Special Operations Forces Truths – Cyber Truths

Major General Stephen G. Fogarty
Major Jamie O. Nasi

INTRODUCTION

The Special Operations Forces (SOF) Truths—humans are more important than hardware, quality is better than quantity, SOF cannot be mass produced, competent SOF cannot be created after emergencies occur, and most special operations require non-SOF assistance—have become tried-and-true guiding principles for the special operations community. [1] This article explains why and how the United States Army can repurpose SOF Truths to serve as guiding principles to recruit, resource, and train effective Cyber leaders, operators, organizations, and capabilities. This article provides the SOF Truths lineage and illustrates their relevance to the cyberspace domain so as to advocate for the incorporation of a set of Cyber Effects Truths for the Army's contribution to the Joint Cyber Mission Force (CMF).

SOF TRUTHS

The earliest known published work incorporating the SOF Truths is the 1987 publication titled *United States and Soviet Special Operations;* a report to Senate Armed Services Committee. The SOF truths appear in the document's forward signed by Earl D. Hutto—Chairman of the Special Operations Panel—which was ghost written by John M. Collins, Senior Specialist in National Defense and retired Army officer with limited firsthand Special Operations experience. [2] [3] By 1988, Brigadier General (BG) Dave Baratto, Commanding General of the John F. Kennedy Special Warfare Center and School, was confronted with the process of codifying special operations' distinctive operational considerations as tenets, and with assimilating them across the military services. His staff added the tenets as truths to complement the newly created SOF imperatives. [4] The SOF imperatives and truths act like the two sides of a coin for recruiting/training and implementing special operations forces. The truths form the basis of how to recruit, resource, and train SOF Soldiers, whereas the imperatives provide the framework that Army SOF commanders apply to mission planning and execution. [5] BG Baratto's initiative is clearly tied to the Army Chief of Staff establishing a separate branch for Special Forces officers on April 9th, 1987, the activation of United States Special Operation Command (USSOCOM) on April 16th, 1987, and the SOF community's need to describe its unique competencies inward to the members of its ranks, and outward to the Army as a whole. [6]

By the early 1990s, USSOCOM—under the leadership of General Wayne Downing—had embraced the SOF truths, albeit the accepted list did not include the original fifth tenet; most special operations require non-SOF assistance. [7] USSOCOM retained the four SOF truths throughout the 1990s and into the new century as shown by General Peter Schoomaker's statement published in August 1999.

> You've got to select people with the highest likelihood of success. Then you've got to train, educate, and assess them constantly. You've got to keep upgrading the quality. We have a set of four SOF truths: Humans are more important than hardware. Quality is better than quantity. SOF cannot be mass produced. SOF cannot be created after a crisis occurs. These truths guide how we think about building our force. They're simple, and we repeat them over and over, and we make it every commander's responsibility to make sure that his people understand them. [8]

In 2010, the SOCOM Commander, Admiral Eric Olsen, reincorporated the fifth—so called—'lost' truth. His reasoning for the decision was to emphasize the importance and contributions that non-SOF personnel provides to SOF. [9] Additionally, he felt the fifth truth helped dispel any "...unrealistic ex-

Major General Stephen G. Fogarty assumed duties as the Commanding General, U.S. Army Cyber Center of Excellence and Fort Gordon on September 8, 2014. A career Intelligence Officer, his assignments include Commanding General, US Army Intelligence and Security Command (INSCOM); CJ-2, International Security Assistance Force; J-2, U.S. Central Command; Director, Joint Intelligence Operations Center-Afghanistan; Commander, NSA Georgia and 116th MI Brigade; Director, Integrated Survey Program, USSOCOM; G2, 101st ABN Division (AASLT); S2, 75th Ranger Regiment and S2, 2nd Ranger Battalion.

MG Fogarty holds a Bachelor of Arts degree in History from North Georgia College. He is a graduate of the U.S. Army War College with a Master's of Science degree in Strategic Studies. He also holds a Master's of Science degree in Administration from Central Michigan University. His military education also includes the MI Officer Basic and Advanced Courses, and the U.S. Army Command and General Staff College.

