AIR LAND SEA BULLETIN




Issue No. 2020-1 Air Land Sea Application (ALSA) Center *Winter 2020*

ALSA Staff

Director
Col Brian Gross, USAF

Deputy Director
COL Matthew Ketchum, USA

Bulletin Editor
MAJ John Robertson, USA

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

Cover Photo Information

Captain Taiwan Veney, cyber warfare operations officer, watches members of the 175th Cyberspace Operations Group. From left, Capt Adelia McClain, SSgt Wendell Myler, SrA Paul Pearson, and SSgt Thacious Freeman analyze log files and provide a cyber threat update using a Kibana visualization on the large data wall at Warfield Air National Guard Base, Middle River, Maryland on 3 June 2017. (Photo by J.M. Eddins Jr.)

DIRECTOR'S COMMENTS

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

We are sad to lose two staff members to other assignments. They are Lt Col Steve Lawhun and Lt Col Brent Blandino, USAF. Lt Col Lawhun will be attending J Model Conversion training at Kirtland Air Force Base (AFB), New Mexico. Lt Col Blandino is stationed with the 325th Fighter Wing, Tyndall AFB, Florida. Both showed great attention to detail and possess outgoing, charismatic personalities that will be hard to replace. We wish them the best of luck in their new assignments.

This edition of the Air Land Sea Bulletin (ALSB) contains five articles to stimulate thought and spur discussion. The first article is, "Whole of Nation Response Framework for a Massive Cyber Attack", is by BGen Gregory Woodrow, USAF; LTC Matthew Giblin, USA; CDR Carter Reue, USN; and Maj Christopher Witbracht, USMC. This article details possible disastrous effects of a massive cyberattack aimed at the US. It explores the cyber defense infrastructure and steps needed to improve readiness and response capabilities to bolster the US' defense.

The second article is "Hybrid Cyber Employment Model: Playing Futbol vs Football", by CAPT Joshua Sanders, USN; LTC Albert Davis, USA; and Maj Thomas Moore, USAF. It explores realigning cyber mission force teams to perform offensive and defensive cyberspace operations. Currently, the teams perform one or the other. Using the example of joint task force Ares, the authors recommend teams moving toward a joint task force structure to conduct cyberspace operations more efficiently.

The third article, "Twenty-first Century ISR Tactics: Ground-to-Air Signaling through QR Codes", by Maj John Long, Maj Amy Long, Capt Kasey Vaughn, and TSgt Andrew Patry, USAF. This article suggests quick response (QR) codes may be useful tools in a limited communications environment. It explores using QR codes to conduct and transmit intelligence, surveillance, and reconnaissance (ISR) information and tells how the ISR community can safeguard information within them.

The fourth article, "Multi-Domain Operations: Expanding Battlefields", is by Maj Kimber Nettis, USAF (with contributions from Col Lori Winn, USAF). It explores the need for joint forces to apply multi-domain operations (MDO) concepts to examine the current battlefield and analyze the overlapping impacts of warfighting domains and influencers.

The fifth article, "Multi-Domain Warfare Officer, the 13O", is by Col Francisco Gallei, USAF. It discusses creating the 13O career field within the USAF to develop and train multi-domain warfare officers. The article details duty expectations for 13Os, explains their purpose on a staff, and provides channels for applying for consideration into the field.

We invite you to seize opportunities to represent your Service and the joint community by sharing articles to be published in future ALSBs and by participating in multi-Service tactics techniques and procedures (TTP) joint working groups. As we tackle the challenges ahead, your ideas matter now 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 J. Gross, Colonel, USAF

Director

WHOLE OF NATION RESPONSE FRAMEWORK FOR A MASSIVE CYBER ATTACK

Pictured are server wire connections, which are part of the cyber environment where the North Carolina National Guard and other agencies battle to protect and deter malicious cyber attacks to North Carolina's cyber infrastructure. This photo was taken on 8 October 2019. (Photo by SSG Brendan Stephens USARNG)

By BGen Gregory "Woody" Woodrow, USAF; CDR Carter Reue, USN; LTC Matthew Giblin, USA; and Maj Christopher Witbracht, USMC

INTRODUCTION

A cyberattack of a magnitude that threatens vital United States (US) interests is one plausible scenario in today's security environment that should encourage the Department of Defense (DOD) to reframe homeland defense. A holistic framework for the direct integration of United States Government (USG) and private sector assets is necessary to respond to the effects of a disastrous attack on critical US infrastructure. Advanced cyber threats from across the globe require mobilizing all the US' resources, not just military capabilities. It is imperative to consider a framework for integrating USG cyber resources into private sector organizations. In an environment of hyper connectivity, it is easy to envision a World War III-level cyberattack, and the need to react with all aspects of US's power.

