AIR LAND SEA BULLETIN

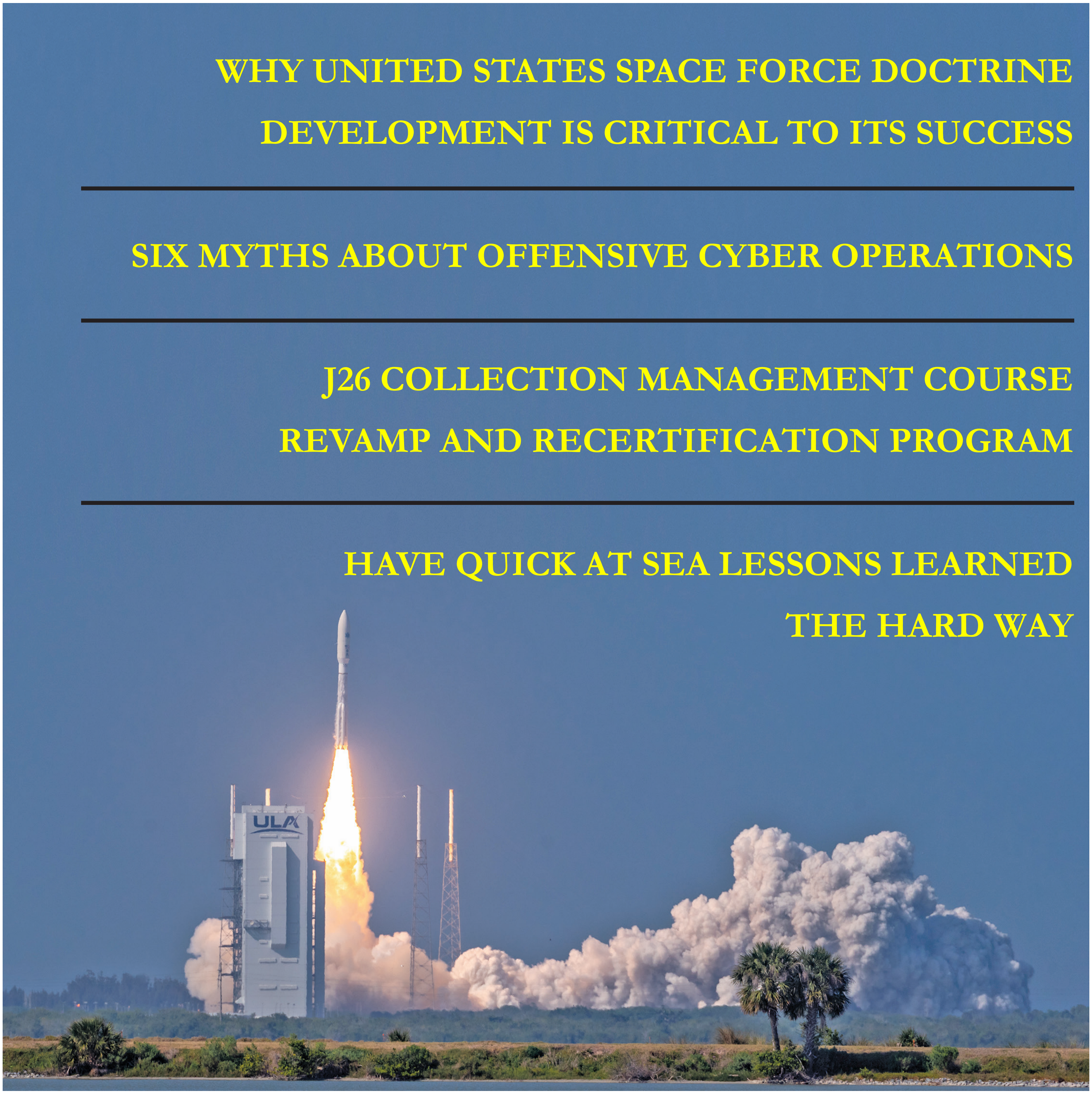
Issue No. 2020-2 Air Land Sea Application (ALSA) Center *Summer 2020*

WHY UNITED STATES SPACE FORCE DOCTRINE DEVELOPMENT IS CRITICAL TO ITS SUCCESS

SIX MYTHS ABOUT OFFENSIVE CYBER OPERATIONS

J26 COLLECTION MANAGEMENT COURSE REVAMP AND RECERTIFICATION PROGRAM

HAVE QUICK AT SEA LESSONS LEARNED THE HARD WAY



ALSA Staff

Director
COL Ian Bennett, USA

Deputy Director
Col Aaron Clark, USAF

Bulletin Editor
Maj John Bradley, USMC

Editor
Ms. Patricia Radcliffe, Civilian, USAF

Layout Artist/Illustrator
Ms. Laura Caswell, Civilian, USN

Publications Officer
Lt Col Tony Curtis, USAF

Purpose: The ALSA Center is a multi-Service Department of Defense field agency sponsored by the US Army Training and Doctrine Command (TRADOC), Marine Corps Training and Education Command (TECOM), Navy Warfare Development Command (NWDC), and Curtis E. LeMay Center for Doctrine Development and Education (LeMay Center). The ALSB is a vehicle to "spread the word" on recent developments in warfighting concepts, issues, and Service interoperability. It provides a cross-Service flow of information among readers around the globe. ALSA publishes the ALSB two times a year. This periodical is governed by Army Regulation 25-30.

Disclaimer: The ALSB is an open forum. The articles, letters, and opinions expressed or implied herein should not be construed as the official position of TRADOC, TECOM, NWDC, the LeMay Center, or ALSA Center.

Submissions: Get published—ALSA solicits articles and readers' comments. Contributions of 5,000 words or less are ideal. Submit contributions double-spaced in MS Word. Include the author's name, title, complete unit address, telephone number, and email address. Graphics can appear in an article, but a **separate computer file for each graphic and photograph (photos must be 300 dpi) must be provided.** Send email submissions to alsadirector@us.af.mil. The ALSA Center reserves the right to edit content to meet space limitations and conform to the ALSB style and format.

Reprints: The ALSA Center grants permission to reprint articles. Please credit the author and the *ALSB*. Local reproduction of the *ALSB* is authorized and encouraged.

CONTENTS

FEATURE ARTICLES

IN HOUSE

AIR LAND SEA BULLETIN

Issue No. 2020-2 Air Land Sea Application (ALSA) Center Summer 2020

WHY UNITED STATES SPACE FORCE DOCTRINE DEVELOPMENT IS CRITICAL TO IT'S SUCCESS

SIX MYTHS ABOUT OFFENSIVE CYBER OPERATIONS

J26 COLLECTION MANAGEMENT COURSE REVAMP AND RECERTIFICATION PROGRAM

HAVE QUICK AT SEA LESSONS LEARNED THE HARD WAY

Cover Photo Information

An Atlas V AEHF-6 rocket successfully launches from Space Launch Complex-41 at Cape Canaveral Air Force Station, Florida, 26 March 2020. The launch of the AEHF-6, a sophisticated communications relay satellite, is the first Department of Defense payload launched for the United States Space Force. (Photo by Joshua Conti)

DIRECTOR'S COMMENTS

Since 1975, the Air Land Sea Application (ALSA) Center has worked to provide timely, relevant, and compelling doctrinal solutions to meet the needs of the warfighter. This enduring task propels the men and women of ALSA to improve processes, seek out new ideas, and navigate through an increasingly complex warfighting environment.

We welcome incoming Director, COL Ian Bennett, United States Army (USA) and Deputy Director, Col Aaron Clark, United States Air Force (USAF). We also welcome Maj Evan Fillman, USAF; MAJ Colin Greata, USA; Maj Eric Pederson, USAF; and SSgt Wesley Gray, USAF, to the to the multi-Service team.

We extend a special farewell and thank you to Deputy Director COL Matthew Ketchum, USA, and LTC James Grandy, USA, who retire after many years of long and faithful military service. We wish them and their families the best of luck on their future endeavors. Also, we say farewell to Lt Col Craig Pachlhofer, USAF, assigned to 9th Attack Squadron as Director of Operations at Holloman Air Force Base (AFB), Nevada; Maj Thomas Moore, USAF, assigned to 67th Cyberspace Wing, Joint-Base San Antonio Lackland, Texas; and SSgt Steven Warner, USAF, assigned to Nellis AFB, Nevada.

This ALSB contains four articles from the warfighter community. The first article is "Why United States Space Force Doctrine Development is Critical to its Success", by Maj Clayton Couch, USAF. This article focuses on the importance of Service doctrine and how now is a critical time for the United States Space Force (USSF) to identify the right people to write it. The author explores the idea of taking advantage of the "clean slate" the USSF has for developing space doctrine. The author also discusses the relationship between joint or Service doctrine and strategy.

The second article is "Six Myths about Offensive Cyber Operations (OCO)", by Lt Col Benjamin Ramsey, USAF, and Mr. Robert Colletti. This article discusses the misunderstanding of OCO and its effects clouding the environment for decision makers. There is a fundamental lack of understanding of cyberspace, the newest warfighting domain, existing among the Services. This article is intended to provide clarity for decision makers by debunking common myths about OCO.

The third article is "The J26 Collection Management Course Curriculum Revamp and Certification Program for the Intelligence Community and Joint Force", by Maj Douglas Wietlisbach, USAF. The author explains how, in many ways, it can be difficult for the Joint Staff and Defense Intelligence Agency to meet the collection management training and certification demands of the combatant commanders. This article is written to inform the warfighter on several collection management courses that help meet the demand on commanders.

The fourth article is "Have Quick at Sea—Lessons Learned the Hard Way", by LCDR Matthew Quintero, United States Navy. In this article the author details his personal experiences and lessons learned using Have Quick at the tactical level. He provides recommendations for the joint force moving forward.

We invite you to seize opportunities to represent your Service and the joint community by sharing articles to be published in future ALSBs and, also, participating in multi-Service tactics, techniques, and procedures (TTP) joint working groups. As we tackle the challenges ahead, your ideas matter more than ever. Your unique perspective can spark innovation for current and future joint TTP. To help shape the discussion and be part of the solution, go to www.alsa.mil and provide input through the "Contact Us" link.

Brian Gross

BRIAN J. GROSS, Colonel, USAF

Director

WHY UNITED STATES SPACE FORCE DOCTRINE DEVELOPMENT IS CRITICAL TO ITS SUCCESS

United Launch Alliance's Atlas V rocket carries the Solar Orbiter into space as it launches on 9 February 2020, at Cape Canaveral Air Force Station, Florida. The Solar Orbiter is a Sun-observing satellite which is intended to perform measurements of the inner heliosphere and perform close observations of the polar regions of the Sun. (Photo by Joshua Conti)

By Major Clayton W. Couch

"Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur."—Gen Guilio Douhet

Doctrine is a word many combat warfighters throw into everyday discussions for various self-serving purposes, but they are reticent to actually read and understand it. While warfighters are privy to their small-unit tactics or weapon system employment, the general and widespread familiarity of joint (or Service) doctrine are often put on a shelf for dusting off during developmental education. One of the few exceptions is those who find themselves in academic circles of military Service advanced warfighting schools (either as employees or students). Unfortunately, it is not these individuals who write or update doctrine because they are bound for more, seemingly, important assignments like unit command. Finding the right process, people, and place to lead strategically imperative doctrine development is critical to Service branch success.

With the recent creation of the United States Space Force (USSF), the question arises: Who will write USSF doctrine? Perhaps, it will fall on staff officers who find themselves assigned to academically inclined doctrine centers, longing to get back to a tactical warfighting unit. If so, what will happen?

Space doctrine could become a strict copy of Air Force Annex 3-14, *CounterSpace Operations* and Joint Publication (JP) 3-14, *Space Operations*, relegating space operations to a supporting Service to the other domain. Another route may be adapting tactics, techniques, and procedures (TTP) hidden within the classified security stovepipe in which most military space capabilities now live and leave them in that classified space and unfit for the force at large to know, embrace, and understand. Either case is untenable for joint operations, much less the current development of multi-domain operations (MDO). Instead, Department of Defense (DOD) leadership must aggressively put its most talented military scholars and tacticians, from all Services, to task. Now is the prime opportunity. The newly created USSF is uniquely positioned to lead space and MDO doctrine development for four reasons. First, the space domain has the most global-reaching effect on the United States (US) military's functional and geographic combatant commands while supporting effects for other instruments of national power, like information and the economy. Second, space (similar to cyber) integrates with all other military domains to support their operations, while the opposite does not always hold true. Third, there is a current momentum to develop space TTP and a general interest in space from the American public. Fourth, and perhaps most importantly, the "clean slate" presented by creation of the USSF affords a drive to create Service-specific doctrine which may force alignment of joint doctrine and multi-domain TTP.

... the space domain has the most global-reaching effect on the United States (US) military's functional and geographic combatant commands ...

The remainder of this article outlines the important relationship between doctrine and strategy, a review of doctrine development, and an overview of historic doctrine from other domains. Applied throughout are ideas and lessons learned for USSF personnel to consider when writing doctrine. This article will conclude with recommendations, based on lessons learned, to provide a framework for the way ahead.

STRATEGIC IMPERATIVES AND DOCTRINE

An important guiding strategic document, the National Defense Strategy of 2018, highlights a very important point: "A long-term strategic competition requires the seamless integration of multiple elements of national power—diplomacy, information, economics, finance, intelligence, law enforcement, and military". It also calls on the military to "integrate with US interagencies". This view transcends most historical military doctrines that primarily focus upon a particular Service or physical domain (such as air, land, or sea). The space doctrine should transcend the other domains because of the importance it holds for economic and intelligence purposes. It should be strategic-level doctrine spanning more than just the military instrument of national power.[1]

Retired Air Force Lt Gen Steven L. Kwast fervently advocated for a separate space force and significantly opening the mission scope. In this era of strategic competition, Lt Gen Kwast notes China's pursuit of a "navy in space" with the equivalent of "battleships and destroyers" that are "able to maneuver and kill and communicate with dominance."[2] He further advocates that if the USSF is not "given the mission to defend the economy of space beyond Earth's orbit, to the moon and beyond, and achieve dominance over any other competitor, it will fail at its purpose to protect our values into the future". Furthermore, he challenges national leadership to take steps to create the USSF and give it the mission to defend the economy of space.[3]

Now that the USSF has been created, what of its mission? According to its website, its mission does not include the defense of the economy.[4] A military Service's role is to organize, train, and equip forces, not conduct the warfighting itself. That is the role of US Space Command, whose mission statement includes "deter aggression and conflict" and "defend US and allied freedom of action."[5] This may include defense of economic, intelligence, and military freedom of action. JP 3-14 states, "DOD space policy is centered to deter adversaries, defend against threats, and pursue resilient space architectures".[6] It is worth quantifying the importance of defending the US and space economies.

A study by RTI (Research Triangle Institute) International puts the economic value of the US Global Positioning System (GPS) constellation's economic gain at $1.4 trillion since being made available for civilian and commercial use in the 1980s. If GPS service were lost, the estimated economic loss is $1 billion per day.[7] This is only for GPS and does not include the economic utility of commercial satellite communications, the burgeoning commercial space-based internet, or commercial space-lift.

What of the value of space resources themselves? Interest is growing. The Colorado School of Mines recently stood up the first interdisciplinary degree program of its kind in Space Resources.[8] A European Space Agency Space Resources Strategy document highlighted a study funded by the Luxembourg government citing market revenues worth 73–170 billion Euros between 2018 and 2045, and for between 845 thousand and 1.8 million full time jobs.[9] The catch is, most of these economic resources are on and beyond the moon—much as Lt Gen Kwast suggested. If America does not drive a strategy that affords its burgeoning commercial enterprises, the freedom of action needed to capitalize on such economic potential now, will it lose the opportunity to do so? If historical examples are to be believed, the answer is yes.

CURRENT AND HISTORICAL NAVAL DOCTRINE

Air Force doctrine states, "space superiority is of primary concern to airmen as it enables the continuous provision and advantages of space-enabled capabilities to joint warfighting operations", and references the JP 3-14 definition of space superiority as "the degree of control in space of one force over any others that permits the conduct of its operations…without prohibitive interference from terrestrial and space based threats."[10] This view may be Service centered, but if taken in context of historical naval doctrine theories, it can serve to support Lt Gen Kwast's recommended mission. Such history is, perhaps, appealing for those hoping the USSF takes on a maritime flavor for terminology.

At the height of the European powers' naval supremacy in the age of sail, needs for naval force were driven as much by economic purposes as they were for support of an army. The discovery of America was driven by economic motives and a search for a shorter passage to India. The prospect of new land, resources, and profit created a great power competition that included nations, pirates, and corporations. Indeed, the power of the British East India Company was substantial, at its peak it was responsible for half of Britain's trade, driving the need for its own army and naval power.[11] Today's corollary might be the likes of Amazon, Google, and SpaceX which, combined, are eclipsing the economic might of nations as they venture into the realms of cyber and space for profit. The significant economic potential of space beyond Earth's immediate sphere may be compared to exploration beyond the view of a nation's coastline. Using a naval analogy, space has been used for reconnaissance missions and as a line of communication in shallow sea lanes near land. This is equivalent to a littoral reconnaissance force with little to no self-defense capability and, therefore, is reliant upon support from nearby ports and in-range land forces to provide for its protection. Perhaps, this historic parallel is worthy of consideration when it comes to what USSF doctrine should look like in an environment of strategic competition. If USSF is to be viewed as its own combat arm and not a force support Service to air, land, and sea; perhaps, its capabilities should evolve to serve a mission similar to that of cruisers protecting economic commerce and lines of communication on the open sea, ultimately extending beyond littoral operations.

... An examination of Corbett's ideas serves as a framework that USSF doctrine can benchmark.

Consider Sir Julian Corbett's *Principles of Maritime Strategy*. An examination of Corbett's ideas serves as a framework that USSF doctrine can benchmark. Current space doctrine posits a primarily defensive mindset. Corbett states "counter-attack is the soul of defense. Defense is not a passive attitude… rightly conceived, it is an attitude of alert expectation". Perhaps, his more important contribution is the fallacy, "you can avoid attack by depriving yourself of the power of offense and resting on defense alone". This is a lesson learned by armies (static defensive trench warfare does not work) and air forces (destroying an enemy air force on the ground is more efficient than defensive counter air). Also, "a naval defensive means nothing but keeping the fleet actively in being—not merely in existence, but in active and vigorous life". Seemingly, this fleet-in-being concept is the current status quo of America's space capability. As such, a larger scope of mission and doctrine should be taken, and pursued aggressively, by the USSF.[12]

In Corbett's view, the whole object of naval warfare is to secure command of the sea or prevent the enemy from securing it, whether directly or indirectly.

Now, consider the multi-domain arena. It is no secret that space and cyber are intertwined. Further, since the physical infrastructure that supports space capability is now only terrestrial, they are subject to attack from physical domains or electronically attack delivered from any of those domains, including cyber. Such operations may cut a critical link in the chain of supporting effects needed to defend space capability. This view flips the roles such that air, land, and sea may become the *supporting* force while space becomes the supported force. Such doctrinal shift requires exploration.

Corbett provides plenty of additional framework ideas worth investigating. "Command of the Sea", he notes, "is not identical in its strategical conditions with the conquest of territory." In contrast, he says, the only right any nation might have on the sea is the right of passage. In other words, this is the equivalent of overflight and a means of communication that space currently holds as defined by international policy. Much like "international waters" beyond a nation's shorelines, perhaps space beyond geosynchronous orbit may be thought of as the open seas. Additionally, Corbett states "it is commerce and finance which now, more than ever, control or check the foreign policy of nations" which brings to his point that "over and above the duty of winning battles, fleets are charged with the duty of protecting commerce."[13]

Corbett's writing does not translate perfectly from the maritime realm to space. For instance, the idea that an enemy may "remove his fleet from the board altogether" to preserve itself from decisive defeat. Such "fleet-in-being" doctrine forces one's own maneuver and tactics along with those of the enemy. Unfortunately, that capability in space is very limited, and once removed from orbit, it cannot readily or economically be placed back on the board. However, he notes that ships are not confined by geography as readily as land forces; and, therefore, are not as predictable. This is not true of space-based assets given the current realities of orbital mechanics, lack of resupply on orbit, and miniscule maneuvering capabilities resident on most assets. In effect, once an object is in orbit, its future location is fairly easy to predict assuming orbital parameters are known. However, Corbett's assertion that "the narrower the sea, the easier it is to watch" may still apply. Everything in proximity to Earth is subject to space object surveillance and identification networks in place to watch them. If space commerce ever moves well beyond the moon, watching those movements could become significantly more difficult using terrestrial sensors alone, while time delays restricted by the speed of light grow with increasing distance.[14]

CURRENT DOCTRINE AND EARLY AIRPOWER THEORY

Looking to the past provides necessary lessons that need not be learned the hard way. Unfortunately in the case of airpower doctrine development, J.F.C. Fuller's statement came true: "To establish a new invention is like establishing a new religion—it usually demands the conversion or destruction of an entire priesthood".[15] Rapid technological change is an impetus for new military applications, and by extension, doctrine and theory for their use as well. A collection of essays by retired Air Force Maj Gen I.B. Holley Jr. discusses this interrelationship in his book: *Technology and Military Doctrine*. Unfortunately for early airpower theorists, the initial placement of the airplane into the Army Signal Corps in lieu of a combat arm itself relegated it, primarily, to reconnaissance use. Such "conversion or destruction" occurred when the US cavalry was supplanted by the airplane and combustion engine. That story is one Maj Gen Holley uses to relate his ideas from which we may learn.

Well before Corbett's writings, cavalry had become a critical combat arm of the land domain. It served four mission functions: the charge, reconnaissance, screen, and strategic attack that relied upon speed and maneuver to conduct attacks deep within enemy territory.[16] The critical enablers for these missions were the speed advantage cavalry held over other land forces and their ability to avoid deterrent forces as a result of short range, poor accuracy, and slow fire rate of muzzle-loading firearms used to oppose them. The airplane had better speed and threat avoidance, making it a logical successor to many missions carried out by cavalry troops. Unfortunately, although doctrinal use of the cavalry for such missions was well tested and defined, this logical succession and application of cavalry mission doctrine did not transfer to the airplane.

Since the Signal Corps was not a combat arm but a Service that supported the Army, its members viewed themselves as ancillaries that assisted the infantry, artillery, and cavalry in carrying out their tactical missions. This mirrors descriptions of assigning space assets to the Air Force to provide support to Army, Marine Corps, Navy, and Air Force missions. This treatment of the airplane resulted in misconceptions and poor strategic direction for its future (i.e., its uses and technological development). Similar to Corbett's outline of how the necessary composition of a fleet is mission driven to protect commerce, so too was the US airplane fleet affected in its early days. As a result of its placement in the Signal Corps: the 1920 record of Army aircraft acceptances shows nearly 1,000 reconnaissance aircraft in its inventory, with only 112 pursuit planes and 20 bombers.[17] Does the current space fleet have a similar composition based on how it has been viewed and organized by the armed Services and national leadership over the past five decades? If this trend holds true, the vector of near-term space doctrine is linked to what the USSF will become down the road, and vice versa. Holley concludes, "if we define our role in space as 'mission support' for operating forces, then will it not logically follow that the organization we build for space will be appropriate for a service or support role?"[18]

Some may ask, what happened to airpower doctrine? Well, as it was developed beyond World War I, the ideas of strategically bombing civilian and industrial centers took hold. This was tested at great cost of life and material in World War II's combined bomber offensives, notably, the idea that the bomber would always get through to its target. The task of formulating doctrine initially fell to the Air Corps Tactical School, while proponents such as Maj Gen "Billy" Mitchelland General "Hap" Arnold contributed in their struggle to develop and gain consensus on strategic airpower doctrines and form a separate air Service. Mitchell, regarded by some as the father of the Air Force, was famously court martialed during his antagonistic quest to form a separate air Service. Arnold, a Mitchell protégé and supporter during the interwar years, eventually became a five-star general and the Chief of US Army Air Forces upon its creation during World War II. After many years of such advocacy, the US Air Force became a separate Service in 1947, though its doctrinal heritage was already decades old.

"... we shall make as many mistakes in formulating space doctrine as we did with cavalry doctrine and airpower doctrine if we do not first get our house in order".[19]

Maj Gen Holley provides a profound warning: "we shall make as many mistakes in formulating space doctrine as we did with cavalry doctrine and airpower doctrine if we do not first get our house in order".[19] Getting our house in order means getting the best people which, in turn, may mean picking those whose ideas go against the grain, as in Billy Mitchell's case. Maj Gen Holley notes that "…the brash and barely respectful subordinate who is forever making waves by challenging the prevailing posture may prove to be the most valuable." Picking the right people is a necessary step toward getting the right doctrine, and calls for an informed and willing participation of many individuals. It is too important to be left to a handful of staff officers, especially those who are not passionate about the possibilities of a separate space force. Furthermore, the economic incentives for technological improvements from the American military-industrial complex means there will be no shortage of capability improvements. What economic (or otherwise) incentive is there for doctrine?[20] Doctrine and organization are intricately related to one another. With the stand-up of the USSF, the time for a new doctrine focus is now.

RECOMMENDATIONS FOR SPACE DOCTRINE DEVELOPMENT

While defining the core values and culture that make the USSF is the role of its leadership, history has shown doctrine and theory often generated itself at lower levels by tactical visionaries. Choosing the right people, processes, and place are key steps to success. The following are recommendations.