Major Jamie O. Nasi is a Psychological Operations Officer assigned to the United States Army John F. Kennedy Special Warfare Center and School Fort Bragg, NC and leads the Special Operations Element at the Army Cyber Center of Excellence at Fort Gordon, GA. MAJ Nasi received his commission as an Armor Second Lieutenant through ROTC at Norwich University. His recent assignments include Secretary of the General Staff, Military Information Support Operations Command (Airborne); Commander, HHC, 4th Military Information Support Operations Group (Airborne); and Detachment Commander, Bravo Company, 6th Military Information Support Operation Battalion (Airborne). He has multiple operational deployments throughout East and West Africa. MAJ Nasi holds a Bachelor of Arts degree in Peace, War, and Diplomacy from Norwich University and a Master of Science Degree in Information Strategy and Political Warfare from the Naval Postgraduate School. His education includes the Armor Officer Basic Course, Maneuver Captain's Career Course, and Joint Professional Military Education Phase I credit through the Naval War College Monterey Program.

pectations as to the capabilities SOF brings to the fight." [10]

Today, the SOF truths are still an integral part of SOF as currently depicted in the United States Army Special Operations Command's (USASOC) ARSOF 2022; a document that provides not only the intellectual framework but also the foundational precepts to ensure SOF will succeed in the future operating environment. [11] A direct correlation is present between the SOF truths and USASOC's priorities outlined in ARSOF 2022; win the current fight, strengthen the global SOF network, further Army SOF/CF interdependence, and preserve the force. [12]

CYBER BRANCH

Until the Army established the Cyber branch in 2014, most cyber work was performed by Soldiers and civilians in the Military Intelligence Corps and Signal Corps. On 1 September, 2014 the Secretary of the Army and Chief of Staff of the Army established the Army's newest branch in recognition that the demands of the cyberspace domain required a dedicated professional cyber workforce to conduct cyber effects operations in support of Unified Land Operations. While slightly ahead of its time, this decision made the Army fully compliant with DoD Directive 8140.01 (Cyberspace Workforce Management) signed on 11 August 2015 that established the Cyberspace Effects Workforce (the authors shorten to simply Cyber Workforce for the remainder of this article) as one of the four personnel areas within the greater cyberspace workforce. The Cyber branch is not only the Army's newest branch, it is also the smallest making it vitally important that only the most talented individuals are selected for the branch. Establishing basic principles for organizing, selecting, training, and operating the Army's contribution to the Joint Cyber Mission

Force is critical, and although the Cyber branch's roots are principally Intelligence and Signal, its future development is likely to be more similar to Special Operations Forces. Therefore, it is appropriate to determine if the tenets used by SOF can be applied to the Army's portion of the Joint Cyberspace Effects Workforce.

Humans Are More Important Than Hardware

It has been a long-standing conviction in the SOF community that humans are more important than hardware. Highly skilled Soldiers with the proper training and direction can accomplish more than the most advanced equipment in the hands of less capable forces. This is because properly prepared Soldiers have the ability to think, learn, reason, and quickly adapt to changing conditions in a way that lesser trained forces, even if better equipped, cannot. For SOF, Soldiers are their center of gravity.[13] In this environment, advanced equipment and systems are simply tools that enable SOF personnel to accomplish their tasks. The same can be said for the growing Cyber Workforce where operational agility, adaptive thinking, and innovative leadership are cornerstones to operational effectiveness. It is important to understand that while advanced platforms and systems are essential enablers for SOF and the Cyber Workforce, the useful shelf life of any specific "cyber" tool or platform is likely to be short, while investment in talent acquisition and subsequent talent management of the Cyber Workforce will produce a long-term return on investment, both now and into the future. Adopting a strategy of equipping the man vs. manning the equipment is equally important for SOF and the Cyber Workforce. This is why it is imperative to invest in rigorous selection, education, and training for our Cyber Workforce so they are prepared to overmatch any current or future US adversaries in and through the cyberspace domain.

Humans Are More Important Than Technology

Quality Is Better Than Quantity.