Mobilizing a proactive whole-of-nation response is not a novel concept. There is historical precedence for augmenting national defense, through policy and private partnerships, to meet the demand of evolving threats and needed capabilities. These were critical junctions in the nation's history where mechanisms were created to pool USG and private sector resources to ensure continuance of the American way of life. Throughout World Wars I and II, the US leveraged its private industry through creating wartime agencies to mobilize the nation's economy. During World War I, President Woodrow Wilson's administration created the Food Administration, the Fuel Administration, the Railroad Administration, the War Industries Board, and other regulatory agencies to ensure a fully resourced mobilization effort. In anticipation of the needs of World War II, President Franklin D. Roosevelt established the War Production Board (WPB). Beginning in 1939, the WPB had 12 regional offices and 120 field offices across the US. The WPB was responsible for converting private American production industries into those that produced war supplies.[1]

The WPB, and other agencies that existed during the World Wars, were facilitated by

expanded executive authorities and driven by patriotism and commercial profit. Facilitation of this level of integration with private-sector cyber resources is critical to the US' response to a World War III-level cyber event. In the wake of the Japanese attack on Pearl Harbor, Hawaii on December 7, 1941, President Roosevelt set sizable and aggressive goals for the nation's industrial force: 60,000 aircraft in 1942 and 125,000 in 1943; 120,000 tanks in the same time period; and 55,000 antiaircraft guns.[2]

War production revolutionized American industry. Companies, already engaged in defense work, expanded. Others, like the automobile industry, transformed to create new product lines. In 1941, more than 3,000,000 cars were manufactured in the United States.[3] Only 139 more were made in the period prior to the war's end. In place of cars, Chrysler made fuselages. General Motors made airplane engines, guns, trucks, and tanks. Packard made Rolls-Royce engines for the British Air Force. At its Willow Run plant in Ypsilanti, Michigan, the Ford Motor Company operated 24-hours a day.[4] The average Ford car had about 15,000 parts. In contrast, the B-24 Liberator long-range bomber had 1,550,000, and one came off the production line every 63 minutes.[5]

Current day military efforts to meet other emerging threats, such as a response to wea -pons of mass destruction (WMD), serve as a model for integrated capabilities to meet the cyber threat. President William J. Clinton signed Presidential Decision Directive 39 in 1995, which mandated an increased US response capability for the threat of WMD attacks on the homeland. This resulted in a National Guard concept to field ten rapid assessment and initial detection teams. These, eventually, became known as the weapons of mass destruction-civil support teams (WMD-CSTs), which now operate across the country.

Since 1998 Congress has authorized and funded CSTs in each state and territory, and one additional CST in New York, California, and Florida. Today, there are 57 National Guard CSTs. These federally-funded units respond immediately to WMD attacks. They provide assistance to civilian authorities and incident commanders by assessing the attack and assisting with requests for additional forces and recovery capabilities. These teams have specialized training and mobile laboratory capabilities designed for responding to, and assessing chemical, biological, radiological, or nuclear attacks. A CST is a military team designed for quick integration into the existing civilian response infrastructure, and is a template which can be emulated to build a similar cyber capability.

The current cyber mission force includes Department of Homeland Security hunt incident response teams, United States Cyber Command (USCYBERCOM) joint task forces, National Guard cyber protection teams, and state defense cyberspace operations (DCO) elements. However, the majority of cyber resources, in terms of human capital and technical infrastructure, exist within the private sector. Private-sector companies depend on cyber professionals daily for their corporate survival. However, there is a separation between the private and USG cyber efforts, other than some recent information sharing initiatives. The full weight of US power, like the power delivered during the World Wars, will never be realized in the cyber domain without an integrated partnership of private and public national resources with a complete ability to account for, and deter, cyber adversaries.[6]

The USG cyber response framework should be considered for an integrated private-sector partnership.

The USG cyber response framework should be considered for an integrated private-sector partnership. The framework should facilitate inserting military personnel into private organizations. This proposed partnership would take the form of embedded teams. For the purposes of this proposed partnership, a notional team will be referred to as a cyber-embedded training team (CETT). The CETT will be comprised of subject matter experts that assimilate into the technology business units resident across many private companies. This is similar to the embedded training teams employed during Operation ENDURING FREEDOM in Afghanistan. The CETT provides leadership, technical, and planning expertise to support the existing private sector cyber capability.

The CETT would consist of personnel with technical, intelligence, legal, and executive-engagement expertise. The following table depicts a proposed CETT with the best-suited military occupational specialties. The proposed

Proposed Cyber Embedded Training Team (CETT)	
Military Occupational Specialty	Rank
Communications/Cyber (17A)	Junior Officer or Senior Enlisted Leader
Intelligence (35A)	
Legal (Staff Judge Advocate) (27A)	
Human Resources/Personnel (executive engagement expertise) (42A)	

Note: United States Army MOSs are provided as an example.

ranks for the team personnel would be junior officers' or senior enlisted leaders'. The quantity of team members would depend on the mission or base requirements.

When deployed to a private-sector company for war-effort support and DCO, the CETT personnel embed with their civilian counterparts. Not only do they provide coordination in accordance with existing military lines of reporting for DCO, but they serve as conduits to identify any unique capabilities that must be leveraged to support the war effort, in regard to cyber responses.

CETT members conducting technical coordination would represent a diverse skill set. CETT members assist with software development for network defense, exploitation, and creative solutions. They conduct code reviews and integrate with civilian information technology (IT) development teams. Personnel with hacking and red-team backgrounds augment the private-sector company's red-team/penetration-team capabilities to further integrate them into DCO. Additionally, having CETT members with incident-response capabilities bolsters the tactics, techniques, and procedures of the private-sector company's security operations centers. CETT personnel with high-demand technical expertise and experience help protect critical infrastructure and key resources.

In the proposed CETT, personnel with an intelligence background would augment existing cyber intelligence capabilities in the private sector. USG and the private-sector personnel would share indicators of compromise (IOC) and the USG personnel would bridge the gap on certain classification issues. The IOC information would be employed by incident response personnel to fine tune their security information and support other active hunt capabilities under DCO.

In this notional partnership, the requirement to leverage the private sector's significant technical resources mandates the need for legal expertise and expanded authorities. Authority for military involvement on a private network would require executive-level emergency authorities. The CETT would have assigned staff judge advocate (SJA) personnel. The SJA would provide legal consultations for private-sector personnel engaging in DCO. The SJA interprets and disseminates cyber rules of engagement to private-sector staff members prior to them executing certain DCO. The CETT-assigned SJA provides onsite coordination with a private company for agreements and contracts. The SJA function may need to provide regional support (serving several CETTs at once) suggesting technical expertise is the only human capital bottleneck to scaling CETTs for major operations. SJAs could also establish malleable contracts prior to any catastrophic event, if relationships and trust were established ahead of time.

While the technical, intelligence, and legal personnel on the notional CETT engage with the private-sector staff at the tactical and operational levels, there is also a requirement for executive engagement. Senior CETT members need to have experience and proficiency in engaging private-sector, executive staff members across corporate officer and director functions. Although the chief information officer and chief information security officer are obvious points of contact, the CETT executive engagement members must be capable of coordinating with the chief operations officer, chief financial officer, and the chief executive officer. This skillset eases DCO coordination and streamlines reporting back to the lead federal agency.

The exact composition of personnel and skillsets to staff a CETT must be identified to ensure that private-sector companies can leverage their familiarity with USG DCO. This article only seeks to define a potential framework and establish the core competencies that a CETT must possess. There may be World War III-level cy-

ber events which require other capabilities that have not been mentioned. The CETT construct would require modularity to add on unique capabilities tailored to a particular scenario. It is also imperative that the DOD and private sector establish these relationships long before a response is needed.

ARGUMENTS AGAINST PRIVATE SECTOR AND USG CYBER INTEGRATION

It seems logical to discuss pairing up teams with common skillsets during a time of national calamity, but there are justifiable reasons against embedding this military capability into the private sector. The American public and private sectors have not seen eye-to-eye in terms of the use and growth of technology. Mandating civil assistance in a World War III cyberattack is an extreme option. This would constitute implementing emergency authority.

The US has done this before, albeit for short periods of time, in difficult situations. The most recent use during wartime is the Smith-Connally Act which passed over President Roosevelt's veto in 1943. The law allowed the USG to seize and operate industries threatened by, or under, strikes that would interfere with war production. It was created as a reaction to 400,000 coal miners who were striking for a pay increase due to war-driven inflation. Also, it was used the next year when the President sent 8,000 troops to quell the Philadelphia Transit Strike.[7]

Many Americans believe the USG overreaches when it comes to civil liberties and privacy, particularly when it comes to tech companies and personal data.

Many Americans believe the USG overreaches when it comes to civil liberties and privacy, particularly when it comes to tech companies and personal data. Recently, the Federal Bureau of Investigations (FBI) had an iPhone™ of a suspected terrorist, but risked losing the data on the phone if they bungled getting access to it. The FBI sought a solution from Apple. Apple argued that writing new software code to crack the security was a violation of the company's First Amendment right, and allowing the USG access would make it too easy for the USG, or foreign governments, to gain access to their products in the future. Before the case went to trial, the USG discovered an alternate means to access the iPhone.[8]

In similar cases, Microsoft, Yahoo, Google, Facebook, and Amazon have been in conflict with the Justice Department, stating USG overreach. The problem, as Microsoft points out, is that the USG seeks and executes warrants for electronic communications far more frequently than it sought and executed warrants for physical documents and communications. The company says, in its suit, that over the past year and a half the USG has demanded customer information 5,624 times. Of those, a whopping 2,576 came with secrecy orders, which bar Microsoft from disclosing the customer warrant. Sixty-eight percent of these orders have no expiration date. Those customers most likely will never find out that the USG searched their files. The reason the USG can do this is an antiquated law titled, the Electronic Communications Privacy Act. This act allows the USG to utilize an easy-to-get administrative subpoena, as opposed to a warrant, to search any personal data that has been stored on a server for more than 180 days.[9]

Beyond the recent struggles between the private sector and the USG regarding the USG's role in technology, these two entities have different incentives and focus areas. Private, high-tech firms are in the business of making money, and are loyal, primarily, to the board that runs them and the shareholders who own them. While contracting with the USG in times of a national emergency may be viewed positively, there is ample evidence that sharing corporate tech secrets with the USG may not be in private firms' best interest or looked upon with favor by shareholders.

Currently, the USG has a limited and specific role to play in defending the nation against cyberattacks of, potentially, significant consequence. This is appropriate because most cyberattacks do not warrant using vast resources. The private sector owns and operates more than 90 percent of all the networks and infrastructure of cyberspace and is, thus, the first line of defense. One of the most important steps for improving the US' overall cybersecurity posture is for companies to prioritize the networks and data that are in their interest to protect, and for them to invest in improving their own cybersecurity. While the USG must prepare to defend the country against the most dangerous attacks, most intrusions can be stopped through rela-

tively basic cybersecurity investments that companies can, and must, make themselves.

ARGUMENTS FOR PRIVATE SECTOR AND USG CYBER INTEGRATION

While there are concerns over the idea of a CETT, there are several reasons why this is an important framework. Cybersecurity attacks have become much more frequent in the past decade. The extent of the threat and the potential impact on private and public sectors are growing exponentially each day. The risk is widespread, potentially catastrophic, and the deterrent is minimal. Private cybersecurity is sufficient for most attacks, but the USG will be held responsible when it is not. USG systems; the financial sector; the electric power grid; infrastructure systems (e.g. water, gas, and transportation); hospitals and other medical institutions; and personal data are all at risk. Cybersecurity threats often originate from overseas locations, making it challenging for domestic law enforcement agencies to track, punish or deter them. These threats seldom rise to the level that necessitates a military response; but what if we, as a society, experienced a cyberattack so severe that it required action from the military?

A "Cyber Pearl Harbor" event most likely would affect several areas of society at once. The DOD's ability to synchronize and coordinate action over several different lines of effort would be invaluable during such an event.[11]

The notion of a "Cyber Pearl Harbor" is a possibility. Instead of a cybersecurity attack, which results in a temporary loss of electricity for a few thousand people, this type of event would, fundamentally, affect a substantial number of Americans in a prolonged way.[10] What if bank statements from the majority of Americans suddenly showed no money in their accounts for months? What if the electric grid became unreliable, especially with systems such as air traffic control? What if hospitals all over the country needed to shut down operations due to a rash of malware? Past incidents involving Stuxnet and WannaCry software demonstrate these scenarios are plausible, if the right actors have a sophisticated, malicious plan in place. Although there may not be a high loss of life in these situations, compared to a war, the American society, at large, would be thrown into a general state of chaos, threatening global stability, and serving as a call to action for American leadership as did the attack on Pearl Harbor, as did the attack on September 11, 2001.

There are three main arguments for having consistent integration between the military and the private sector in responding to a cyberattack, specifically to a "Cyber Pearl Harbor" level event. First, the DOD would be the only body that could provide unity of effort to effectively respond, in an overarching way, to an attack of this proportion. Unfortunately, the private sector would be too fragmented in their response. Second, the DOD is better resourced than most other departments in the USG, and it has a current, cyber-capable force that protects its internal systems during peacetime. It can be deployed easily when the need arises. Third, the private sector owns the preponderance of the technical infrastructure, so they would have a vested interest in partnerships for this type of situation.

A "Cyber Pearl Harbor" event most likely would affect several areas of society at once. The DOD's ability to synchronize and coordinate action over several different lines of effort would be invaluable during such an event.[11] However, involvement in the private sector is a very sensitive issue. A "Cyber Pearl Harbor" would necessitate a deeper level of coordination between the public and private sectors than is currently envisioned and governed by law. Today, private-sector companies likely would focus on solutions that benefit their particular situation and would not have an overarching ability to provide for stability during a breakdown of civil order. Only the USG can address a major attack on US sovereignty and the cascading chaos that could follow. The cyber nature of this type of attack creates sensitivities that must be addressed through public-private integration, before an attack occurs.

Beyond bringing a needed level of interagency coordination during a disaster-response scenario, the DOD has a readily available pool of trained personnel that could provide immediate value when responding to a massive cyberattack. Each branch of Armed Service has some form of a cyber team and they are coordinated through the USCYBERCOM. Below the combatant command level, each branch has day-to-day control over its own teams. Each team brings relevant

domain experience to the table in the areas of information security, network operations and analysis, and planning and contingency support. These various Service teams would experience synergy when they join to form CETTs. Having an integrated cyber force for strategic direction and communication, along with the operational and tactical capabilities inherent in the CETT structure, will allow the DOD to put their best foot forward when responding to a massive cyberattack.

Although the military has a trained cyber fighting force, the private sector owns the majority of the technical infrastructure and trained employees who support the software and hardware.[12] Each Service only has one cyber school to train new warriors, and the Cyber Mission Force (CMF) only has approximately 6,000 people across 133 teams.[13] These teams are designed to support each of the services and the combatant commands. The CETT structure could broaden the resource base to a massive cyberattack by leveraging resources beyond the CMF in not only the FAANG companies (Facebook, Apple, Amazon, Netflix, Google), but also other Fortune 500 companies that have technical resources. The private sector employs thousands more tech experts than the military, and there are universities around the country that teach relevant information technology skillsets to students.

Just as in World War II, when America harnessed its civilian industrial might to quickly increase the production of military planes and automobiles, the DOD leadership would need to call on resources from civilian counterparts to oppose a massive cyberattack.

CONCLUSION

The current level of coordination among private sector and USG cyber professionals is not sufficient to respond to a massive Pearl Harbor-type cyber attack. Cyberattacks focused on specific private-sector industries and capabilities will continue to occur as threat actors evolve their attack vectors. Additionally, the DOD will continue to experience cyberattacks against its networks. While the extent of damage and disruption required for a cyber-initiated, World War III-level response may not seem likely today, each day the possibility becomes more prevalent. Although the DOD has a trained cyber force and a reliable command and control structure to enable unity of effort, the private sector owns a majority of the cyber infrastructure and a much larger volume of tech-savvy employees.

The CETT framework, for a response capability, has its strengths and weaknesses. However, the CETT provides a solution to achieve unity of effort and ensure integration. The rapid evolution of technology will force a reframing of current legal authorities, sooner or later. Proactive thought that challenges America's current comfort zone far outweighs the risk of a disastrous cyberattack. Establishing a blueprint for how the public and private sectors will achieve unity of effort to combat these threats is a vital step toward evolving the US' readiness and response capabilities to ensure America's defense.

END NOTES

[1] PBS. "War Production." PBS. September 2007. Accessed February 24, 2019. http://www.pbs.org/thewar/at_home_war_production.htm.

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] Bosma, Michael. "Application of National Guard Civil Support Teams in Support of Weapons of Mass Destruction Mitigation Efforts." March 7, 2001. