community, SOF operators receive advanced, frequent training in order to gain, maintain, and improve these skills. From the beginning, cadre members teach SOF trainees that "humans are more important than hardware,"[57] and that they have joined a profession committed to lifelong learning. This focus on human quality is critical because special operations depend on adaptable individuals who are able to improvise and innovate in order to accomplish missions in sensitive environments. SOF must also be able to operate in small teams with little support, relying largely upon their own abilities for sustainment and survival.[58] These traits all suggest that SOF are well-suited to learn, maintain, apply, and teach cyber force protection skills.

SOF are also consistently engaged with partner nations due to regional alignment and persistent presence in embassies and other forward-deployed locations.[59] This status allows SOF to conduct security cooperation missions on a continual basis throughout the world. These missions are also part a deliberate effort to expand and strengthen the Global SOF Network in order to help prevent conflict and ensure that the United States has reliable partners when

conflict does occur.[60] Due to this continual overseas engagement, SOF will encounter an increasing cyber threat with damaging consequences.

Since SOF have the ability to learn and retain advanced skills, and are frequently deployed in an environment where they will face frequent cyber threats, they should be armed with cyber force protection capabilities. These capabilities will enable SOF to better protect their systems, their information, and themselves. Beyond this, SOF will have the opportunity to practice their skills by teaching them to partners in the Global SOF Network.

USSOF should train their international partners in cyber force protection in order to hone their own abilities, and to enhance those of their partners. With a growing cyber threat, partner SOF are just as likely as USSOF to face cyber attacks. In many cases, partner SOF may be significantly more exposed to these threats than their US counterparts. This is especially true of countries dealing with domestic insurgencies, conflicts with other nations, or ongoing terrorist attacks. These countries, such as Iraq, Afghanistan, the Philippines, and Ukraine, receive a large share of USSOF security cooperation attention. More stable SOF partners, such as the NATO states, are likely to work alongside USSOF in future conflict escalations worldwide. In this situation, it is in the best interest of USSOF for their partners to share a common level of cyber force protection in order to mitigate the negative effects of a cyber attack that could threaten a common mission or potentially allow threats access to US systems via compromised partner networks.[61] Additionally, combatant commanders employ USSOF across the range of military operations and throughout all phases of conflict, including during steady-state activities that seek to strengthen security and prevent conflict.[62] This broad-ranging employment increases USSOF and their partners' exposure to cyber threats in comparison to conventional military forces.

A Focus on Cyber Force Protection

Current efforts to institute cyber force protection in DOD are insufficient for SOF operating abroad. DOD Directive 8140.01 mandates that all military and civilian members conduct initial and annual information assurance training.[63] Subsequent implementation of this policy has yielded what is currently known as the "DoD Cyber Awareness Challenge," an interactive, online training course that teaches participants about creating passwords, properly using removable media, properly using social media, avoiding phishing scams, and other baseline skills.[64] It takes a participant one to two hours to complete this training. While this is valuable for the overall force, especially for those operating on static government systems, it is not enough to ensure proper cyber protection for SOF operators and teams who rely upon flexible, ad-hoc combinations of civilian and government technologies to communicate while deployed.

SOF require flexibility in their communication systems because they usually deploy in small teams that are unable to take large equipment packages, and because they must operate and share certain information with their host nation partners who do not utilize the same systems and networks. Thus, SOF cannot rely solely upon US government systems for effective communication. Instead, to operate in an environment where they have minimal equipment and must share information with dissimilar partners, SOF do what they are trained to do: they adapt and develop creative solutions. This often means utilizing commercial, off-the-shelf (COTS) technologies, to include laptops, smart phones, WiFi routers, and other various devices.

The downside of utilizing networked COTS devices is that each presents cyber vulnerabilities. Such devices rarely have significant security features implemented by default. For example, out-of-the-box laptops do not require a password to login, and unless a user hides

them, most router SSIDs are available for anyone to view and target. This lack of security is due to the fact that companies develop COTS devices with ease of use as a top priority. Without human intervention to improve security, hackers can easily gain access to a network through these weak nodes. SOF are also likely to conduct personal business over the Internet on COTS devices, to include communicating with family members through video chat, voice over IP, social media, and email. Each of these various programs, websites, and technologies offer different opportunities for hackers to exploit. Because the United States does not maintain hardened government networks in most of the places where SOF conducts SC, SOF must either build a network themselves with COTS devices or connect to an existing foreign network. Thus, the government network security features that most users take for granted, such as encryption, firewalls, software patching, virus scanning, and others, will not necessarily be present without additional effort. The DOD Cyber Security Challenge does not prepare users to understand the basics of underlying technologies; nor does it prepare them to sufficiently secure systems and small networks. Further effort is needed to prepare SOF to deal with these challenges.

SOF must understand the basics of information and networking technology, and they must be able to implement an acceptable level of security on COTS devices and networks. With baseline knowledge of networking, software, and hardware, operators will be armed with the language and framework to comprehend how networked information technology systems operate. By learning the security features of common laptops, smart phones, routers, and other devices they will be able to harden and protect systems from attack. With exposure to other security measures such as encryption, tunneling, and redirection SOF will be capable of communicating over networks with greater confidence that their information will not be vulnerable to adversaries. Additionally, by understanding how hackers exploit people and

systems, operators can better identify and stop hacking and *social engineering* attempts.[xiii] These skills are critical to ensure that SOF are familiar with the nature of the threat and can protect their systems, their information, and themselves from malicious cyber actors.

The Way Ahead

A solution to achieve common cyber force protection skills across SOF focuses first on training. All new SOF operators should receive a course on cyber force protection as part of their initial training. This concept is similar to language instruction, which most SOF also receive during initial training, but with much less time and money invested. While language training can last up to six months, basic cyber force protection training can occur in a much shorter timeframe. For example, the author attended a two day, hands-on course in 2015 that gave students a basic understanding of networking, and the ability to protect themselves when using personal electronic devices.[65] This short block of instruction was much more engaging and effective than the DOD Cyber Awareness Challenge, and it applied more directly to SOF and their unique missions. A cyber force protection training program may run longer, but it need not approach the average length of language training in order to accomplish its goals.

An effective training program would focus on underlying technologies, best practices, advanced security techniques, and common exploitation methods to be aware of. The course would teach students the basics of networking technologies, including the *Open Systems Interconnection (OSI) model*, *static* and *dynamic addressing*, *subnets*, the *domain name system*

[xiii] Walker, *CEH*, 410. *Social Engineering* is "a non-technical method of hacking. Social engineering is the art of manipulating people, whether in person (human-based) or via computing methods (computer-based), into providing sensitive information."