SOF relies on small teams of highly trained specialized personnel to operate across a range of critical capabilities, surgical strike to unconventional warfare, and numerous types of operating environments, permissive to hostile. Due to these considerations, SOF cannot sacrifice standards to create a larger force as it would likely lose its decisive advantage over the enemy. The Cyber Workforce also functions in complex environments with a myriad of operational risks and opportunities. They conduct operations in peacetime as well as periods of active hostilities, and their actions have the potential to create tactical, operational, and strategic effects—amid the rapid rate the cyberspace domain changes; fueled by advancements in technology and the absence of physical borders. Our adversaries in this environment are technically savvy, highly motivated, adaptive, and persistent. Our Cyber Workforce must not only be technically and tactically superior, but must operate morally, ethically, and within the law of armed conflict and specified rules of engagement. The training, education, and ability to work as a highly functioning member of a team required to conduct successful operations in and through the cyberspace domain simply requires a level of talent possessed by only a few. To allow or to enable the Cyber Workforce to succeed in this environment requires intensive talent management, realistic education and training, and persistent operations.

Quality Is More Important Than Quantity

SOF Cannot Be Mass Produced.

It takes skill to recruit and select, and years to train SOF Soldiers. After initial assessment and qualification training, pipeline training for individual operators and teams may take years of additional education and training to meet stringent operational requirements. This is by no means a cookie cutter approach to training and education; flexibility is built into the system exposing SOF to diverse opportunities that forces innovation to continually incorporate lessons learned and advanced techniques into their highly specialized formations. SOF must continually evolve to decisively beat adaptive adversaries. Like SOF, an effective Cyber Mission Force requires specialized recruitment, selection, training and career management processes to effectively access talent, train and educate the individuals and teams and aggressively manage their development. The Cyber Workforce unique mission and operational environment demands its members embrace a life time of learning otherwise our adversaries will enjoy overmatch. Technology changes at a rapid pace and so must the capabilities and development of our Cyber Workforce. The training pipeline to develop a single interactive operator requires over two years of intense training and education to become a mission ready, productive member of a Cyber Mission team. Production of Fully Operationally Capable (FOC) Cyber Mission Force teams takes many years as proven by DoD's multi-year Cyber Mission Force build schedule. The capacity to surge and meet urgent mission requirements is very limited; therefore, careful thought must be given to future force manning, mission alignment, and skill development requirements. Failure to maintain appropriate capability and capacity will have severe consequences for SOF and the Army's contribution to the CMF.

> Today, the SOF truths are still an integral part of SOF as currently depicted in the United States Army Special Operations Command's (USASOC) ARSOF 2022.

Cyber Forces Cannot Be Mass Produced

Competent Special Operations Forces Cannot Be Created After Emergencies Occur.

It is imperative that SOF forces exist and train in peacetime and are not a byproduct of an emergency. While it takes significant time to train competent SOF operators, it requires even more time to develop cohesive teams able to consistently and successfully perform the missions in the environments previously discussed. Similarly, a competent Cyber Workforce cannot be created in a crisis for these same reasons. The capability to conduct synchronized and successful cyber effects and electronic warfare operations cannot be developed overnight. They are the result of realistic training exercises and actual online operations. Most importantly, the Cyber Workforce must maintain persistent contact with emerging technologies, threats, and adversaries. Easy access to a persistent training environment featuring robust cyber ranges and a thinking and capable opposing force equipped with the most current tools, techniques, and technologies is required to assure the Joint Cyber Mission Force can over match adversaries in the cyberspace domain. This level of expertise cannot be built quickly.

Competent Cyber Mission Forces Cannot Be Created After Emergencies Occur

Most SOF Activities Require Non-SOF Assistance.

It is remarkably uncommon for a SOF element to operate unilaterally without outside support. Although SOF are highly skilled and extraordinarily trained, to maximize effectiveness, they often require non-SOF subject matter experts and capabilities; intelligence, logistical, and interagency support are just a few of the various types of support SOF may require. Close relationships with interagency and multinational partners are often the key to successful SOF operations. This truth is also applicable to the Cyber Workforce, which is often dependent on Signal, Intelligence, Electronic Warfare, Fires, and Information Operations capabilities as well as interagency, multinational, and commercial partners. Critical to this process is changing the culture in the Army to encourage effective collaboration with all the stakeholders in the cyberspace domain. This places a high premium on the Cyber Workforce to establish collaboration mechanisms outside of the highly classified and compartmentalized environment when possible and to ensure that stakeholders are represented by appropriately cleared liaisons. It is essential that the Cyber Workforce develops a culture that mandates ruthless collaboration with partners in academia, industry, interagency, and internationally.