1. Choose tacticians with innovative ideas and a passion for pushing the envelope. Blitzkrieg and maneuver warfare theories came from experienced field-grade officers who later reached their fame at the flag officer level in World War II. Heinz Guderian was a communications officer before becoming the blitzkrieg genius who led mobile panzer units to swift victory in 1939 and 1940.[21] The right tacticians need not all come from a space background. Airpower theory, too, was driven by those at similar field-grade levels of experience. More recent US Air Force examples are Colonels John Warden and John Boyd. Warden, author of *The Air Campaign*, was known for developing the air attack plan on Iraq dubbed "Instant Thunder," and ultimately the basis for the airpower plan used during Operation Desert Storm. Boyd is best known for the creation of the Observe-Orient-Decide-Act (OODA) Loop, initially born from his dogfighting expertise while an instructor at the US Air Force Weapons School, he eventually taught his warfighting concepts at the US Marine Corps Command and General Staff College. Both individuals pushed the boundaries of their trade and the comfort level of their superiors. Services should handpick and delegate authority to officers from all warfighting domains who understand their Service's current tactics and doctrine, but also possess a drive for changing the status quo.

The right tacticians need not all come from a space background.

2. Write a doctrinal vision that transcends joint operations within the Earth orbit. A radical idea is that the USSF will reach beyond the near Earth environment. Much like the primacy and clout of British and Spanish naval power exceeding that of their armies, the USSF should envision operations well beyond the "shorelines" of Mother Earth. If the doctrinal status quo fails to change, the USSF will find itself the equivalent of a littoral naval fleet, useful only for operations near its base of origin. A "blue water" equivalent that extends well beyond Earth's influence will drive technological improvements needed to make such a vision a reality.

3. Make USSF doctrine the benchmark for new multi-domain doctrine. Space and cyber sit at the intersection of all joint, geographic, and functional combatant commands in the DOD. Furthermore, the space domain's integration and support to economic, political, and national intelligence organizations uniquely suit it for needed intergovernmental coordination required for true MDO goals. In some regards, such an important coordination function, beyond military use, may justify space as its own separate instrument of national power.

4. Doctrine developers in the USSF must first study and take note of past doctrinal failures and successes. The aforementioned doctrinal shift from cavalry to the airplane and the airplane to space for missions such as reconnaissance, screening, and deep interdiction provide valuable lessons. Doctrine developers chosen for this role should either possess a necessary historical and doctrine familiarity, be given that training as part of the task, or have with them experts in these fields to complete the task.

5. Service Chiefs and national leadership need to appropriately delegate authority to accomplish the mission. The job of the leaders is to organize, train, and equip Service members and civilian workers. Organizing with the right people for each task, providing them the resources and time needed to digest information away from their primary duties, and equipping them with the facilities or conference attendance are requisite to successful doctrine development. This is not to say that an equivalent to the Air Corps Tactical School needs to be created and funded. Rather, a gathering of personnel at a doctrine conference is a good first step, followed by iterative gatherings of invested personnel until a worthwhile working doctrine is produced. This is how most Air Force TTP documents are rewritten as new technologies get fielded and tactics improve. Revising doctrine

documents follows a similar model, but usually does not get the needed support or personnel because such personnel are prioritized for operational mission execution. In short, for doctrine development to succeed, it requires prioritization as a strategic imperative, even at a short-term cost of personnel needed for current mission execution.

6. Make the doctrine simple. If it is not simple, it will not be read, remembered, or understood by USSF personnel. This is the greatest pitfall of current doctrine across the Services, joint doctrine included. If senior leaders want their personnel to read and embrace the intent of its guiding documents, the doctrine must be easy to digest and align with the culture of the organization.

CONCLUSION

It is time to forge the USSF of 2030 and beyond. The force we have will look very different from the force we need if the USSF is asked to protect US commercial and economic assets beyond the near-Earth environment. Those who view this as unlikely or not worth the cost fail to see the threat and the potential for change in a strategic environment. In the event they are right, imagine the technological progressions that can still be applied to the near-Earth environment. This is no different than the second- and third-order gains reaped by the US as a result of the National Aeronautics and Space Administration's pursuit of putting a man on the moon. In the event they are wrong and the USSF takes their stance, the US will be at a significant disadvantage to those nations who do pursue such capability. Losing primacy on the high seas in the age of discovery spelled strategic decline for the Spanish, Dutch, and British governments and corporations like the British East India Company. If the US and allies want the strategic upper hand, the time to act is now.

Major Clayton W. Couch is assigned to Air Force Tactical Exploitation of National Capabilities (AF TENCAP) at Schriever Air Force Base, Colorado.

END NOTES

[1] Department of Defense. Summary of the 2018 National Defense Strategy of the United States of America. DOD website. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

[2] Tingley, Brett. "Recently Retired USAF General Makes Eyebrow Raising Claims about Advanced Space Technology." The Warzone website. December 11, 2019. https://www.thedrive.com/the-war-zone/31445/recently-retired-usaf-general-makes-eyebrow-raising-claims-about-advanced-space-technology

[3] Lt Gen Kwast, Steve. "Where the Space Force Must Go." Politico website. January 17, 2020. https://www.politico.com/news/2020/01/17/where-the-space-force-must-go-098884

[4] US Space Force Fact Sheet. United States Space Force Website. Accessed Mar 5, 2020. https://www.spaceforce.mil/About-Us/Fact-Sheet

[5] United States Space Command Fact Sheet. United States Space Command Website. February 26, 2020. https://www.spacecom.mil/About/Fact-Sheets-Editor/Article/1948216/united-states-space-command-fact-sheet/

[6] Joint Publication 3-14 "Space Operations." 10 April 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14.pdf

[7] McTigue, Kathleen. "Economic Benefits of the Global Positioning System to the US Private Sector." National Institute of Standards and Technology website. October 2, 2019. https://www.nist.gov/news-events/news/2019/10/economic-benefits-global-positioning-system-us-private-sector-study

[8] Space Resources Program page. Colorado School of Mines website. Accesed Mar 5, 2020. https://space.mines.edu/

[9] ESA Space Resources Strategy. ESA website. Accessed Mar 5, 2020. https://sci.esa.int/documents/34161/35992/1567260390250-ESA_Space_Resources_Strategy.pdf

[10] Annex 3-14 Counterspace Operations. Curtis E. Lemay Center for Doctrine Development and Education. 27 August 2018. https://www.doctrine.af.mil/Portals/61/documents/Annex_3-14/Annex-3-14-Counterspace-Ops.pdf

[11] Blakemore, Erin. "How the East India Company became the World's most Powerful Business." National Geographic website. September 6, 2019. https://www.nationalgeographic.com/culture/topics/reference/british-east-india-trading-company-most-powerful-business/

[12] Corbett, Sir Julian S. "Principles of Maritime Strategy." Dover Publications, Inc. Mineola, New York, 2004. Originally published by Longmans, Green, and Co., London and New York, 1911.

[13] Ibid.

[14] Ibid.

[15] Holley, I. B., Jr. Technology and Military Doctrine: Essays on a Challenging Relationship. Air University Press, Maxwell Air Force Base, AL. 2004. https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0093_HOLLEY_TECHNOLOGY_MILITARY_DOCTRINE.pdf

[17] Holley. Technology and Military Doctrine

[18] Ibid.

[19] Ibid.

[20] Ibid.

[21] Boyd, John R. "Discourse on Winning and Losing." Briefing Transcript, USMC Command and Staff College, Marine Corps University, MCB Quantico, VA. 25 April/2 May/3 May, 1989. https://static1.squarespace.com/static/5497331ae4b0148a6141bd47/t/5af842f8758d4615555d3f6d/1526219514965/Patterns+of+Conflict+Transcript.pdf

SIX MYTHS ABOUT OFFENSIVE CYBER OPERATIONS

Tech Sgt Kyle Hanslovan, center, a cyber-warfare specialist serving with the 175th Cyberspace Operations Group of the Maryland Air National Guard, works in the Hunter's Den (with unidentified Airmen)at Warfield Air National Guard Base, Middle River, Maryland, 2 December 2017. (Photo by JM Eddins Jr.).

By Lt Col Benjamin Ramsey, USAF and Mr. Robert Colletti

BACKGROUND

The Department of Defense designated cyberspace as its newest warfighting domain in 2011. Immediately thereafter, an academic debate over the practicality and nature of cyberspace warfare ensued, with many experts including cyber scholar, Marin Libicki, Chief Technology Officer at Human Rights First, Welton Chang, and author, Sarah Granger weighing in.[1] Academic objections to the acceptance of cyberspace as a warfighting domain did little to detract from the development and maturation of United States (US) Cyber Command. Nonetheless, misunderstandings continue to appear in academic articles about the nature of offensive cyber operations (OCO), in part because many aspects of OCO are secret due to operational requirements. As senior military leaders lobby for resources and policy makers struggle to fit OCO into the spectrum of international competition, both groups display an unintentional bias toward treating cyberspace as exempt from doctrine that applies to the physical warfighting domains. Misunderstandings of OCO and its effects are clouding the environment for decision makers. This article is intended to increase clarity for decision makers by debunking common myths about OCO.

MYTH 1: OCO DEVELOPMENT IS SWIFT AND EXECUTION IS VIRTUALLY INSTANTANEOUS.

Authors have, erroneously, characterized cyber operations as being nearly instantaneous (e.g., they travel "from one point on the globe to any other, in less time than it takes an average person to blink," or they "happen at the speed of light").[2] This is the non-kinetic equivalent of claiming the time between weapon release and impact is the speed of an airstrike. As with flight operations, OCO can last several hours and is the culmination of weeks, months, or years of gathering intelligence and developing capabilities. The preparation leading to effective OCO is never a "relatively short period of time".[3] Characterizing cyber effects as so rapid that "time, as it is traditionally understood in military affairs, has become irrelevant" at best inaccurate, hindering military leadership from appreciating the true challenges of executing these operations.[4]

Some military leaders have blamed the significant difficulties associated with executing OCO on limited authorities and oppressive bureaucracy. These leaders claim OCO would become "easy and quick" with few restrictions.[5] The reality is, the challenges associated with performing mission analyses, obtaining technical intelligence, and overcoming adversary defenses overshadow all legal and administrative obstacles that apply to OCO. Indeed, Joint Publication (JP) 3-0 recognizes that, "asymmetric attacks can be countered with well-planned joint operations synchronized with actions of interagency partners, international organizations, [nongovernmental organizations], multinational forces, and elements of the private sector."[6] This level of synchronization requires significant time to achieve.

An analogy to help understand the challenges associated with OCO is the raid on Osama bin Laden's compound on May 2, 2011 in Abbottabad, Pakistan. Military leaders did not simply "sprinkle Special Forces fairy dust" on the targeted compound in the way some military exercises "sprinkle cyber fairy dust" on challenging adversaries. In reality, the US collected vast quantities of intelligence about the targeted compound to provide military planners the greatest possible clarity. The special forces team that ultimately killed Osama bin Laden in his compound repeatedly practiced the raid against a full-sized compound replica in the weeks leading up to the mission. An abundance of intelligence collection and realistic mission training are likewise required for OCO to effectively engage an adversary.

MYTH 2: OCO IS THE DECISIVE "EASY BUTTON" DEPICTED IN ACTION MOVIES.

Military planners should avoid limiting their expectations of OCO as another means to achieve dramatic or explosive effects. A recent article describes an OCO that would overheat "a phone battery to cause a low-yield explosion." The author proposes this outcome could "neutralize" an adversary.[7] For this battery-based OCO to succeed, there are a series of criteria that must be met. The cyber operators must know the make and model of the target phone; have established access to the software on it; know, in real-time, when the adversary has the phone close enough for an explosion or fire to cause serious harm; and, most significantly, know there is a physical vulnerability in the phone that allows it to be exploded on command. Any of these criteria is difficult to achieve and, to count upon all four occurring simultaneously during combat, is foolish. A close examination of each of the criteria makes apparent the improbability of such a series of events.

Military planners should avoid limiting their expectations of OCO as another means to achieve dramatic or explosive effects.

The first criterion, that cyber operators know the exact make and model of the target phone through technical intelligence sources, is plausible. However, simple operational security (OPSEC) practices (such as using multiple phones) increase the required weight of effort. A knowledgeable and well-trained adversary could replace a phone frequently to avoid being tracked. This technique is well-known to criminals, as portrayed in the television show *The Wire*.

If intelligence sources are able to determine the exact phone make and model, the next situational criterion is access. This, too, is plausible through a number of avenues (such as a covert connection over a cellular network). Cyber operators would need to establish and verify access, check for system changes, and confirm the user's identity prior to mission execution. An adversary can dramatically increase the necessary intelligence efforts by keeping the phone powered off except for short periods of use or through other common OPSEC techniques.