(DNS), *routing*, wired media, and wireless technologies.[xiv] Instructors would reinforce this knowledge by having students set up small networks with wireless routers, laptops, and smart phones. The course would then cover best security practices for hardware, software, and social media. Hardware security measures would include *device selection*, *configuration*, and *signal management*.[xv] Software security measures would include the use of *patching*, *firewalls*, *anti-viruses*, *intrusion detection systems*, *web browser configuration*, and *self-auditing*.[xvi] Social media security measures would include *two-factor authentication* and implementation of *select privacy features*.[xvii] Instruction on advanced security measures such as *encryption*, *tunneling*, and the *proxy servers* would provide students with the means to further protect the privacy,

[xiv] The *OSI model* is a concept for visualizing networks and their devices in seven layers. TCP/IP (transmission control protocol/Internet protocol) utilizes both *static and dynamic addresses* that consist of four numbers separated by dots (ie. 192.168.0.1). Public static addresses are owned by entities, can be associated with a *domain name* (ie. www.google.com), and do not change. Users can also define static addresses in their own networks, but often use dynamic addresses, which a router can change as needed. *Routing* is the process by which data packets travel over TCP/IP networks such as the Internet, and is done by computing devices called routers. *Subnets* are a way of allowing users to define and segregate networks. *DNS* servers store domain names and their associated static IP addresses, allowing users to connect to a specific site (ie. www.google.com) without knowing the site's IP address.

[xv] Proper *device selection* entails understanding supply-chain threats as well as the pros and cons of a device's security and performance features. Devices usually have security features that can be *configured* through the user interface. An example would be turning off the service set identifier (SSID) broadcast on a WiFi router. *Signal management* includes using specific technologies only when necessary to communicate, and limiting the intensity (amplitude) of associated wireless signals.

[xvi] *Patching* is the practice of regularly updating software and firmware with new releases improved for security. *Firewalls* block incoming and outgoing traffic based on different rules. *Anti-viruses* scan devices for known vulnerabilities. *Intrusion detection systems* look for and report anomalous behavior that might indicate malicious activity on a system. Users can improve *web browser* security by implementing features such as pop-up blocking and security plugins. *Self-auditing* entails activities such as reviewing computer log files and looking for abnormal behavior on a system.

[xvii] Social media sites and other web services most often employ *two-factor authentication* by sending an SMS text to the user requesting a log in. The text includes a one-time use pass code that the user must enter in addition to their normal user name and password. Social media sites offer different *privacy features* that users can implement to improve their security. A simple example is sharing Facebook posts only with friends instead of making them public.

discreetness, and potential for attribution of their communications.[xviii] Students would implement each of these best practices and techniques on their networks in order to appreciate their purposes and effects. Lastly, instructors would expose students to common hacker exploits such as denial of service, man in the middle attacks, backdoors, and social engineering approaches in order to give students an appreciation for how to recognize and guard against such methods. This would all be done in an unclassified environment.[66]

To take advantage of the skills gained through training, organization and doctrine should account for the capability of cyber force protection and advise its application. As SOCOM has done with other capabilities, it may designate one of its service component commands as the proponent for cyber. This does not mean that the other service SOF elements will not participate, but simply that the designated proponent manages the program and its associated doctrine. However, this is where organizational changes should stop since SOF should not consider cyber force protection a specialized skill to be practiced by a select few, but a common capability amongst all operators. The designated proponent should also draft doctrine to describe the cyber threat environment, how it affects SOF, and how SOF can protect themselves and their partners therein. Tactics and techniques publications should also list necessary cyber force protection skills, describe how they are learned and taught, and detail how they can be applied. Regulations should account for the requisite regularity of re-training, as well as the how often the training program should be reviewed and updated.

[xviii] *Encryption* is the scrambling of a message so that it is unintelligible to a third party. There are various methods of encryption: hardware or software-based full-disk encryption, file encryption (ie. using TrueCrypt), connection encryption (ie. using a virtual private network [VPN]). See http://truecrypt.sourceforge.net/. *Tunneling* is the practice of utilizing one communications protocol within another in order to either bypass a firewall or better secure the content of a conversation. An example is hyper text transfer protocol (HTTP) tunneling. The Onion Router (TOR) is a service that helps protect the location and anonymity of users by redirecting their communications through many *proxy servers*. See https://www.torproject.org/.

Armed with these skills and the doctrine to advise their use, SOF will be able to practice and enhance their cyber force protection by training their partners in the Global SOF Network. Of course, as they do with any mission where they must train foreign forces, SOF should first evaluate a force's needs and capabilities. Not all partner forces will require the same level of training, and some may require none. Perhaps more importantly, not all partner forces will be able to understand the concepts and their application to the same degree. There may also be cases where it is not in the best interest of USSOF to share these skills with a partner force because of security concerns. Thus, not all partners will receive training, and training given to the ones that do will vary; this situation is no different from that of any other capability in which SOF train foreign forces. And while cyber force protection is important, it is unlikely to be the topic around which a SOF security cooperation training engagement focuses. Therefore, SOF should work to incorporate this training into the overarching engagement theme as much as possible. For example, a Special Forces team may spend three days of a one-month urban warfare training engagement teaching their counterparts the basics, and then may test the partner force's application of what they have learned in a culminating exercise to raid a building in an urban environment.

By training all USSOF operators in cyber force protection, designating a responsible proponent, creating a doctrinal framework, and allowing SOF to train their partners in the Global SOF Network, SOCOM can best develop, apply, and retain cyber skills throughout the organization. Since every individual SOF operator is affected by cyber threats, it follows that each should have a baseline capability in cyber force protection, just as every member of the military knows how to properly utilize a protective mask in the event of a chemical attack. The unique traits of SOF, such as high intelligence, adaptability, employment in small groups, and

frequent training engagement with foreign military partners set the conditions for cyber skill understanding, retention, and application. This protection focus does not preclude the pursuit of cyber-related offensive, intelligence, or information operations capabilities, all of which may also be useful to special operations. However, cyber force protection skills are more widely applicable and immediately relevant across the organization than these other capabilities. They are also less expensive to train in terms of both money and time involved per individual. Common cyber force protection skills will, however, help leaders identify especially-talented individuals and will enable implementation of other cyber efforts. Lastly, cyber force protection training can be done in an unclassified environment, broadening the options for where training can take place and who can participate. This is an especially important advantage when considering training for international partner forces.