> The same can be said for the growing Cyber Workforce where operational agility, adaptive thinking, and innovative leadership are cornerstones to operational effectiveness.

Most Cyber Activities Require Non-Cyber Workforce Assistance

CONCLUSION

It is apparent the SOF Truths are in fact relevant to the Cyber Workforce, and with minor modification can form a useful set of tenets to better enable assessment, selection, and training of the Army's contribution to the Joint Cyber Mission Force. Although additional Cyber Workforce Truths may be identified in the future, the five listed below can be applied immediately by the Army's newest branch:

Humans are more important than technology,

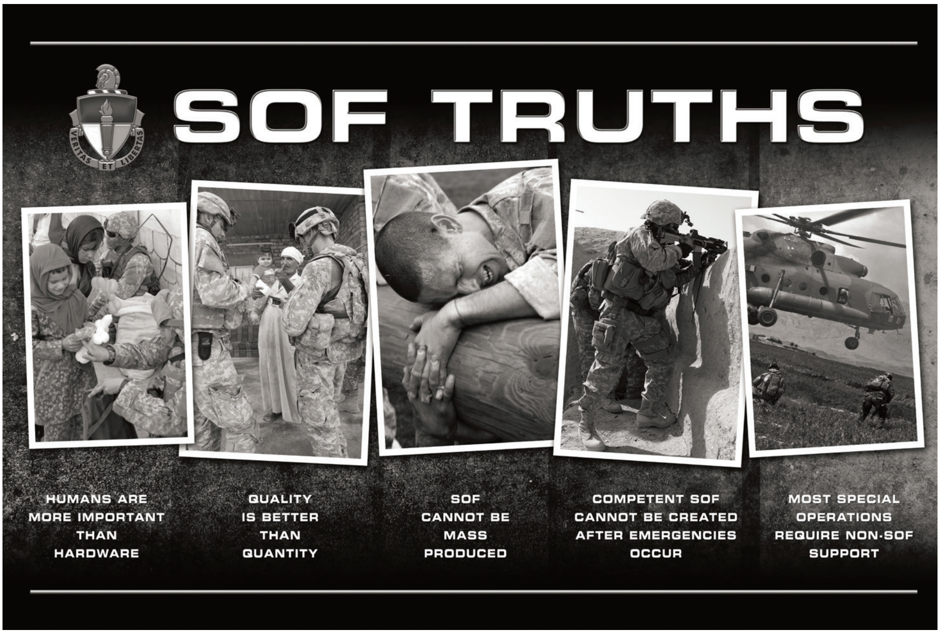
Quality is more important than quantity,

Cyber Forces personnel cannot be mass produced,

Competent Cyber Mission Forces cannot be created after emergencies occur,

Most cyber activities require non-Cyber Workforce assistance.

Predating the decision to form the Cyber branch, the Army transitioned the former Signal Center of Excellence at Fort Gordon, Georgia into the Cyber Center of Excellence or CCoE. The CCoE is the home of the Signal School and the newly formed Cyber School. The Cyber School is in the process of training and educating the officers, warrant officers, and noncommissioned officers who are the core of the new branch and the Cyber Workforce. Per Headquarters Department of the Army execution order 057-14, the CCoE is the Army's Force Modernization Proponent for Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, and Facilities (DOTMLPF) requirements, capabilities, and activities related to Cyberspace Operations, Signal/Communications Networks and Information Services, and Electronic Warfare. The Army Force Modernization Proponent System provides guidelines and functions for establishing and maintaining an effective force supporting Army warfighting requirements. As such, the CCoE is adopting the Cyber Truths as part of its strategy to educate, train, and develop current and future Cyber Workforce members to ensure their readiness to conduct cyber effects operations in support of Unified Land Operations.