An exploding phone can only cause damage or distract people within a small area, so mission success depends upon confirmation that the target phone is in proximity to the adversary. For example, a sniper could visually verify the target phone is in the adversary's hand and beside the adversary's head. However, this questions why the sniper would not be the weapon of choice in that scenario. A better option would be for the cyber operator to access the camera and acceleration sensors on the target phone to verify its proximity to the adversary, although this approach places an additional dependency on the previous two criteria.

Cyber operations require substantial resources to develop, test, certify, and sustain a capability ...

Finally, like many proposed weapon systems, the most difficult hurdle to overcome is resourcing. Cyber operations require substantial resources to develop, test, certify, and sustain a capability that must be continuously funded and operated by cyber specialists. As with any other kinetic weapon, the exploding phone technique would have to be tested many times to validate the weapons affect. Furthermore, the ecosystem of mobile devices is vast. With new hardware and software constantly emerging, it is unlikely the entire development cycle could be completed before the adversary's phone is upgraded or replaced.

If, somehow, all of these criteria were met, the effect is likely to be underwhelming. Although an exploding battery could cause burns or start a fire, the irony is that more people have died from swallowing coin-sized batteries than from exploding ones.[8] Since all commercially-available mobile devices face regulatory pressure to mitigate possible damages from battery failure, even the prospect of such a defect could rapidly drive a product off the market.

MYTH 3: ALL OF CYBERSPACE IS VULNERABLE TO FIRE-AND-FORGET "CYBER WEAPONS".

A 500-pound bomb will be just as destructive ten years from now as it was ten years ago and it is effective against many types of physical targets. Conversely, OCO mission success depends upon every aspect of the target configuration. Any changes in network topology, electromagnetic interference, passwords, software, or time of day have the potential to thwart OCO that required weeks, months, or years to develop. The misrepresentation of OCO as target-agnostic "cyber bullets, bombs, missiles, or intercontinental ballistic missiles," is counterproductive.[9]

In 2015 the US Air Force published an "Air Force Operating Concept" that described the possibility of the cyberspace equivalent of a heat-seeking missile by the 2030s.[10] Portions of the vignette are technically feasible, such as its description of fiber optic line tapping to gain access to a network "air gapped" from the Internet. Other aspects of the vignette are contradictory. For example, "fire-and-forget" malware that uses "highly autonomous logic" to automatically exploit an unexplored network cannot also produce "precise, predictable effects" because the target network and the autonomous actions of the malware are unpredictable.[11] The effects of releasing autonomous malware into an adversary's network could not be fully controlled, just as with the release of biological weapons.

Furthermore the vignette describes the ability of advanced malware to detain a pursued adversary in an elevator. It is technically possible for malware to stop an elevator from moving, perhaps, by disabling a building's electrical system. However, if a pursuit team already has access to real-time adversary location data, the ability to remotely detain the adversary in an elevator would be superfluous. Pursuing forces could cut power to a building more easily by using Soldiers or guided munitions than with advanced OCO.

It is unlikely that cyber operators, intelligence analysts, or intelligent malware could quickly map technical configurations of an elevator system, find a vulnerability, develop an exploitation, and produce the desired effect on command while tracking the exact location of the adversary. OCO will continue to require active human participation and ingenuity to be effective. Even today, the least complex OCO requires creative troubleshooting by well-trained teams to overcome unexpected obstacles within target networks.

MYTH 4: SOFTWARE AND HARDWARE HETEROGENEITY IS AN EFFECTIVE DEFENSE AGAINST OCO.

Authors that tout heterogeneity to protect key cyber terrain fail to account for the diversity of means by which cyber operators gain access. For example, the claim that "a heterogeneous network … cannot be completely taken down by a single vulnerability" is demonstrably false.[12] This misconception may arise from a narrow understanding of OCO effects as being the product of self-propagating malware, such as the Shamoon worm that disabled 30,000 Saudi Aramco computers in 2012.[13]

A software vulnerability is not necessary to gain unauthorized access into a target network. The numerous access methods for OCO include passwords garnered through social engineering, a vulnerable wireless access point plugged into a trusted network segment, and a co-opted insider. Once cyber operators gain access into the target network and establish administrator privileges, it does not matter whether the network uses one operating system or one hundred; the cyber operators can perform any activity on the network as easily as a fully-trusted administrator can.

Swift attribution of sophisticated OCO is risky due to the challenge of accurately identifying the hostile actor.

MYTH 5: OCO CAN BE DETERRED WITH THREATS OF AN IMMEDIATE RESPONSE.

Swift attribution of sophisticated OCO is risky due to the challenge of accurately identifying the hostile actor. A significant body of research concludes that "attribution is a critical issue that is difficult to overcome" in cyberspace.[14] For example, in a joint report the US and the United Kingdom highlighted a Russian-associated threat group that utilized Iranian-associated malware for their operations and hijacked ongoing Iranian operations for their own use.[15] Therefore, while a victim may have initially compromised by one threat group, an entirely different threat group can transform an otherwise covert operation into OCO.

Unidentified Marines with Marine Corps Forces Cyberspace (MARFORCYBER) Command pose for photos in the cyber operations center at Lasswell Hall aboard Fort Meade, Maryland, 5 February 2020. MARFORCYBER Marines conduct offensive and defensive cyber operations in support of United States Cyber Command and operate, secure, and defend the Marine Corps Enterprise Network. (Photo illustration by Staff Sgt Jacob Osborne, USMC)

Additionally, numerous significant OCO have taken place against diverse targets (such as military satellites, political candidates, universities, and supermarkets) that remain unattributed to this day. Cyber operators took control of the Roentgen Satellite astronomy platform and rendered it permanently useless in 1998, and also held a SkyNet military satellite hostage in 1999. To date, both groups of cyber operators remain unknown.[16] Similarly, OCO that caused a half million dollars in damage to the National Aeronautics and Space Administration's Maryland offices in 1989, took control of the CBS News homepage in 2003, and disabled South Korean broadcast networks and banks in 2013 remain unattributed.

JP 3-0 states "deterrence prevents adversary action through the presentation of a credible threat of unacceptable counteraction" and goes on to assert that "ideally, deterrent forces should be able to conduct decisive operations immediately."[17] To maintain deterrence a response generally must be swift. However, hasty attribution and rapid retaliation necessitates that a decision maker is willing to risk punishing the wrong actor. A quick strike against the incorrect actor would undermine deterrence by demonstrating a clear inability to accurately attribute OCO.

MYTH 6: A STATE CAN DETER OR COMPEL AN ADVERSARY STATE USING ONLY OCO.

Thomas Shelling's work, *Arms and Influence*, describes two forms of coercion: deterrence (passive coercion) and compellence (active coercion).[18] A large body of research on the nature of cyber deterrence finds that, without "reliable models to assess the relative strength of different states' offensive cyber capabilities or estimate the effects of [OCO], the concept of deterrence stability makes little sense in cyberspace."[19] At least two conditions required for deterrence are impractical using covert OCO: the threat must be communicated accurately to the target and the target must clearly understand the threat.[20] A vague threat of consequences in, and through, cyberspace cannot be an effective deterrent. The exact effects of an OCO are nearly impossible to quantify, even for a sophisticated attacker. Furthermore, if the adversary state knew what key cyber terrain the US held at risk and understood what the generated effects would be, the adversary could neutralize the threat with focused cybersecurity measures. A rational course of action for the adversary state would be to commit the necessary resources, up to the expected cost of the threatened effects, to secure its cyber terrain and nullify the threat. It is far more cost effective to remediate a cyberspace vulnerability than to develop an effective OCO based on a vulnerability.

The outlook for cyber compellence is similarly doubtful. Historical attempts at compellence using only OCO reveal a pattern of ineffectiveness. Among the first attempts at OCO compellance were the unprecedented, distributed denial-of-service attacks against Estonia's government, banking, and news broadcasting networks in 2007.[21] The OCO was significant in scope and enacted in response to Estonia's plans to relocate the remains of a Soviet World War II memorial. Not only did the OCO fail to influence Estonia's decision to relocate Soviet graves and a prominent statute, it also led to the creation of the North Atlantic Treaty Organization Cooperative Cyber Defense Center of Excellence in Estonia the following year.

Similarly, a Russian OCO against the Ukrainian power grid in December 2015 served as a proof-of-concept and a coercive act.[22] This OCO required "many months" of disciplined intelligence gathering and tool development, yet was only able to cause a six-hour disruption of electrical service for less than one percent of the Ukrainian population.[23] As a comparison, the average electrical service outage following a winter storm in the US states of Vermont and Maine are 15 and 42 hours, respectively. These examples demonstrate that OCO, by itself, has failed to be perceived as "an unacceptable risk to the adversary's achievement of objectives."[24]

While "deterrence and compellence are marginal as pure actions in cyberspace," doctrine offers an alternative.[25] JP 3-0 explains that "[special operations forces] contributions can provide operational leverage by gathering critical information; undermining an adversary's will or capacity to wage war; and enhancing the capabilities of conventional US, multinational, or indigenous/surrogate forces."[26] OCO can provide many similar options to commanders, but should only be applied toward deterrence as part of multi-domain approach.

CONCLUSION

It is imperative the US and its allies approach the application and maturation of OCO as rigorously as they approach novel missions in the physical warfighting domains. The first step toward self-improvement must always be an honest appreciation of reality, as faulty assumptions often lead to faulty solutions. This article describes some common misconceptions about OCO that are counterproductive to informed decision-making. Knowledgeable cyberspace operations professionals must do more to share their insights, at the unclassified level, with the general public. Only then can policy advisors and academics accurately debate OCO limitations and opportunities in service to national security.

Lt Col Ramsey is a Branch Chief in the Operations Directorate of US Cyber Command.
Mr. Colletti is a Future Operations Planner in the Operations Directorate of US Cyber Command.

END NOTES

[1] Martin C. Libicki, “Cyberspace Is Not a Warfighting Domain”” RAND Corporation, 2012, https://www.rand.org/pubs/external_publications/EP51077.html; Welton Chang and Sarah Granger, “Warfare in the Cyber Domain”, *Air and Space Power Journal*, Fall 2012, http://www.airpower.au.af.mil/apjinternational/apj-s/2012/2012-3/2012_3_10_chang_s_eng.pdf.

[2] Martti Leho, “The Modern Strategies in the Cyber Warfare,” in *Cyber Security: Power and Technology*, eds. Martti Lehto and Pekka Neittaanmaki (Switzerland: Springer International, 2018), 7; Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), 30-31.

[3] Ibid, 25.

[4] Ibid.

[5] James E. McGhee, “Liberating Cyber Offense”, *Strategic Studies Quarterly*, Winter 2016, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-10_Issue-4/McGhee.pdf.

[6] Office of the Joint Chiefs of Staff, “Joint Publication 3-0: Joint Operations”, 22 October 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910.

[7] Jennifer Phillips, “Tactical Maneuver in the Cyber Domain”, *Joint Force Quarterly*, no. 93 (2nd Quarter 2019):19, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-93/jfq-93.pdf

[8] US Fire Administration, “Electronic Cigarette Fires and Explosions in the United States: 2009-2016”, FEMA, July 2017, https://www.usfa.fema.gov/downloads/pdf/publications/electronic_cigarettes.pdf; Alex Horton, “Vape Pen Kills Man After Exploding In His Mouth”, *The Washington Post*, 5 February 2019, https://www.washingtonpost.com/health/2019/02/05/vape-pen-kills-man-after-exploding-his-mouth/; Asher Fogle, “Toddler Dies After Swallowing a Button Battery”, *Good Housekeeping*, 6 January 2016, https://www.goodhousekeeping.com/health/news/a36283/toddler-death-battery/.

[9] David E. Sanger, “US Cyberattacks Target ISIS in a New Line of Combat”, *The New York Times*, 24 April 2016, https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[10] US Air Force, “Air Force Future Operating Concept”, (September 2015):31, https://www.af.mil/Portals/1/images/airpower/AFFOC.pdf

[11] Ibid.

[12] William D. Bryant, “Resiliency in Future Cyber Combat”, *Strategic Studies Quarterly*, Winter 2015, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-09_Issue-4/Bryant.pdf

[13] Nicole Perlroth, “In Cyberattack on Saudi Firm, US Sees Iran Firing Back”, *The New York Times*, 23 October 2012, https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

[14] David D. Clark and Susan Landau, “Untangling Attribution”, *Harvard National Security Journal*, Vol. 2, No. 2 (2011), 25-40.

[15] National Cyber Security Centre, “Advisory: Turla group exploits Iranian APT to expand coverage of victims”, 21 October 2019, https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims.

[16] Patrick Tucker, “The NSA is Studying Satellite Hacking”, Defense One, 20 September 2019, https://www.defenseone.com/technology/2019/09/nsa-studying-satellite-hacking/160009/.