Conclusion

Given the growing prevalence of cyber actions in military conflict and international relations, it is evident that SOF will face increasing threats in the cyber domain. The global ubiquity of networked devices compounds these threats, and the number of such devices continues to multiply exponentially as technology improves, costs decrease, and consumer demand increases. These political, social, and economic developments are shaping the environment in which SOF must operate: an environment that overlaps increasingly with the cyber domain. SOF are also unique within the military due to their persistent engagement in security cooperation missions worldwide. Limited communications support during these missions means that SOF cannot rely upon well-hardened, static DOD networks. Rather, they

must adapt with ad-hoc setups augmented by COTS equipment, which can vary from mission to mission.

USSOCOM can best adapt to this changing environment by training all of its SOF in cyber force protection. This training would provide SOF with a foundational understanding of underlying technologies. It would also offer instruction on the technical specifics and best practices related to hardware, software, and social media. Finally, it would explain how hackers conduct basic exploits, and how to avoid these both technically and socially.

There are several advantages to a focus on cyber force protection. First, the skill set is relevant to all SOF because they must be able to protect themselves, their information, and their systems in the cyber domain. Conversely, all SOF may not be involved in cyber intelligence, cyber information operations, or offensive cyber operations. Second, even though all SOF may not be involved in these other types of cyber activities, cyber force protection training would provide the prerequisite comprehension necessary for these more advanced pursuits. Third, this concept would require less time and money per individual than training in more advanced areas. Fourth, this training could be done in an unclassified environment, which ties into the fifth advantage: SOF could train their partners in the Global SOF Network to implement cyber force protection. By doing this, SOF would reinforce their own understanding and capabilities through teaching. Increased capabilities across the Global SOF Network would also work to better prevent conflict and mitigate negative effects to friendly forces when it does occur.

Implementation of this concept will incur monetary, temporal, and stress-related costs. Training pipelines for USSOF are already packed with a broad set of skills that operators must master before even gaining entry to operational units. Fitting cyber force protection into these pipelines will not be without challenge due to tight schedules and budgets. Also, already-stressed

trainees may have varied reactions to the addition of another requirement. More research is needed to define the exact scope of the training, how to resource it, and how to schedule it. This research should consider how these decisions might affect SOF training organizations, budgets, and trainees.

Cyber force protection training may also not be limited to SOF. The concept of formation-wide cyber force protection training for SOF is relevant because of SOF's unique circumstances, and it is possible because of SOF's unique characteristics arising from selection and career progression processes that value high intelligence and adaptability. However, conventional military forces may benefit from the same, as they will also face increasing cyber threats, even if on a less-frequent basis than SOF. Further research should explore this possibility as well.

Despite growing threats in the cyber domain, USSOF have the ability to respond with resolve. This effort starts with training all SOF in cyber force protection. This will help mitigate cyber threats to tactical special operations teams working to achieve operational or strategic effects. These teams can then train the Global SOF Network to protect itself in the cyber domain, further preventing adversaries across the globe from gaining an upper-hand in operations or intelligence.

Endnotes

[1] James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community*, Statement for the Record, Washington, D.C.: Senate Armed Services Committee, February 9, 2016, http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf, 3.

[2] Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?," *Strategic Studies Quarterly* (Fall 2010): 102-135, http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf, 111.

[3] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall 2013): 41-73, http://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136, 70;
Goodman, "Cyber Deterrence," 123.

[4] Charlie Dunlap, "Cyber Operations and the New Department of Defense Law of War Manual: Initial Impressions," Lawfare, June 15, 2015, https://www.lawfareblog.com/cyber-operations-and-new-defense-department-law-war-manual-initial-impressions.

[5] Timothy L. Thomas, "Google Confronts China's Three Warfares," *Parameters* (Summer 2010): 101-113, http://fmso.leavenworth.army.mil/documents/googleconfrontschina.pdf, 109-110.

[6] Threat Knowledge Group, *The Islamic State and Information Warfare: Defeating ISIS and the Broader Global Jihadist Movement*, Threat Knowledge Group Special Report, January 2015, http://threatknowledge.org/wp-content/uploads/2015/11/TKG-Report-ISIS-Info-Warfare.pdf, 1;
Radware, *ISIS Cyber Attacks: ERT Threat Alert*, Radware Ltd., Tel Aviv, Israel, April, 2015. https://security.radware.com/uploadedFiles/Resources_and_Content/Threat/ERT%20Threat%20Alert%20-%20ISIS%20Cyber%20Attacks.pdf, 3-4;
Roderic Broadhurst, Peter Grabosky, Mamoun Alazab, and Steve Chon, "Organizations and Cybercrime," *International Journal of Cyber Criminology* 8, no. 1 (January – June 2014): 8-15.

[7] US Special Operations Command, *United States Special Operations Command Special Operations Forces Operating Concept*, MacDill Air Force Base, FL: USSOCOM, May 2013, https://fortunascorner.files.wordpress.com/2013/05/final-low-res-sof-operating-concept-may-2013.pdf, 3.

[8] The White House, *National Security Strategy*, Washington, D.C.: The White House, February 2015, https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf, 1, 3-4, 7, 9, 12-13.

[9] US Joint Chiefs of Staff, *The National Military Strategy of the United States of America: 2015*, Washington, D.C.: Joint Staff, June 2015, http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf, 2-4, 9, 11, 16.

[10] Department of Defense, *DOD Cyber Strategy*, Washington, D.C.: Department of Defense, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, 13-15.

[11] US Special Operations Command, *United States Special Operations Command SOCOM 2020:*

Forging the Tip of the Spear, MacDill Air Force Base, FL: USSOCOM, accessed October 30, 2015, http://www.defenseinnovationmarketplace.mil/resources/SOCOM2020Strategy.pdf, 3.

[12] US Special Operations Command, *Special Operations Forces Operating Concept*, 15.

[13] Ibid, 15-17.

[14] US Army Special Operations Command, *ARSOF Next: A Return to First Principles*, Fort Bragg, NC: USASOC, accessed October 30, 2015, http://www.soc.mil/swcs/SWmag/archive/ARSOF_Next/ARSOF%20Next.pdf, 20-21.

[15] Jon R. Lindsay, "Reinventing the Revolution: Technological Visions, Counterinsurgent Criticism, and the Rise of Special Operations," *The Journal of Strategic Studies* 36, no. 3 (2013): 424, 440, 442.

[16] Jeffry L. Edgar, "The Role of Special Operations Forces in Information Warfare: Enablers, not Cyber Warriors," Master's thesis, Naval War College, Newport, RI, May 2000, http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA381914, 1.

[17] Ibid.

[18] Ibid., 1-2, 11-12, 14-15.

[19] Matthew Nordmoe, "The Ghost in the Machine: Defining Special Operations Forces in Cyberspace," Master's thesis, The College of International Security Affairs, National Defense University, Fort Bragg, NC, 2015, http://www.academia.edu/12465632/The_Ghost_in_the_Machine_Defining_Special_Operations_Forces_in_Cyberspace, 1, 80-81, 87-88, 90-92.

[20] Patrick M. Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Forces Quarterly* 79 (4th Quarter, 2015): 46-53, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79.pdf, 47.

[21] Ibid, 46-49.

[22] Ibid, 49-51.

[23] Ibid, 50.

[24] Ibid, 51.

[25] Ibid, 49-52.

[26] Patrick Duggan (US Army Special Forces officer, SOF-cyber author), phone interview by Erik Sarson, September 25, 2015.

[27] US Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, Washington, D.C.: Joint Staff, August 11, 2011, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf, III-30.

[28] Ibid, III-30 – III-35.

[29] US Joint Chiefs of Staff, *Cyberspace Operations*. Joint Publication 3-12 (R), Washington, D.C.: Joint Staff, February 5, 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf, II-12.

[30] Paulo Shakarian, Jana Shakarian, and Andrew Ruef, *Introduction to Cyber Warfare: A Multidisciplinary Approach*, Waltham, MA: Elsevier, 2013, 3.

[31] Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014, 40-45;
Richard R. Brooks, *Computer and Network Security: Navigating Shades of Gray*, Boca Raton, FL: CRC Press, 2014, 29, 247-249.

[32] Harry R. Yarger, *Building Partner Capacity*, MacDill Air Force Base: JSOU Press, February 2015. http://jsou.socom.mil/JSOU%20Publications/JSOU15-1_Yarger_BPC_FINAL.pdf, 73.

[33] US Congress, House, *Statement of General Joseph L. Votel, US Army, Commander, United States Special Operations Command before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities*, Washington, D.C.: US Congress, March 18, 2015, http://www.socom.mil/Documents/2015%20USSOCOM%20Posture%20Statement.pdf, 8;
US Special Operations Command, *Special Operations Forces Operating Concept*, 6-9.

[34] Terry Costlow, "Mobile Mashup: The Military's Proliferating Mix of Smartphones and Tablets," Defense Systems, March 23, 2015, https://defensesystems.com/articles/2015/03/23/military-unconventional-mix-smartphone-tablets.aspx;
Defense Systems Staff, "Special Forces Aiming to Lock Down Blackberry 10 Devices," Defense Systems, April 17, 2015, https://defensesystems.com/articles/2015/04/17/special-operations-blackberry-integrity-agent.aspx;
Spencer Ackerman, "Real Men Use Android: Special Forces Favor Google Phone," Wired, October 29, 2010, http://www.wired.com/2010/10/special-forces-want-android-apps-for-warzone-john-maddens/.

[35] Owen Matthews, "From Russia with Malware," *Newsweek Global* 164, no 19 (May 15, 2015): 28-29.

[36] Deepak Sharma, "China's Cyber Warfare Capability and India's Concerns," *Journal of Defence Studies* 5, no. 2 (April 2011): 64, 66, http://www.idsa.in/system/files/jds_5_2_dsharma.pdf.

[37] FireEye Labs, *APT30 and the Mechanics of a Long-Running Cyber Espionage Operation*, Milpitas, CA: FireEye, Inc., April, 2015, https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf, 3;
FireEye Labs, *APT28: A Window into Russia's Cyber Espionage Operations*. Milpitas, CA: FireEye, Inc., 2014, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf, 3.

[38] David Alexander, "The OPM Hack was a lot Worse than Previously Disclosed," The Huffington Post, September 23, 2015, http://www.huffingtonpost.com/entry/opm-hack_us_5602f64be4b08820d91b59c2.

[39] Gabi Siboni and Sami Kronenfeld, "Developments in Iranian Cyber Warfare: 2013-2014," *Military and Strategic Affairs* 6, no. 2 (August 2014): 83, 90, 95-97.

[40] Radware, *ISIS Cyber Attacks*, 2, 4.

[41] McAfee, *Net Losses: Estimating the Global Impact of Cybercrime*, McAfee, Inc., Santa Clara, CA, 2014, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf, 18.

[42] Roderic Broadhurst, Peter Grabosky, Mamoun Alazab, and Steve Chon, "Organizations and Cybercrime," *International Journal of Cyber Criminology* 8, no. 1 (January – June 2014): 15-16.

[43] Internet Society, *Global Internet Report 2015*, Internet Society, Reston, VA, 2015, http://www.internetsociety.org/globalinternetreport/assets/download/IS_web.pdf, 9, 101.

[44] Michael Covington and Rush Carskadden, "Threat Implications of the Internet of Things," in *2013 5th International Conference on Cyber Conflict*, edited by K. Podins, J. Stinissen, and M. Maybaum. Tallinn, Estonia: NATO CCD COE Publications, 2013, https://ccdcoe.org/cycon/2013/proceedings/d1r1s6_covington.pdf, 10.

[45] Telematics News, "Mercedes-Benz Offers New Range of 'Connect Me' Services," Telematics News, May 22, 2014, http://telematicsnews.info/2014/05/22/mercedes-benz-offers-new-range-of-connect-me-services_m5223/;
Nikkei Asian Review, "Toyota to Make Networked Cars Standard in Japan, US," Nikkei Asian Review, October 17, 2015, http://asia.nikkei.com/Tech-Science/Tech/Toyota-to-make-networked-cars-standard-in-Japan-US.

[46] Clapper, *Worldwide Threat Assessment*, 1.

[47] James Lyne, *Security Threat Trends 2015*, Sophos Ltd., Oxford, UK, 2014, https://www.sophos.com/en-us/threat-center/medialibrary/PDFs/other/sophos-trends-and-predictions-2015.pdf?cmp=70130000001xKqzAAE, 2;
Joshua Wright, "Hacking the Internet of Things," Army Cyber Institute Talks, National Defense University, Washington, D.C., September 22, 2015, https://www.youtube.com/watch?v=4Yh3GmrKM3w.

[48] Deloitte Center for the Edge and Maker Media, *Impact of the Maker Movement*, Maker Media Inc., San Francisco, CA, 2014, http://makermedia.com/wp-content/uploads/2014/10/impact-of-the-maker-movement.pdf, 4-6.

[49] Ray Hsu, "The World is Ours to Make: The Impact of the Maker Movement," EDN Network, February 18, 2015, http://www.edn.com/design/diy/4438686/The-world-is-ours-to-make--The-impact-of-the-maker-movement.

[50] Mark Hatch, *The Maker Movement Manifesto: Rules for Innovation in the New World of Crafters, Hackers, and Tinkerers*, New York: McGraw Hill, accessed October 30, 2015, http://www.techshop.ws/images/0071821139%20Maker%20Movement%20Manifesto%20Sample%20Chapter.pdf, 13, 33;
The White House, *Building a Nation of Makers: Universities and Colleges Pledge to Expand Opportunities to Make*, Washington, D.C.: The White House, June, 2014, https://www.whitehouse.gov/sites/default/files/microsites/ostp/building_a_nation_of_makers.pdf, 2.

[51] Deloitte Center for the Edge and Maker Media, *Impact of the Maker Movement*, 4, 6.

[52] Dale Dougherty, *Maker Market Study: An In-Depth Profile of Makers at the Forefront of Hardware Innovation*, Maker Media Inc., San Francisco, CA, 2012, http://cdn.makezine.com/make/sales/Maker-Market-Study.pdf, 13;
Adafruit, "Arduino," accessed January 22, 2016, https://www.adafruit.com/category/17.

[53] Marc-Olivier Schwartz, "Wireless Security Camera with the Arduino Yun," Adafruit, May 4, 2015, https://learn.adafruit.com/wireless-security-camera-arduino-yun/introduction.

[54] Smokeyd, "Arduino Radio Spectrum Analyzer Prototype on a Breadboard," Nurdspace, accessed January 22, 2016, https://nurdspace.nl/Arduino_Radio_Spectrum_Analyzer_prototype_on_a_breadboard;
Jesse Congdon, "Arduino Powered 2.4 GHz Spectrum Analyzer," Hackaday, July 25, 2011, http://hackaday.com/2011/07/25/arduino-powered-2-4-ghz-spectrum-analyzer/.

[55] Christina Sarson, Editorial Input, February 17, 2016. Christina offered that this problem might be similar to the IED problem in Iraq and Afghanistan.

[56] Scott D. McDonald, Brock Jones, and Jason M. Frazee, "Phase Zero: How China Exploits It, Why The United States Does Not," *Naval War College Review* 65, no. 3 (Summer 2012): 123, 125, https://www.usnwc.edu/getattachment/eef71cb7-abe7-4410-adaf-d78d085d933e/Phase-Zero--How-China-Exploits-It,-Why-the-United-;
Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*, Washington, D.C.: Institute for the Study of War, September 2015, http://understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf, 11;
Clapper, *Threat Assessment*, 3, 10.

[57] US Special Operations Command, *United States Special Operations Command Fact Book 2015*, MacDill Air Force Base, FL: USSOCOM, 2015, http://www.socom.mil/Documents/2015%20Fact%20Book.pdf, 56.

[58] US Joint Chiefs of Staff, *Special Operations*, Joint Publication 3-05, Washington, D.C.: Joint Staff, July 16, 2014, http://www.dtic.mil/doctrine/new_pubs/jp3_05.pdf, I-2, I-5;
US Special Operations Command, *Command Fact Book 2015*, 58;
US Army Special Operations Command, *ARSOF* 2022, Fort Bragg, NC: USASOC, accessed January 20, 2016, http://www.soc.mil/Assorted%20Pages/ARSOF2022_vFINAL.pdf, 18;
The author is a graduate of the Special Forces Qualification Course, and a current member of the US Army Special Forces, the largest element within the USSOF community.

[59] US Joint Chiefs of Staff, *Foreign Internal Defense*, Joint Publication 3-22, Washington, D.C.: Joint Staff, July 12, 2010, http://www.dtic.mil/doctrine/new_pubs/jp3_22.pdf, IV-16 – IV-19;
US Joint Chiefs of Staff, *Special Operations*, III-20 – III-22;
US Joint Chiefs of Staff, *Security Force Assistance*, Joint Doctrine Note 1-13, Washington, D.C.: Joint Staff, April 29, 2013, http://www.dtic.mil/doctrine/notes/jdn1_13.pdf, IV-2.

[60] US Special Operations Command, *SOCOM 2020*, 5;
Yarger, *Building Partner Capacity*, 84-86.

[61] Christina Sarson, Editorial Input, February 17, 2016. Christina pointed out that enemies could potentially gain access to US systems through partner networks.

[62] US Joint Chiefs of Staff, *Special Operations*, I-8 – I-9;
US Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*. Joint Publication 1, Washington, D.C.: Joint Staff, March 25, 2013, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf, II-4.

[63] Robert O. Work, *Cyberspace Workforce Management*, Department of Defense Directive 8140.01, Washington, D.C.: Deputy Secretary of Defense, August 11, 2015, 2. http://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf.

[64] Information Assurance Support Environment, "DoD Cyber Awareness Challenge," Defense Information Systems Agency, Fort Meade, MD, accessed February 11, 2016, http://iatraining.disa.mil/eta/cyberchallenge_v3_fy15/launchPage.htm.

[65] The author attended a two-day, contractor-led course entitled "Cyber Security & Personal Electronic Devices," sponsored by the Special Operations Detachment-Europe, at Camp Dawson WV, February 5-6, 2015.

[66] Ibid. The concept presented herein expands upon the general outline of this course.

Glossary

Access Control – "Security attribute for limiting and controlling access to information." (Brooks, *Computer and Network Security*, 71)

Authentication – "The process of determining whether a network entity (user or service) is legitimate – usually accomplished through a user ID and password. Authentication measures are categorized by something you know (user ID and password), something you have (smart card or token), or something you are (biometrics)." (Walker, *CEH*, 387)

Availability – "The condition of a resource being ready for use and accessible by authorized users." (Walker, *CEH*, 387)

Cipher Text – "An obscured version of a [plain text] message." (Brooks, *Computer and Network Security*, 76)

Computer Network Attack (CNA) – "Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves." (JP 3-13, 1998 version, I-9)
This term has been superseded by "offensive cyberspace operations (OCO)."