SOF TRUTHS

HUMANS ARE MORE IMPORTANT THAN HARDWARE

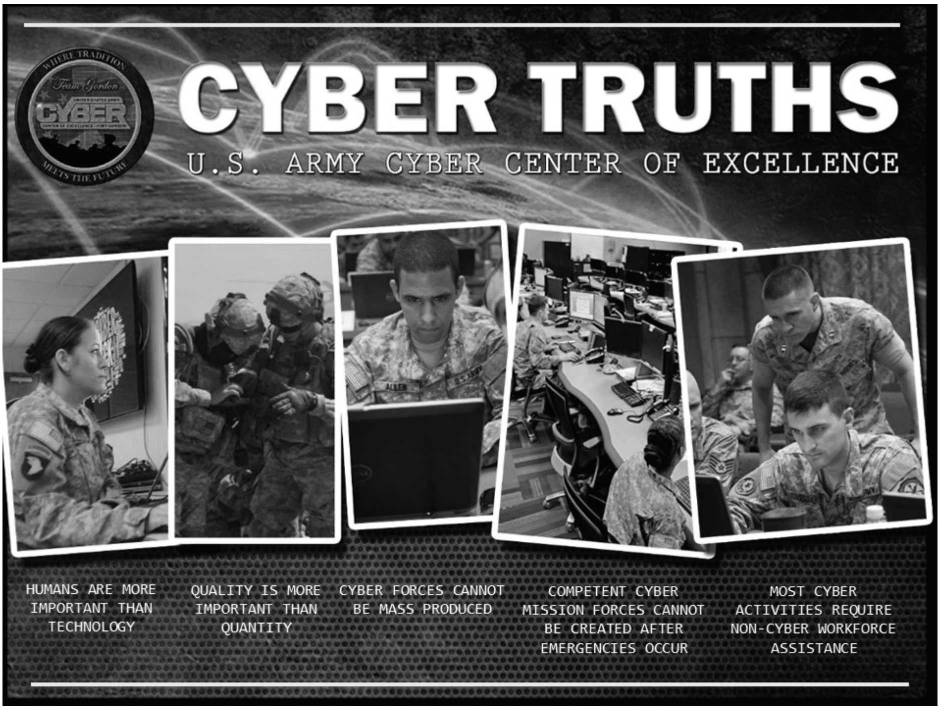
QUALITY IS BETTER THAN QUANTITY

SOF CANNOT BE MASS PRODUCED

COMPETENT SOF CANNOT BE CREATED AFTER EMERGENCIES OCCUR

MOST SPECIAL OPERATIONS REQUIRE NON-SOF SUPPORT

U.S. Army Special Operations Center of Excellence, U.S. Army Special Operations Center of Excellence Downloadable ARSOF Media, soc.mil, accessed April 14, 2016, http://www.soc.mil/SWCS/Posters.htm.



CYBER TRUTHS

U.S. ARMY CYBER CENTER OF EXCELLENCE

HUMANS ARE MORE IMPORTANT THAN TECHNOLOGY

QUALITY IS MORE IMPORTANT THAN QUANTITY

CYBER FORCES CANNOT BE MASS PRODUCED

COMPETENT CYBER MISSION FORCES CANNOT BE CREATED AFTER EMERGENCIES OCCUR

MOST CYBER ACTIVITIES REQUIRE NON-CYBER WORKFORCE ASSISTANCE

NOTES

[1] United States Special Operation Command, *SOF Truths,* accessed March 30, 2016, http://www.socom.mil/pages/softruths.aspx.

[2] John Collins, "The Warlord on Special Operations Forces," *War on the Rocks,* September 10, 2013, accessed 30 March 2016, http://warontherocks.com/2013/09/warlord-on-special-operations-forces/.

[3] It is important to note that the SOF truths were likely articulated ideas already present within the ARSOF community prior to the publication's release date.

[4] Sean D. Naylor, *Adm Olsen Adds "Lost" 5th SOF Truth to Doctrine,* Navyseals.com, accessed March 30, 2016, http://navyseals.com/nsw/adm-olsen-adds-lost-5th-sof-truth-doctrine/.

[5] U.S. Department of the Army, *ADRP 3-05 Special Operations,* (Washington DC: GPO, 2012).

[6] Naylor, *Adm Olsen Adds "Lost" 5th SOF Truth to Doctrine.*

[7] Ibid.

[8] Eli Cohen and Noel Tichy, *Operation – Leadership,* fastcompany.com, accessed March 30, 2016, http://www.fastcompany.com/37511/operation-leadership.

[9] Naylor, *Adm Olsen Adds "Lost" 5th SOF Truth to Doctrine.*

[10] Ibid.

[11] U.S. Army Special Operations Command, "ARSOF 2022," *Special Warfare Magazine* 26, no. (2013): 9.

[12] Ibid.

[13] U.S. Army Special Operations Command, "ARSOF 2022," 18.