[17] Joint Publication 3-0: Joint Operations”, 22 October 2018

[18] Thomas Shelling, “Arms and Influence”, New Haven, CT: Yale University Press, 1966.

[19] Edward Geist, “Deterrence Stability in the Cyber Age”, *Strategic Studies Quarterly*, Winter 2015, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-09_Issue-4/Geist.pdf.

[20] United States Air Force, “Doctrine Annex 3-0: Operations and Planning”, 4 November 2016, https://www.doctrine.af.mil/Portals/61/documents/Annex_3-0/3-0-D15-OPS-Coercion-Continuum.pdf.

[21] “Hackers Take down the Most Wired Country in Europe”, *Wired*, 21 August 2007, https://www.wired.com/2007/08/ff-estonia/.

[22] Quentin E. Hodgson, et al., “Understanding and Countering Coercion in Cyberspace”, RAND Corporation, 2019, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2961/RAND_RR2961.pdf.

[23] Kim Zetter, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid”, *WIRED*, 3 March 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[24] Joint Publication 3-0: Joint Operations”, 22 October 2018

[25] Gartzke, 59.

[26] Joint Publication 3-0: Joint Operations”, 22 October 2018

THE J26 COLLECTION MANAGEMENT COURSE CURRICULUM REVAMP AND CERTIFICATION PROGRAM FOR THE INTELLIGENCE COMMUNITY AND JOINT FORCE

Unidentified Kosovo Force Regional Command East United States Soldiers, along with members of Torres Advanced Enterprise Solutions, bag evidence found during a site exploration exercise at a training facility in Ferizaj, Kosovo 15 October 2019. The site exploitation course teaches students how to acquire information about an enemy. Whether it is cell phones hidden in a wall or maps found in a desk, site exploitation class attendees receive the skills needed to go in and find information. (Photo by Sgt Patrick Kirby, USA)

By Maj Douglas Wietlisbach, USAF

The Joint Staff and the Defense Intelligence Agency (DIA) are hard at work meeting the collection management (CM) training and certification demands of today's warfighter and combatant commander. Historically, collection managers were assigned their role with little, if any, training or experience in the various aspects of CM, various DOD reviews and reports noted this discrepancy. To rectify this current shortfall, DIA offers training courses and an accredited certification program.

Students gain knowledge through experiential learning activities and discussions designed to support key enterprise learning objectives.

DIA offers the Collection Management Basic Course (CMBC), a 2-week classroom experience consisting of a fundamental overview of CM tasks, roles, and relationships of collection managers within the context of the Joint Intelligence Process (JIP). Students gain knowledge through experiential learning activities and discussions designed to support key enterprise learning objectives. Course materials include concepts applicable to all echelons, from the tactical to the strategic levels. Classroom engagements support the student's visualization of broad concepts, including: the joint intelligence process, how intelligence requirements become collections requirements (CRs), the CR lifecycle, and the various CM relationships in the Defense Intelligence Community.

Additionally, students participate in simulations demonstrating the five major CM functions: writing CRs, collection strategy architecture, selection of assets, development of collection plans, and discovery of CM improvements through assessments. This is accomplished via a building-block approach and success of the student depends upon learning the various concepts of Collections Requirements Management, the intelligence disciplines, and systems of record (such as CRATE, PRISM, and COUGAR).

DIA also offers the Collection Management Intermediate Course (CMIC), which is the follow-on course from the CMBC.

DIA also offers the Collection Management Intermediate Course (CMIC), which is the follow-on course from the CMBC. Currently, this course is being revamped by the Academy for Defense Intelligence (ADI) to update the curriculum and better align its learning objectives with the recently approved joint training standards. The first CMIC course iteration took place in June of 2020 at DIA, with mobile training teams brings the program to offsite locations after ADI determined the instruction meets all course objectives. CMIC is designed to expound upon the CMBC instruction, taking the foundational knowledge to the next level by giving the student more in-depth knowledge on proper communication functions; intelligence discipline-specific intelligence, surveillance, and reconnaissance assets; and assessments. Students test their knowledge with a capstone exercise integrating their CM knowledge and abilities by going through a computer-generated scenario simulating what a collection manager will experience in crisis operations.

Also on the horizon is the Collection Management Advanced Course (CMAC), being developed through the collective efforts of Training, Tradecraft, and Certification (J2621) and a dedicated panel of subject matter experts (SMEs). The impetus of this course is to fill a requirement to ensure collection manager leaders understand the role and training requirements of their subordinates and ensure leadership has the training and knowledge to effectively and efficiently execute their role. This course is envisioned for the DIA civil service grade GG-14 and the projected course length is 3–5 days, depending on the feedback from the SME panel and the needs of the students. The projected implementation of this course is set for 2021. The Certified Collection Management Professional-Fundamentals (CCMP-F) program is part of a DOD-wide initiative to bring the intelligence workforce to a professional level. The Undersecretary of Defense for Intelligence directed the development of professional certification programs to ensure an integrated, agile intelligence workforce that can meet the intelligence community's needs in a dynamic environment. Its purpose is to develop, define, and measure broad-based core competencies for CM professionals across the Defense Collection Management Enterprise (DCME). The DCME includes all agencies, Services, and combatant commands involved in Defense Collection Management.

The knowledge required to pass the certification exam from the Essential Body of Knowledge (EBoK) will enhance intelligence professionals, regardless of discipline.

The CCMP-F was developed by, and for, collection managers. The vision is to develop a CM workforce of certified professionals through: establishing a common lexicon of terms for CM professionals, maximizing the capability of these professionals to work in a multi-international environment, and allowing these CM professionals to apply their skills and knowledge to operations at all echelons. This certification program is open to all civilians, military members, and contractors, especially those that work with CM. However, a CM background is not required. The knowledge required to pass the certification exam from the Essential Body of Knowledge (EBoK) will enhance intelligence professionals, regardless of discipline.

Individuals who are interested in the program can log into https://dodcertpmo.defense.gov/CollMgmt, on an unclassified system, for the most up-to-date information. The test is a proctored and contains 100 multiple-choice questions and takes place in one of 17 worldwide exam facilities. The questions on the test are generated from the EBoK, which is online for viewing/printing. Those interested may pick up a hard copy at the office located in DIA headquarters. The key to passing this test is to study the EBoK, and think of this exam as retaking a driver's license exam. Most people have a valid driver's license and operate vehicles coherently enough to use them when needed, but how many people remember all of the rules and guidance listed in the licensing manual? How far should one park from a fire hydrant? When is a turn right on red permissible? What are all of the rules on passing a school bus? Those who want to pass, better study! The current pass rate is 49%. Those who study an average of 20 hours have a much higher success rate than those who study less. Those who pass are certified for two years and may renew using one of two routes: retake the exam or submit a log of 100 professional development units (PDUs). PDUs document students' continuing education and learning in the field of CM and all PDUs tie back into the knowledge, skills, and abilities listed in the EBoK and tested in the exam.

There are several benefits to becoming a certified member, and the one that applies to all certificants is the post nominal students earn. It is a definitive delineator that says, the person entitled to display it has taken the only peer-reviewed testing medium overseen by a psychometrician and, therefore, has a solid foundation. (A psychometrician is a doctor in the field in psychology and education who is devoted to testing, measurement, assessment, and related activities.)

For enlisted military members, there are defined benefits for gaining this certification via the Credentialing Opportunities On-Line program. The United States Army grants 40 promotion points for enlisted members who become certificants, and the other Services have displayed various degrees of credence and reciprocity.

These are the current offerings for CM and J2621is striving to expand and expound its offerings and portfolio. There appears to be a "one and done" implementation schema when it comes to CM, and while force development and the desire to broaden the experiences of intelligence professionals may drive this pragmatic approach, everyone is strongly encouraged to examine CM principles and practices. The processes and lessons learned in CM contribute to the effective prosecution of the JIP and the assessments are often overlooked aspects that are keys to a unit's success. Leaders cannot improve their unit or processes without measuring themselves with validity and accuracy. This is just one of the many benefits inherent in CM and will enhance a person's ability to support the mission whether directly involved in CM or not.

Maj Douglas Wietlisbach is an Air Force officer serving as the Branch Chief for J2621 and the functional manager for CM at the DIA. His main responsibilities are training, doctrine, and policy.

HAVE QUICK AT SEA—LESSONS LEARNED THE HARD WAY

A United States Navy F/A-18E Super Hornet, assigned to the "Tomcatters" of Strike Fighter Squadron (VFA) 31, flies above the aircraft carrier USS Theodore Roosevelt (CVN 71) 27 February 2020. The Theodore Roosevelt Carrier Strike Group is on a scheduled deployment to the Indo-Pacific. (Courtesy photo)

By LCDR Matthew Quintero

Adversaries have long held the ability to thwart or exploit the United States (US) military's tactical communications. Today, technologies to find and jam frequencies in the ultra-high frequency (UHF) spectrum are becoming cheaper to produce and distribute. This capability not only allows enemies to jam US transmissions, but it allows them to find, fix, and target US forces. Use of proven anti-jam technologies, such as Have Quick (HQ), is mandatory for tactical air communications in joint operations. The need for anti-jam technology was articulated in the 2004 Air Land Sea Application (ALSA) Center "Have Quick" multi-Service tactics, techniques, and procedures publication (MTTP):

"Joint and combined operations mandate the requirement for the exchange of voice information among and between forces. The fielded capabilities of the HAVE QUICK (HQ) radio have been effective in providing securable, low probability of intercept/electronic attack voice communications in the anti-jam mode for the implementing forces."

Adversaries have long held the ability to thwart or exploit the United States (US) military's tactical communications.

HQ I was introduced in the 1980s. It provided a slow, frequency-hopping capability for UHF, line-of-sight, voice communications. About a decade later, HQ II provided additional anti-jam protection, improved frequency hopping algorithms, and faster hopping over an expanded range of frequencies. Currently, HQ II is the most widely used form of joint anti-jam, voice, line-of-sight communications.

HQ does not entail voice encryption and is not a secure radio. However, HQ does require cryptography to set its hopping algorithms. Only participants using the same crypto can hear a coherent transmission. Every day a new crypto segment is used to create the word of day (WOD). Afterwards, the user must set a time of day (TOD). Two users attempting to communicate must have the same TOD and WOD set into their radios. This is easier said than done. Preparing a force for HQ communications requires dedicated planning and practice. The 2004 publication understated this notion. It stated:

> *"For effective use of the HQ radios on the modern battlefield, planners must develop a communications plan that ensures successful employment of the HQ radio in a joint environment."*

As the Carrier Air Wing ELEVEN Communications Officer during the Nimitz Strike Group's 2016-2017 workups and deployment cycle, I became the de facto subject matter expert for HQ radios. During that experience, I found some important HQ knowledge was corporate and much had been lost since it debuted in the 1980s. This article recounts lessons learned by the carrier strike group team in using HQ radios. Those lessons tell of hundreds of wasted man-hours in an attempt to use a "training crypto" known as KAL-269. Finally, I will provide suggestions for improving future ALSA HQ publications.

HOW AN AIRCRAFT CARRIER SETS UP RADIOS

It is important to know how a HQ radio is set up on US ships to understand why it is such a chore for the Navy to get HQ right. When shipboard operators sit down to talk on a radio, they pick up a handset and dial in a two-digit number to select the communications network they want. They are not changing a radio frequency; instead, they are patching into a radio which always has a certain frequency set. Serving the UHF spectrum, these radios are 1970s-era WSC-3s. At any time, only around twenty of these radios are operational. Of the twenty, only a few have the modifications required to make them HQ capable, of which only one or two operate consistently.

The bank of WSC-3 radios are kept in a room in the mast to minimize the distance from the radios to their antennas. Personnel trained as information systems technicians (ITs) are tasked with setting up and maintaining the WSC-3s. Rarely are the ITs trained on the radios' purpose or how to talk on them. The WSC-3s are connected by hundreds of yards of wires down to the center of the ship where they are "patched". The "patch room" contains a wall of round dials that correspond to every radio which is assigned a network number. Miles of cables connect hundreds of user handset terminals throughout the ship to the patch room. On those handsets are usually personnel trained as Operations Specialists (OSs). OS Sailors are trained to talk on the radios and control ships and aircraft but are not trained on how to work the radios. At a couple of stations on the carrier, the OS Sailors control a small panel that allows them limited remote control of the HQ-enabled WSC-3, only. With this panel they can switch between 20 preset networks (including HQ networks), take the radio in and out of HQ mode, and initiate or receive a HQ TOD signal. A TOD signal may be referred to by the Brevity term MICKEY.

Setting up HQ on the WSC-3 is a tedious process where codes and frequencies must be hand rolled in one by one on the terminal face and various switches turned on and off in a specific order. If a radio fails to enter HQ mode, the process must be repeated. Once the radio is set, the TOD must be synchronized among all participants in the HQ network. This is a tedious endeavor.

... most WSC-3 radios on ships still require an over-the-air (OTA) TOD to synch with the network.

TIMING IS EVERYTHING

Most Navy aircraft built in the post-Global Positioning System (GPS) era can use a GPS TOD for HQ. Unfortunately, most WSC-3 radios on ships still require an over-the-air (OTA) TOD to synch with the network. Getting an OTA TOD into a WSC-3 is difficult. In theory, the OS with the remote-control panel can hail an aircraft using GPS, request a

TOD, and be done. In actuality, somewhere along the convoluted cable path from user to radio, the time signal incurred enough distortion to unsynch the radio's TOD. OTA synchs could only be effective using the switches on the radio itself. This process required ITs to go out of their comfort zones and talk directly to aircraft when new TODs were required.

I brought a senior IT into an E-2 Hawkeye and showed him an ARC-210 radio and how quickly I could hail an aircraft, switch frequencies, coordinate a MICKEY, switch to HQ, and get a good check. The concept clicked, and this paid dividends for the rest of the deployment. The technically savvy IT was had been hamstrung by a "stay in your lane" mentality. He just needed someone to empower him to do what was required to accomplish his mission.

HQ does not time synch like the Joint Tactical Information Distribution System (JTIDS).

On the topic of timing, there is a misconception that should be addressed. HQ does not time synch like the Joint Tactical Information Distribution System (JTIDS). Synching one radio with another does not mean synching with all radios. On several workup cycles and deployments, I have seen the same argument arise as the ships and aircraft come together and work through HQ growing pains. The ships will achieve good HQ checks and not be able to talk to aircraft.

Conversely, the aircraft will have good checks with each other but not with the ships. Then, the blame game begins, however, they are both right and wrong. Usually, the ships are able to synch with each other using a "distorted" GPS TOD, or (more likely) by forcing their radios to produce a TOD based on no external inputs. That type of TOD is known as an emergency TOD. The ships then work hard to pass this emergency TOD on to the other ships in their group, and they will all synch. Aircraft, on the other hand, will use the GPS self-TOD capabilities of their newer radios almost exclusively. As stated in appendix I of the 2017 ALSA *Tac Radios MTTP*, "airborne platforms…have limited on-station time". So they may not be keen to work out HQ timing issues with surface units for an extended period. This lack of coordination often results in two networks on two different time synchs.

Underscoring these sentiments, a ship commander asked me, "if we are synching with each other (ships), why aren't we all synching up?" Therein is the issue. After explaining how it "didn't work like JTIDS," the follow-on question was, "Why don't we just have the aircraft synch to our time?" This would have worked for the carrier strike group but would have been a poor solution for participation in the joint environment on deployment. Owning the problem should be the first step in HQ troubleshooting.

THE KAL-269 CALAMITY

For HQ training inside the continental United States (CONUS), the joint air forces are proficient with HQ II frequency management training (FMT) mode. I have worked with US Air Force airborne warning and control systems (AWACS) and fighters using FMT many times. Setting up FMT does not require crypto; it is merely an exercise in synching time signals. In preparation for deployment, the Nimitz Strike Group's air defense board decided to train using KAL-269 CONUS crypto. We cracked open our ALSA MTTP publications, saw mention of KAL-269, and decided this would provide better training. The assumption was KAL-269 would be KAL-9200 (HQ II operational crypto), basically, but OK for CONUS use. This was a poor assumption.

The strike group went down a rabbit hole, for about two months, in attempting to use KAL-269. The ALSA MTTP for *Tac Radios* does not explain using KAL-269 in depth, other than for CONUS. This is because it is very seldom, or never, utilized and its use has been forgotten. Once the strike group came up with the good idea of using KAL-269, it immediately ran into hurdles. I worked directly with the strike group communications staff who had no experience with HQ or KAL-269. Additionally, the regional vault serving the ship's Electronic Key Management System (EKMS) local element had no experience with HQ or KAL-269 material, as it had never been requested. It took a much longer than normal time for the actual tape canisters, containing the HQ and KAL-269 material, to be located and shipped out to the carrier.

After receiving the KAL-269, we had a

problem with how to distribute the WOD to the other ships and aircraft. The ALSA *Tac Radios* MTTP says:

"(4) The following policies apply to distributing, reproducing, and using KAL-269 WOD segments:

(a) The KAL-269 is distributed through COMSEC [communications security] channels. After reaching the unit level, treat the KAL-269 in accordance with Service regulations.

(b) Reproduce KAL-269 at the unit level (as necessary)."

On the other hand, The National Security Agency (NSA) produces and distributes the KAL-269. In the process of obtaining this obscure material, we had direct communications with the NSA office responsible for it. Their representative made it clear that under no circumstances were we to print copies of COMSEC for distribution, including KAL-269 material. We now had two different sources telling us two different things. The strike group erred on the side of caution, which made transmission difficult as codes had to be transmitted to aircraft and ships by an alternate means every day.

In this effort, I trained hundreds of aviators and ship technicians to handle KAL-269. Weeks later, the carrier received the can of tape. Finally, it was game day, and we put in the KAL-269. The results were underwhelming. It took us only a few minutes to realize KAL-269 was nothing but HQ I training network WODs. HQ I training was significantly inferior to HQ II FMT network training. As described in the 1991 Joint Publication (JP) 6-06.1 Joint Have Quick Planners Guide publication, it is "training WOD", and it provides the users with five training networks (T-nets). This was an exercise in requesting, distributing, and loading COMSEC for the sake of requesting, distributing, and loading COMSEC. This process seemed to go against the spirit of the EKMS in that we had no reason to have these codes on hand. With that argument, the strike group quickly abandoned their KAL-269 plans. We continued to use FMT networks for training.

On my recommendations, the air wing commander was able to convince the strike group that KAL-269 provided a negligible training benefit to the strike group. Furthermore, we risked mishandling crypto for insignificant training benefits. If the ALSA publication had spelled out that KAL-269 was training WOD that provided the five HQ I T-nets, we would have never spent two months chasing our tails. It seems these facts have slowly been taken out of the governing publications since 1991. The ALSA Tac Radios publication dated 2017 states:

"The KAL-269 (CONUS WOD) is used in CONUS, as defined by the Joint COMSEC Management Office."

ALSA "Have Quick" 2004 states:

"KAL-269, (CONUS WOD), is used in CONUS, as defined by the Joint COMSEC Management Office. Ordering instructions are contained in COMSEC Material System-21."

JP 6-06.1 states:

"KAL-269, 'Continental United States (CONUS) Training WOD,' is used for training in CONUS. Ordering should follow what is given in appendix B."

... T-Nets and FMT-Nets are two different things.

My final lesson is, T-Nets and FMT-Nets are two different things. When trying to explain to commanders that KAL-269 was only providing "T-Nets", they would often confuse that with "FMT-Nets" that do not require COMSEC. The ALSA publication does a good job of breaking out the HQ I and II capabilities when it comes to "training networks", but it may need to spell out, specifically, that not all T-nets are the same. In my experience both ship-drivers and aviators like to refer to HQ II FMA-nets as "A-nets" and HQ II FM-nets as either "Training networks or T-Nets."

RECOMMENDATIONS

1. Bring back "Appendix C USN CVW 17 Have Quick II REFERENCE CARD USING AN/ARC-182 RADIO" from the 2004 ALSA "Have Quick" MTTP.

I have personal experience now with

ARC-182, ARC-210, and WSC-3 radios. The ARC-182 HQ setup process is almost identical to the WSC-3 HQ setup. Having served in two Carrier Air Wings (CVWs), the document can easily be renamed to a universal "USN CVW Have Quick…" reference. While this document seems Service specific, I guarantee it would have benefits for our sister Services, especially the Air Force. The guide is a reference for aviators and surface operators to speak the same language. Lessons gleaned from this document could help multiple Services understand where their differences lie. On the carrier, I was able to print off Appendix C and provide to OS and IT Sailors. This guide allowed operator and technician cross-training. Expanding this guide to include modern ARC-210 type radios would improve it even further.

2. Continue the trend of "operator-ization" of the Have Quick section of ALSA Tac Radios.

ALSA updated the guides for HQ and removed much of the technical bloat which made them more operator friendly. When it comes to network types and timing considerations, a few more words expanding these concepts would have been appreciated. The trend, since the introduction of HQ II, has been to describe the capabilities of HQ II by first explaining the capabilities of HQ I. For example, appendix J of Tac Radios breaks down "Basic HQ I NETs" into A-nets, B-nets, and T-nets. Further down the page, it breaks "HQ II NETs" into FMA-nets and FMT-nets. It took me a long time to figure out that T-nets are not FMT-nets and A-nets are not FMA-nets. With all the current WSC-3s being HQ II capable, I seriously doubt there are any users of pure HQ I in the Joint Forces. Instead, I recommend re-categorizing the network types from HQ I and HQ II to "training" and "anti-jam" nets, and under those titles list out T-nets, FMT-nets, A-nets, and FMA-nets. I believe this simple rewording can allow operators to better understand these concepts.

As joint forces continue to procure interoperable and self-synching networks, the rudimentary nature of HQ TOD must be emphasized.

As joint forces continue to procure interoperable and self-synching networks, the rudimentary nature of HQ TOD must be emphasized. Synching with one does not mean synching with all. All units must have the same TOD and it must be from a GPS time source. The emergency TOD is an extremely useful function, but it often allows the uninformed to think they are set up correctly. These concepts may need emphasis in future versions of ALSA MTTP publications.

3. Explain T-NETS and KAL-269.

The risk of requesting and handling obscure COMSEC was not worth the reward of five T-nets. ALSA and joint publications were our references in this endeavor, as there was no corporate knowledge available on KAL-269. Somewhere, the part about KAL-269 being a "training" crypto was removed from the ALSA publication. The ALSA publication should have explicitly said, "KAL-269 provides five HQ I T-nets". I think this knowledge was lost since HQ I first rolled out in the 1980s. For that reason, HQ II FMT training is the only "CONUS" use of HQ that has occurred for many years. FMT-nets provide a much more useful way of training ship operators and aircrew in setting up HQ and synching TOD. We learned all of this the hard way. Clarification in future ALSA publications may save others from a lot of wasted time.

FIGHTER INTEGRATION (FI) MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES (MTTP) MCRP 3-20.0/NTTP 3-22.6/AFTTP 3-2.89

Air Land Sea Application Center released the newest revised version of FI in June. The purpose of the FI MTTP is to provide the warfighter a single-source set of integration standards intended to enhance commonality when operating with multiple types and models of fighter aircraft from across the Services. It establishes baseline intercept contracts with the associated communications plan, bringing cohesion to the battle problem.

An F-35B Lightning II takes off from the flight deck of the USS Wasp (LHD-1) during flight operations 22 May 2015. (Photo by Cpl Anne K. Henry, USMC)

The FI MTTP publication addresses air-to-air operations that are not mission specific. Fighter aircraft types include F-15C/E, F-16, F-18A-F, F-22A, and F-35A-C. This publication establishes standards for basic FI execution. The summer 2020 release updates participating platforms, aircraft community standard operating procedures, and communication plans.

The FI publication is classified SECRET and can be found on ALSA's SECRET Internet Protocol Network portal (noted in the back of this bulletin) and Services doctrine portals.

JOINT ALL-DOMAIN OPERATIONS (JADO)

ALSA's top research priorities are JADO and joint all-domain command and control (JADC2). The purpose of this research project is to follow the Services as they begin to develop joint, integrated, all-domain solutions to provide operational and tactical warfighters agile and resilient operational and battle management capabilities. The scope of the research includes near- and mid-term efforts to develop capabilities at the operational level and below. Future JADO capabilities will build the capability to synchronize hundreds of kill chains in multiple hours, regardless of domain or functional ownership.

Each Service is contributing to build JADO capabilities by holding joint working groups, planning conferences, and operational vignettes. As the Services continue to work together on a joint solution, ALSA will be there to capture emerging tactics, techniques, and procedures as they are established.

The Chennault Events, led and hosted by the Curtis E. LeMay Center for Doctrine Development, and Education (LeMay Center), is a good example of how the Services are integrating. The wargaming events took place in December 2019 at the LeMay Center and participants were from each Service and some coalition partner countries. The purpose of the games was to test and refine the Air Force's concepts in each domain, working as a Joint node able to complete distributed kill chains. The series culminated in the release of Annex 3-1, Department of the Air Force Role in Joint All-Domain Operations, in June 2020. In addition, the Army's Combined Arms Doctrine Directorate continues to work with Army Futures Command to pull Joint all-domain ideas into Army doctrine as they undergo experimentation and validation.

Let ALSA know where we can get involved.

CURRENT ALSA MTTP PUBLICATIONS

AIR AND SEA BRANCH–POC alsaA@us.af.mil

TITLE	DATE	PUB #	DESCRIPTION/STATUS
ACC *Multi-Service Tactics, Techniques, and Procedures for Air Control Communication* **Public Release**	14 FEB 20	ATP 3-52.4 MCRP 3-20F.10 NTTP 6-02.9 AFTTP 3-2.8	Description: This publication provides MTTP for the control and coordination of air operations in tactical command and control managed areas of responsibility. **Status: Current**
AMD *Multi-Service Tactics, Techniques, and Procedures for Air and Missile Defense* **Distribution Restricted**	14 MAR 19	ATP 3-01.15 MCTP 10-10B NTTP 3-01.8 AFTTP 3-2.31	Description: This publication provides joint planners a consolidated reference on Service air defense systems, processes, and structures to include integration procedures. **Status: Current**
AOMSW *Multi-Service Tactics, Techniques, and Procedures for Air Operations in Maritime Surface Warfare* **Distribution Restricted**	15 FEB 16	ATP 3-04.18 MCRP 3-25J NTTP 3-20.8 AFTTP 3-2.74	Description: This publication consolidates Service doctrine, TTP, and lessons-learned from current operations and exercises to maximize the effectiveness of air attacks on enemy surface vessels. **Status: Revision**
AVIATION URBAN OPERATIONS *Multi-Service Tactics, Techniques, and Procedures for Aviation Urban Operations* **Distribution Restricted**	27 APR 16	ATP 3-06.1 MCRP 3-35.3A NTTP 3-01.04 AFTTP 3-2.29	Description: This publication provides MTTP for tactical-level planning and execution of fixed- and rotary-wing aviation urban operations. **Status: Revision**
DYNAMIC TARGETING *Multi-Service Tactics, Techniques, and Procedures for Dynamic Targeting* **Distribution Restricted**	10 SEP 15	ATP 3-60.1 MCRP 3-16D NTTP 3-60.1 AFTTP 3-2.3	Description: This publication provides the JFC, operational staff, and components MTTP to coordinate, de-conflict, synchronize, and prosecute dynamic targets in any AOR. It includes lessons learned, and multinational and other government agency considerations. **Status: Revision**
FIGHTER INTEGRATION *Multi-Service Tactics, Techniques, and Procedures for Fighter Integration* **Classified SECRET**	15 JUN 20	MCRP 3-20.7 NTTP 3-22.6 AFTTP 3-2.89	Description: This publication is a single-source set of integration standards intended to enhance commonality when operating with multiple-mission design series or type, model, and series fighter aircraft during an air-to-air mission. It establishes baseline intercept contracts with the associated communications plan. **Status: Current**
JFIRE *Multi-Service Procedures for the Joint Application of Firepower* **Distribution Restricted**	15 SEP 19	ATP 3-09.32 MCRP 3-16.6A NTTP 3-09.2 AFTTP 3-2.6	Description: This is a pocket-sized guide of procedures for calls for fire, CAS, and naval gunfire. It provides tactics for joint operations between attack helicopters and fixed-wing aircraft performing integrated battlefield operations. **Status: Current**
JSEAD *Multi-Service Tactics, Techniques, and Procedures for the Suppression of Enemy Air Defenses in a Joint Environment* **Distribution Restricted**	15 DEC 15	ATP 3-01.4 MCRP 3-22.2A NTTP 3-01.42 AFTTP 3-2.28	Description: This publication contributes to Service interoperability by providing the JTF and subordinate commanders, their staffs, and SEAD operators a single reference. **Status: Revision**
KILL BOX *Multi-Service Tactics, Techniques, and Procedures for Kill Box Employment* **Distribution Restricted**	18 JUN 18	ATP 3-09.34 MCRP 3-31.4 NTTP 3-09.2.1 AFTTP 3-2.59	Description: This MTTP publication outlines multi-Service kill box planning procedures, coordination requirements, employment methods, and C2 responsibilities. **Status: Revision**
PR *Multi-Service Tactics, Techniques, and Procedures for Personnel Recovery* **Distribution Restricted**	4 JUN 18	ATP 3-50.10 MCRP 3-05.3 NTTP 3-57.6 AFTTP 3-2.90	Description: This MTTP publication for personnel recovery is a single source, descriptive, reference guide for staffs and planners executing the military option of personnel recovery using joint capabilities. **Status: Revision**
SCAR *Multi-Service Tactics, Techniques, and Procedures for Strike Coordination and Reconnaissance* **Distribution Restricted**	31 JAN 18	ATP 3-60.2 MCRP 3-20D.1 NTTP 3-03.4.3 AFTTP 3-2.72	Description: This publication provides strike coordination and reconnaissance MTTP to the military Services for conducting air interdiction against targets of opportunity. **Status: Revision**
SURVIVAL, EVASION, AND RECOVERY *Multi-Service Procedures for Survival, Evasion, and Recovery* **Distribution Restricted**	21 AUG 19	ATP 3-50.3 MCRP 3-02H NTTP 3-50.3 AFTTP 3-2.26	Description: This is a weather-proof, pocket-sized, quick-reference guide of basic information to assist Service members in a survival situation regardless of geographic location. **Status: Current**

AIR AND SEA BRANCH–POC alsaA@us.af.mil

TITLE	DATE	PUB #	DESCRIPTION/STATUS
UAS *Multi-Service Tactics, Techniques, and Procedures for Tactical Employment of Unmanned Aircraft Systems* **Distribution Restricted**	22 JAN 15	ATP 3-04.64 MCRP 3-42.1A NTTP 3-55.14 AFTTP 3-2.64	Description: This publication establishes MTTP for UAS by addressing tactical and operational considerations, system capabilities, payloads, mission planning, logistics, and multi-Service execution. **Status: FY19 Rescind Approved**

LAND BRANCH–POC alsaB@us.af.mil

TITLE	DATE	PUB #	DESCRIPTION/STATUS
ADVISING *Multi-Service Tactics, Techniques, and Procedures for Advising Foreign Forces* **Distribution Restricted**	13 NOV 17	ATP 3-07.10 MCRP 3-33.8A NTTP 3-07.5 AFTTP 3-2.76	Description: This publication discusses how advising fits into security assistance/security cooperation and provides definitions for specific terms as well as listing several examples to facilitate the advising process. **Status: Revision**
AIRFIELD OPENING *Multi-Service Tactics, Techniques, and Procedures for Airfield Opening* **Approved for Public Release**	27 OCT 18	ATP 3-17.2 MCRP 3-20B.1 NTTP 3-02.18 AFTTP 3-2.68	Description: This publication provides guidance for operational commanders and staffs on opening and transferring an airfield. It contains information on Service capabilities, planning considerations, airfield assessment, and establishing operations in all operational environments. **Status: Project Assessment**
BIOMETRICS *Multi-Service Tactics, techniques, and Procedures for Tactical Employment of Biometrics in Support of Operations* **Approved for Public Release**	30 APR 20	ATP 2-22.85 MCRP 3-33.1J NTTP 3-07.16 AFTTP 3-2.85 CGTTP 3-93.6	Description: Fundamental TTP for biometrics collection planning, integration, and employment at the tactical level in support of operations is provided in this publication. **Status: Current**
CF-SOF *Multi-Service Tactics, Techniques, and Procedures for Conventional Forces and Special Operations Forces Integration and Interoperability* **Distribution Restricted**	4 APR 18	FM 6-05 MCWP 3-36.1 NTTP 3-05.19 AFTTP 3-2.73 USSOCOM Pub 3-33	Description: This is a comprehensive reference for commanders and staffs at the operational and tactical levels with standardized techniques and procedures to assist in planning and executing operations requiring synchronization between CF and SOF occupying the same area of operations. **Status: Revision**
DEFENSE SUPPORT OF CIVIL AUTHORITIES (DSCA) *Multi-Service Tactics, Techniques, and Procedures for Defense Suport of Civil Authorities* **Approved for Public Release**	25 SEP 15	ATP 3-28.1 MCWP 3-36.2 NTTP 3-57.2 AFTTP 3-2.67	Description: DSCA sets forth MTTP, at the tactical level, to assist the military planner, commander, and individual Service forces in employing military resources in response to domestic emergencies, in accordance with US law. **Status: Revision**
EO *Multi-Service Tactics, Techniques, and Procedures for Unexploded Explosive Ordnance Operations* **Distribution Restricted**	12 MAR 20	ATP 4-32.2 MCRP 3-17.2B NTTP 3-02.4.1 AFTTP 3-2.12	Description: This publication provides commanders and their units guidelines and strategies for planning and operating in an explosive ordnance environment while minimizing the impact of explosive ordnance on friendly operations. **Status: Current**
MILITARY DIVING OPERATIONS (MDO) *Multi-Service Service Tactics, Techniques, and Procedures for Military Diving Operations* **Approved for Public Release**	2 JAN 19	ATP 3-34.84 MCRP 10-10D.1 NTTP 3-07.7 AFTTP 3-2.75 CGTTP 3-95.17	Description: This publication is a single-source, descriptive-reference guide to ensure effective planning and integration of multi-Service diving operations. It provides combatant command, joint force, joint task force, and operational staffs a comprehensive resource for planning military diving operations, including considerations for each Service's capabilities, limitations, and employment. **Status: Project Assessment**
NONLETHAL WEAPONS (NLW) *Multi-Service Service Tactics, Techniques, and Procedures for the Tactical Employment of Nonlethal Weapons* **Distribution Restricted**	29 MAY 20	ATP 3-22.40 MCWP 3-15.8 NTTP 3-07.3.2 AFTTP 3-2.45 CGTTP 3-93.2	Description: This publication provides a single-source, consolidated reference on employing nonlethal weapons. Its intent is to make commanders and subordinates aware of using nonlethal weapons in a range of scenarios including security, stability, crowd control, determination of intent, and situations requiring the use of force just short of lethal. **Status: Current**
OP ASSESSMENT *Multi-Service Tactics, Techniques, and Procedures for Operation Assesment* **Approved for Public Release**	07 FEB 20	ATP 5-0.3 MCRP 5-10.1 NTTP 5-01.3 AFTTP 3-2.87	Description: This publication serves as a commander and staff guide for integrating assessments into the planning and operations processes for operations conducted at any point along the range of military operations. **Status: Current**

LAND BRANCH–POC alsaB@us.af.mil

TITLE	DATE	PUB #	DESCRIPTION/STATUS
PEACE OPS *Multi-Service Tactics, Techniques, and Procedures for Conducting Peace Operations* **Approved for Public Release**	2 MAY 19	ATP 3-07.31 MCWP 3-33.8 AFTTP 3-2.40	Description: This publication offers a basic understanding of joint and multinational PO, an overview of the nature and fundamentals of PO, and detailed discussion of selected military tasks associated with PO. **Status: Current** **Ownership of this MTTP and responsibility for future revisions has been transferred to the Peacekeeping and Stability Operations Institute**
TACTICAL CONVOY OPERATIONS *Multi-Service Tactics, Techniques, and Procedures for Tactical Convoy Operations* **Distribution Restricted**	22 FEB 17	ATP 4-01.45 MCRP 3-40F.7 AFTTP 3-2.58	Description: This is a quick-reference guide for convoy commanders operating in support of units tasked with sustainment operations. It includes TTP for troop-leading procedures, gun-truck employment, countering IEDs, and battle drills. **Status: Revision**

COMMAND AND CONTROL (C2), CYBER AND SPACE BRANCH–POC: alsaC@us.af.mil

TITLE	DATE	PUB #	DESCRIPTION/STATUS
AIRSPACE CONTROL *Multi-Service Tactics, Techniques, and Procedures for Airspace Control* **Distribution Restricted**	14 FEB 19	ATP 3-52.1 MCRP 3-20F.4 NTTP 3-56.4 AFTTP 3-2.78	Description: This MTTP publication is a tactical-level document which synchronizes and integrates airspace C2 functions and serves as a single-source reference for planners and commanders at all levels. **Status: Current**
AIR-TO-SURFACE RADAR SYSTEM EMPLOYMENT *Multi-Service Tactics, Techniques, and Procedures for Air-to-Surface Radar System Employment* **Distribution Restricted**	23 OCT 19	ATP 3-55.6 MCRP 2-10A.4 NTTP 3-55.13 AFTTP 3-2.2	Description: This publication covers theater-level, air-to-surface radar systems and discusses system capabilities and limitations performing airborne command and control; wide area surveillance for near-real-time targeting and target development; and processing, exploiting, and disseminating collected target data. **Status: Current**
BREVITY *Multi-Service Brevity Codes* **Distribution Restricted**	28 MAY 20	ATP 1-02.1 MCRP 3-30B.1 NTTP 6-02.1 AFTTP 3-2.5	Description: This publication defines multi-Service brevity which standardizes air-to-air, air-to-surface, surface-to-air, and surface-to-surface brevity code words in multi-Service operations. **Status: Current**
ISR OPTIMIZATION *Multi-Service Tactics, Techniques, and Procedures for Intelligence, Surveillance, and Reconnaissance Optimization* **Distribution Restricted**	3 SEP 19	ATP 3-55.3 MCRP 2-2A NTTP 2-01.3 AFTTP 3-2.88	Description: This publication provides a comprehensive resource for planning, executing, and assessing surveillance, reconnaissance, and processing, exploitation, and dissemination operations. **Status: Current**
TACTICAL CHAT *Multi-Service Tactics, Techniques, and Procedures for Internet Tactical Chat in Support of Operations* **Distribution Restricted**	24 JAN 14	ATP 6-02.73 MCRP 3-40.2B NTTP 6-02.8 AFTTP 3-2.77	Description: This publication provides commanders and their units guidelines to facilitate coordinating and integrating tactical chat when conducting multi-Service and joint force operations. **Status: FY20 Rescind Approved**
TACTICAL RADIOS *Multi-Service Communications Procedures for Tactical Radios in a Joint Environment* **Approved for Public Release**	19 MAY 17	ATP 6-02.72 MCRP 3-30B.3 NTTP 6-02.2 AFTTP 3-2.18	Description: This is a consolidated reference for TTP in employing, configuring, and creating radio nets for voice and data tactical radios. **Status: Revision**
TAGS *Multi-Service Tactics, Techniques, and Procedures for the Theater Air-Ground System* **Distribution Restricted**	21 MAY 20	ATP 3-52.2 MCRP 3-25F NTTP 3-56.2 AFTTP 3-2.17	Description: This publication promotes Service awareness regarding the role of airpower in support of the JFC's campaign plan, increases understanding of the air-ground system, and provides planning considerations for conducting air-ground ops. **Status: Current**

FUTURE AIR LAND SEA BULLETINS (ALSB)

Got a story?
Want to tell it?
Help us help you!

The Air Land Sea Application (ALSA) Center develops multi-Service tactics, techniques, and procedures (MTTP) with the goal of meeting the immediate needs of the warfighter. In addition to developing MTTP, ALSA provides the ALSB forum to facilitate tactically and operationally relevant information exchanges among warfighters of all Services.

There is no better resource for information than the people doing the jobs. Personal experiences, studies, and individual research lead to inspirational and educational articles. Therefore, we invite our readers to share their experiences and, possibly, have them published in an upcoming ALSB.

We want to take your expertise and lessons learned from recent operations or any other multi-Service or multi-nation missions in which you have been involved, and spread that knowledge to others. Get published by sharing your experiences and expertise.

You are invited to use this platform to share your insights on topics that may not be covered in doctrine or address an operational gap that highlights emerging needs for supporting multi-Service publications.

Please keep submissions unclassified and in accordance with the instructions in the requirements box on this page.

Air Land Sea Bulletin Article Requirements and Deadlines

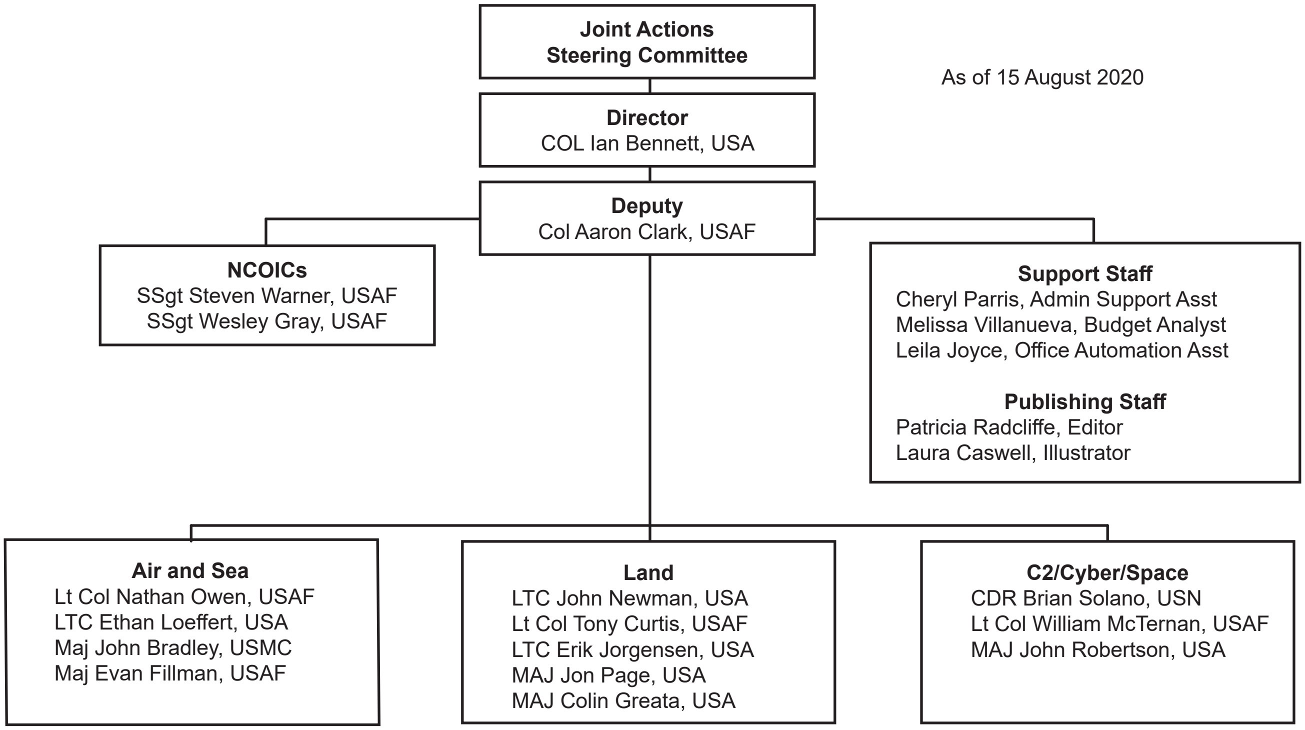
Submissions must:

- Be unclassified
- Be 5,000 words or less
- Be publicly releasable
- Be double spaced
- Be in MS Word format
- Include the author's name, unit address, telephone numbers, and email address.
- Include current, high resolution, 300 dpi (minimum), original photographs and graphics. Public affairs offices can be good sources for photographs or graphic support.

Article and photo submission deadlines are below. Early submissions are highly encouraged and appreciated.

Issue	Deadline	Point of Contact
Winter 2021	1 October 2020	alsaB@us.af.mil (757) 225-0964
Summer 2021	1 March 2021	alsaC@us.af.mil (757) 225-0903
Winter 2022	1 October 2021	alsaA@us.af.mil (757) 225-0854

ALSA ORGANIZATION



As of 15 August 2020

Joint Actions Steering Committee

Director
COL Ian Bennett, USA

Deputy
Col Aaron Clark, USAF

NCOICs
SSgt Steven Warner, USAF
SSgt Wesley Gray, USAF

Support Staff
Cheryl Parris, Admin Support Asst
Melissa Villanueva, Budget Analyst
Leila Joyce, Office Automation Asst

Publishing Staff
Patricia Radcliffe, Editor
Laura Caswell, Illustrator

Air and Sea
Lt Col Nathan Owen, USAF
LTC Ethan Loeffert, USA
Maj John Bradley, USMC
Maj Evan Fillman, USAF

Land
LTC John Newman, USA
Lt Col Tony Curtis, USAF
LTC Erik Jorgensen, USA
MAJ Jon Page, USA
MAJ Colin Greata, USA

C2/Cyber/Space
CDR Brian Solano, USN
Lt Col William McTernan, USAF
MAJ John Robertson, USA

ALSA JOINT WORKING GROUPS

Date	Publication	Location	Point of Contact
11-15 January 21	Airfield Opening	Joint Base Langley-Eustis, VA	Land Branch alsaB@us.af.mil
25-29 January 21	Advising	Joint Base Langley-Eustis, VA	Land Branch alsaB@us.af.mil
22-26 February 21	Advising	Joint Base Langley-Eustis, VA	Land Branch alsaB@us.af.mil
1-5 March 21	Military Diving Operations	Joint Base Langley-Eustis, VA	Land Branch alsaB@us.af.mil
All Dates are Tentative			

ALSA MISSION

ALSA's mission is to rapidly and responsively develop multi-Service tactics, techniques and procedures, studies, and other like solutions across the entire military spectrum to meet the immediate needs of the warfighter.

ALSA is a multi-Service organization governed by a Joint Actions Steering Committee, chartered by a memorandum of agreement, under the authority of the Commanders of the United States Army Training and Doctrine Command; Marine Corps Training and Education Command; Navy Warfare Development Command; and Headquarters, Curtis E. LeMay Center for Doctrine Development and Education.

VOTING JASC MEMBERS

Mr. Howard K. Brewington

Deputy Director, Mission Command Center of Excellence

No Photo Available

Col Eric R, Quehl

Director, Policy and Standards Division, Training and Education Command

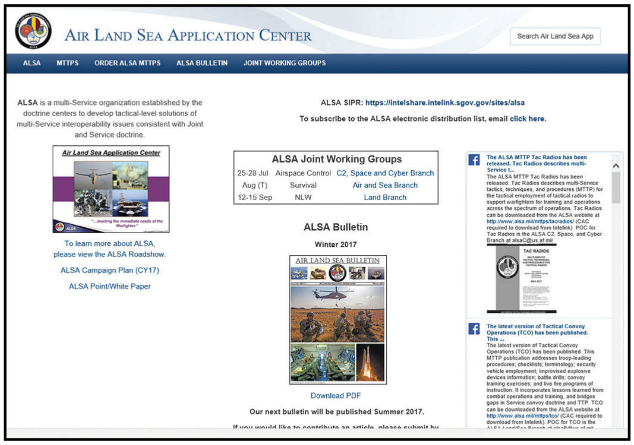
RADM Fred I. Pyle

Commander, Navy Warfare Development Command

Maj Gen Brad M. Sullivan

Commander, Curtis E. LeMay Center for Doctrine Development and Education

ONLINE ACCESS TO ALSA PRODUCTS



AIR LAND SEA APPLICATION CENTER

ALSA is a multi-Service organization established by the doctrine centers to develop tactical-level solutions of multi-Service interoperability issues consistent with Joint and Service doctrine.

Air Land Sea Application Center

"...meeting the immediate needs of the Warfighter."

To learn more about ALSA, please view the ALSA Roadshow.

ALSA Campaign Plan (CY17)

ALSA Point/White Paper

ALSA SIPR: https://intelshare.intelink.sgov.gov/sites/alsa

To subscribe to the ALSA electronic distribution list, email click here.

ALSA Joint Working Groups

25-28 Jul	Airspace Control	C2, Space and Cyber Branch
Aug (T)	Survival	Air and Sea Branch
12-15 Sep	NLW	Land Branch

ALSA Bulletin

Winter 2017

AIR LAND SEA BULLETIN

Download PDF

Our next bulletin will be published Summer 2017.

If you would like to contribute an article, please submit by

The ALSA MTTP Tac Radios has been released. Tac Radios describes multi-Service t...
The ALSA MTTP Tac Radios has been released. Tac Radios describes multi-Service tactics, techniques, and procedures (MTTP) for the tactical employment of tactical radios to support warfighters for training and operations across the spectrum of operations. Tac Radios can be downloaded from the ALSA website at http://www.alsa.mil/mttps/tacradios/ (CAC required to download from Intelink). POC for Tac Radios is the ALSA C2, Space, and Cyber Branch at alsaC@us.af.mil

TAC RADIOS

The latest version of Tactical Convoy Operations (TCO) has been published. This ...
The latest version of Tactical Convoy Operations (TCO) has been published. This MTTP publication addresses troop-leading procedures; checklists; terminology; security vehicle employment; improvised explosive devices information; battle drills; convoy training exercises; and live fire programs of instruction. It incorporates lessons learned from combat operations and training, and bridges gaps in Service convoy doctrine and TTP. TCO can be downloaded from the ALSA website at http://www.alsa.mil/mttps/tco/ (CAC required to download from Intelink). POC for TCO is the ALSA Land/Sea Branch at alsaB@us.af.mil

ALSA Public Website
http://www.alsa.mil

ALSA SIPR Site
https://intelshare.intelink.sgov.gov/sites/alsa

JEL+
https://jdeis.js.mil/jdeis/index.jsp?pindex=84

ALSA CENTER

ATTN: ALSB

114 ANDREWS STREET

JOINT BASE LANGLEY-EUSTIS, VA

23665-2785

OFFICIAL BUSINESS

Scan Me

Air Land Sea Application Center

http://www.facebook.com/ALSA.Center

http://www.twitter.com/ALSA_Center

Air Land Sea Application Center

ALSA