Confidentiality – "A security objective that ensures a resource can be accessed only by authorized users. This is also the property that sensitive information is not disclosed to unauthorized individuals, entities, or processes." (Walker, *CEH*, 390)

Cryptography – "The science of communicating using secret codes." (Brooks, *Computer and Network Security*, 75)

Cyber Force Protection – Measures taken to prevent or mitigate hostile actions against information technology systems and their associated users, data, and communications media, upon which DOD relies.
(Author's definition, drawing from the JP 3-0 definition of Force Protection)

Cyber Information Operations (Cyber IO) – Operations conducted in or through cyberspace to influence, disrupt, corrupt, or usurp adversary or potential adversary decision making.
(Author's definition, drawing from the JP 3-13 definition of IO)

Cyber Intelligence Operations – Operations conducted in or through cyberspace for the purpose of gathering intelligence. (Author's definition)

Cyber Persona – "The digital representation of an individual or entity identity in cyberspace." (JP 3-12, vi)

Cyberspace – "The global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." (JP 3-12, v)

Cyberspace Operations (CO) – "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." (JP 3-12, v)

Encryption – "Conversion of plain text to cipher text through the use of a cryptographic algorithm." (Walker, *CEH*, 393)

Force Protection - "Measures taken to prevent or mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information." (JP 3-0, III-30)

Foreign Internal Defense (FID) – "The participation by civilian and military agencies of a government in any of the action programs taken by another government or other designated organization, to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to their security." (JP 3-22, ix)

Global SOF Network – "A synchronized network of people and technology (US, allies, and partner nations [PNs]) designed to support commanders through inter-operable capabilities that enable special operations." (JP 3-05, I-1)

Information Assurance (IA) – "Actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation." (JP 3-12, GL-4)

Information Operations (IO) – "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own." (JP 3-13, 2014 version, GL-3)

Information Warfare (IW) – "Actions taken to affect adversary information and information systems while defending one's own… during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries." (JP 3-13, 1998 version, I-1)
This term has been superseded by "information operations (IO)."

Integrity – "The security property that data is not modified in an unauthorized and undetected manner. Also, this is the principle and measures taken to ensure that data received is in the same condition and state as when it was originally transmitted." (Walker, *CEH*, 398)

Malware – "A program or piece of code inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system. Malware consists of viruses, worms, and other malicious code." (Walker, *CEH*, 400)

Nonrepudiation – "The means by which a recipient of a message can ensure the identity of the sender and that neither party can deny having sent or received the message. The most common method is through digital certificates." (Walker, *CEH*, 401)

Offensive Cyberspace Operations (OCO) – "Cyberspace operations intended to project power by the application of force in or through cyberspace." (JP 3-12, GL-4)

Open Systems Interconnection (OSI) Reference Model – "A network architecture framework developed by ISO that describes the communications process between two systems across the Internet in seven distinct layers." (Waker, *CEH*, 402)

Protocol – "A formal set of rules describing data transmissions, especially across a network. A protocol determines the type of error checking, the data compression method, how the sending device will indicate completion, how the receiving device will indicate the message was received, and so on." (Walker, *CEH*, 404)

Proxy Server – "A device set up to send a response on behalf of an end node to the requesting host. Proxies are generally used to obfuscate the host from the Internet." (Walker, CEH, 404)

Security Cooperation (SC) – "DOD interactions with foreign defense establishments to build defense relationships that promote specific US security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide US forces with peacetime and contingency access to a host nation." (JP 3-22, x)

Security Force Assistance (SFA) – "The set of Department of Defense (DOD) activities that contribute to unified action by the United States Government (USG) to support the development of capability and capacity of foreign security forces (FSF) and supporting institutions." (JDN 1-13, vii)

Social Engineering – "A non-technical method of hacking. Social engineering is the art of manipulating people, whether in person (human-based) or via computing methods (computer-based), into providing sensitive information." (Walker, *CEH*, 410)

Special Forces (SF) – "United States Army forces organized, trained, and equipped to conduct special operations with an emphasis on unconventional warfare capabilities." (JP 3-05, GL-10)

Special Operations Forces (SOF) – For the purposes of this paper, SOF may refer to both US and international military forces designated to conduct special operations. The US definition includes "those Active and Reserve Component forces of the Services designated by the Secretary of Defense and specifically organized, trained, and equipped to conduct and support special operations." (JP 3-05, GL-11)

Tunneling – "Transmitting one protocol encapsulated inside another protocol." (Walker, *CEH*, 412);
"Taking the packets for one protocol and inserting them as data into the payload field of another protocol." (Brooks, *Computer and Network Security*, 129)

Unconventional Warfare (UW) – "Operations and activities that are conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerilla force in a denied area." (JP 3-05, xi)

US Special Operations Command (USSOCOM/SOCOM) – "A unified combatant command performing the functions of programming, budgeting, acquisition, organizing, training, equipping, and providing combat-ready SOF for employment by [combatant commanders] and developing strategy, doctrine, tactics, and procedures for SOF." (JP 3-05, I-3)

US Special Operations Forces (USSOF) – Forces subordinate to USSOCOM including Army SOF (Special Forces, Rangers, Special Operations Aviators, Civil Affairs Soldiers, Military Information Support Operators, Training Cadre, and Sustainment Soldiers) under the US Army Special Operations Command, Navy SOF (SEALs [Sea, Air, Land Operators], Special Warfare Combat Craft Crewmen, and Enablers) under the Naval Special Warfare Command, Air Force SOF (Special Tactics Teams, Special Operations Aviators, and Support Air Commandos) under the US Air Force Special Operations Command, and Marine Corps SOF (Critical Skills Operators, Special Operations Officers, Special Operations Capabilities Specialists, and Special Operations Combat Service Specialists) under the Marine Corps Special Operations Command. (USSOCOM Fact Book, 18-30)

Bibliography of Scholarly and Professional Works

Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, and Steve Chon. "Organizations and Cybercrime." *International Journal of Cyber Criminology* 8, no. 1 (January – June 2014): 1-20.

Brooks, Richard R. *Computer and Network Security: Navigating Shades of Gray*. Boca Raton, FL: CRC Press, 2014.

Covington, Michael J. and Rush Carskadden. "Threat Implications of the Internet of Things." In *2013 5th International Conference on Cyber Conflict*, edited by K. Podins, J. Stinissen, and M. Maybaum. Tallinn, Estonia: NATO CCD COE Publications, 2013. https://ccdcoe.org/cycon/2013/proceedings/d1r1s6_covington.pdf.

Duggan, Patrick M. "Strategic Development of Special Warfare in Cyberspace." *Joint Forces Quarterly* 79 (4th Quarter, 2015): 46-53. http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79.pdf.

Edgar, Jeffry L. "The Role of Special Operations Forces in Information Warfare: Enablers, not Cyber Warriors." Master's thesis, Naval War College, Newport, RI, May 2000. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA381914.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2 (Fall 2013): 41-73, http://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136.

Goodman, Will. "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* (Fall 2010): 102-135. http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf.

Lindsay, Jon R. "Reinventing the Revolution: Technological Visions, Counterinsurgent Criticism, and the Rise of Special Operations." *The Journal of Strategic Studies* 36, no. 3 (2013): 422-453.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, eds. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. New York, Oxford University Press, 2015.

McDonald, Scott D., Brock Jones, and Jason M. Frazee. "Phase Zero: How China Exploits It, Why The United States Does Not." *Naval War College Review* 65, no. 3 (Summer 2012): 123-136. https://www.usnwc.edu/getattachment/eef71cb7-abe7-4410-adaf-d78d085d933e/Phase-Zero--How-China-Exploits-It,-Why-the-United-.

Nordmoe, Matthew. "The Ghost in the Machine: Defining Special Operations Forces in Cyberspace." Master's thesis, The College of International Security Affairs, National Defense University, Fort Bragg, NC, 2015. http://www.academia.edu/12465632/The_Ghost_in_the_Machine_Defining_Special_Operations_Forces_in_Cyberspace.

Ricks, Chuck. *The Role of the Global SOF Network in a Resource Constrained Environment.* MacDill Air Force Base: JSOU Press, 2013. http://jsou.socom.mil/JSOU%20Publications/Global%20SOF%20Network%20Resource%20Constrained%20Environment_FINAL.pdf.

Rosenzweig, Paul. *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World*. Santa Barbara, CA: ABC-Clio LLC, 2013.

Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. *Introduction to Cyber Warfare: A Multidisciplinary Approach*. Waltham, MA: Elsevier, 2013.

Sharma, Deepak. "China's Cyber Warfare Capability and India's Concerns." *Journal of Defence Studies* 5, no. 2 (April 2011): 62-76. http://www.idsa.in/system/files/jds_5_2_dsharma.pdf.

Siboni, Gabi and Kronenfeld, Sami. "Developments in Iranian Cyber Warfare: 2013-2014." *Military and Strategic Affairs* 6, no. 2 (August 2014): 83-104.

Singer, Peter W. and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014.

Snegovaya, Maria. *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*. Washington, D.C.: Institute for the Study of War, September 2015. http://understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf.

Thiele, Ralph D. "Crisis in Ukraine – The Emergence of Hybrid Warfare." *ISPSW Strategy Series: Focus on Defense and International Security* 347 (May, 2015): 1-13. http://mercury.ethz.ch/serviceengine/Files/ISN/190792/ipublicationdocument_singledocument/079a09dd-8d89-40e9-affc-70857997cead/en/347_Thiele_RINSA.pdf.

Thomas, Timothy L. "Google Confronts China's Three Warfares." *Parameters* (Summer 2010): 101-113. http://fmso.leavenworth.army.mil/documents/googleconfrontschina.pdf.

Thomas, Timothy. "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" *Journal of Slavic Military Studies* 27, no. 1 (January-March, 2014): 101-130.

Threat Knowledge Group. *The Islamic State and Information Warfare: Defeating ISIS and the Broader Global Jihadist Movement*. Threat Knowledge Group Special Report. January 2015. http://threatknowledge.org/wp-content/uploads/2015/11/TKG-Report-ISIS-Info-Warfare.pdf.

Walker, Matt. *CEH Certified Ethical Hacker All-in-One Exam Guide*. Second Edition. McGraw Hill: New York, 2014.

Yarger, Harry R. *Building Partner Capacity*. MacDill Air Force Base: JSOU Press, February 2015. http://jsou.socom.mil/JSOU%20Publications/JSOU15-1_Yarger_BPC_FINAL.pdf.

Bibliography of Government Sources

Clapper, James R. *Worldwide Threat Assessment of the US Intelligence Community*. Statement for the Record. Washington, D.C.: Senate Armed Services Committee. February 9, 2016. http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

Department of Defense. *DOD Cyber Strategy*. Washington, D.C.: Department of Defense, April 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Headquarters, Department of the Army. *Unconventional Warfare.* Army Techniques Publication No. 3-05.1. Washington, D.C.: Department of the Army, September 6, 2013. https://armypubs.us.army.mil/doctrine/DR_pubs/dr_c/pdf/atp3_05x1.pdf.

Information Assurance Support Environment. "DoD Cyber Awareness Challenge." Defense Information Systems Agency, Fort Meade, MD. Accessed February 11, 2016. http://iatraining.disa.mil/eta/cyberchallenge_v3_fy15/launchPage.htm.

The White House. *Building a Nation of Makers: Universities and Colleges Pledge to Expand Opportunities to Make*. Washington, D.C.: The White House, June, 2014. https://www.whitehouse.gov/sites/default/files/microsites/ostp/building_a_nation_of_makers.pdf.

The White House. *National Security Strategy*. Washington, D.C.: The White House, February 2015. https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

US Army Special Operations Command. *ARSOF 2022*. Fort Bragg, NC: USASOC, accessed January 20, 2016. http://www.soc.mil/Assorted%20Pages/ARSOF2022_vFINAL.pdf.

US Army Special Operations Command. *ARSOF Next: A Return to First Principles.* Fort Bragg, NC: USASOC, accessed October 30, 2015. http://www.soc.mil/swcs/SWmag/archive/ARSOF_Next/ARSOF%20Next.pdf.

US Congress. House. *Statement of General Joseph L. Votel, US Army, Commander, United States Special Operations Command before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities*. Washington, D.C.: US Congress, March 18, 2015. http://www.socom.mil/Documents/2015%20USSOCOM%20Posture%20Statement.pdf.

US Joint Chiefs of Staff. *Cyberspace Operations*. Joint Publication 3-12 (R). Washington, D.C., Joint Staff, February 5, 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

US Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms*. Joint Publication 1-02. Washington, D.C., Joint Staff, November 8, 2010 (as amended through November 15, 2015). http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

US Joint Chiefs of Staff. *Doctrine for the Armed Forces of the United States*. Joint Publication 1 (JP 1). Washington, D.C., Joint Staff, March 25, 2013. http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.

US Joint Chiefs of Staff. *Foreign Internal Defense*. Joint Publication 3-22 (JP 3-22). Washington, D.C., Joint Staff, July 12, 2010. http://www.dtic.mil/doctrine/new_pubs/jp3_22.pdf.

US Joint Chiefs of Staff. *Joint Operations*. Joint Publication 3-0 (JP 3-0). Washington, D.C., Joint Staff, August 11, 2011. http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.

US Joint Chiefs of Staff. *Joint Operation Planning*. Joint Publication 5-0 (JP 5-0). Washington, D.C., Joint Staff, August 11, 2011. http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.

US Joint Chiefs of Staff. *Security Force Assistance*. Joint Doctrine Note 1-13 (JDN 1-13). Washington, D.C., Joint Staff, April 29, 2013. http://www.dtic.mil/doctrine/notes/jdn1_13.pdf.

US Joint Chiefs of Staff. *Special Operations*. Joint Publication 3-05 (JP 3-05). Washington, D.C., Joint Staff, July 16, 2014. http://www.dtic.mil/doctrine/new_pubs/jp3_05.pdf.

US Joint Chiefs of Staff. *The National Military Strategy of the United States of America: 2015*. Washington, D.C.: Joint Staff, June 2015. http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.

US Special Operations Command. *United States Special Operations Command Fact Book 2015*. MacDill Air Force Base, FL: USSOCOM, 2015. http://www.socom.mil/Documents/2015%20Fact%20Book.pdf.

US Special Operations Command. *United States Special Operations Command SOCOM 2020: Forging the Tip of the Spear*. MacDill Air Force Base, FL: USSOCOM, accessed October 30, 2015. http://www.defenseinnovationmarketplace.mil/resources/SOCOM2020Strategy.pdf.

US Special Operations Command. *United States Special Operations Command Special Operations Forces Operating Concept.* MacDill Air Force Base, FL: USSOCOM, May 2013. https://fortunascorner.files.wordpress.com/2013/05/final-low-res-sof-operating-concept-may-2013.pdf.

Work, Robert O. *Cyberspace Workforce Management*. Department of Defense Directive 8140.01. Washington, D.C.: Deputy Secretary of Defense, August 11, 2015. http://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf.

Bibliography of Technical Sources

Adafruit. “Arduino.” Accessed January 22, 2016, https://www.adafruit.com/category/17.

Congdon, Jesse. “Arduino Powered 2.4 GHz Spectrum Analyzer.” Hackaday, July 25, 2011. http://hackaday.com/2011/07/25/arduino-powered-2-4-ghz-spectrum-analyzer/.

FireEye Labs. *APT28: A Window into Russia’s Cyber Espionage Operations.* Milpitas, CA: FireEye, Inc., 2014. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.

FireEye Labs. *APT30 and the Mechanics of a Long-Running Cyber Espionage Operation*. Milpitas, CA: FireEye, Inc., April, 2015. https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf.

McAfee. *Net Losses: Estimating the Global Impact of Cybercrime*. McAfee, Inc., Santa Clara, CA, 2014. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

Radware. *ISIS Cyber Attacks: ERT Threat Alert*. Radware Ltd., Tel Aviv, Israel, April, 2015. https://security.radware.com/uploadedFiles/Resources_and_Content/Threat/ERT%20Threat%20Alert%20-%20ISIS%20Cyber%20Attacks.pdf.

Schwartz, Marc-Olivier. “Wireless Security Camera with the Arduino Yun.” Adafruit, May 4, 2015. https://learn.adafruit.com/wireless-security-camera-arduino-yun/introduction.

Smokeyd. “Arduino Radio Spectrum Analyzer Prototype on a Breadboard.” Nurdspace. Accessed January 22, 2016, https://nurdspace.nl/Arduino_Radio_Spectrum_Analyzer_prototype_on_a_breadboard.

Wright, Joshua. “Hacking the Internet of Things.” Army Cyber Institute Talks, National Defense University, Washington, D.C., September 22, 2015. https://www.youtube.com/watch?v=4Yh3GmrKM3w.

Bibliography of Other Sources

Ackerman, Spencer. "Real Men Use Android: Special Forces Favor Google Phone." Wired, October 29, 2010, http://www.wired.com/2010/10/special-forces-want-android-apps-for-warzone-john-maddens/.

Alexander, David. "The OPM Hack was a lot Worse than Previously Disclosed." The Huffington Post, September 23, 2015. http://www.huffingtonpost.com/entry/opm-hack_us_5602f64be4b08820d91b59c2.

Costlow, Terry. "Mobile Mashup: The Military's Proliferating Mix of Smartphones and Tablets." Defense Systems, March 23, 2015. https://defensesystems.com/articles/2015/03/23/military-unconventional-mix-smartphone-tablets.aspx.

Defense Systems Staff. "Special Forces Aiming to Lock Down Blackberry 10 Devices." Defense Systems, April 17, 2015. https://defensesystems.com/articles/2015/04/17/special-operations-blackberry-integrity-agent.aspx.

Deloitte Center for the Edge and Maker Media. *Impact of the Maker Movement*. Maker Media Inc., San Francisco, CA, 2014. http://makermedia.com/wp-content/uploads/2014/10/impact-of-the-maker-movement.pdf.

Dougherty, Dale. *Maker Market Study: An In-Depth Profile of Makers at the Forefront of Hardware Innovation*. Maker Media Inc., San Francisco, CA, 2012, http://cdn.makezine.com/make/sales/Maker-Market-Study.pdf.

Dunlap, Charlie. "Cyber Operations and the New Department of Defense Law of War Manual: Initial Impressions." Lawfare, June 15, 2015. https://www.lawfareblog.com/cyber-operations-and-new-defense-department-law-war-manual-initial-impressions.

Hagel, John, John Seely Brown, and Duleesha Kulasooriya. *A Movement in the Making*. Deloitte University Press, 2013. http://dupress.com/articles/a-movement-in-the-making/.

Hatch, Mark. *The Maker Movement Manifesto: Rules for Innovation in the New World of Crafters, Hackers, and Tinkerers*. New York: McGraw Hill, accessed October 30, 2015. http://www.techshop.ws/images/0071821139%20Maker%20Movement%20Manifesto%20Sample%20Chapter.pdf.

Hsu, Ray. "The World is Ours to Make: The Impact of the Maker Movement." EDN Network, February 18, 2015. http://www.edn.com/design/diy/4438686/The-world-is-ours-to-make--The-impact-of-the-maker-movement.

Internet Society. *Global Internet Report 2015*. Internet Society, Reston, VA, 2015. http://www.internetsociety.org/globalinternetreport/assets/download/IS_web.pdf.

Lyne, James. *Security Threat Trends 2015*. Sophos Ltd., Oxford, UK, 2014. https://www.sophos.com/en-us/threat-center/medialibrary/PDFs/other/sophos-trends-and-predictions-2015.pdf?cmp=70130000001xKqzAAE.

Matthews, Owen. "From Russia with Malware." *Newsweek Global* 164, no 19 (May 15, 2015): 26-33.

Nikkei Asian Review. "Toyota to Make Networked Cars Standard in Japan, US." Nikkei Asian Review, October 17, 2015. http://asia.nikkei.com/Tech-Science/Tech/Toyota-to-make-networked-cars-standard-in-Japan-US.

Telematics News. "Mercedes-Benz Offers New Range of 'Connect Me' Services." Telematics News, May 22, 2014. http://telematicsnews.info/2014/05/22/mercedes-benz-offers-new-range-of-connect-me-services_m5223/.

"The 'Gerasimov Doctrine' and Russian Non-Linear War." *In Moscow's Shadows*, blog, accessed October 30, 2015. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.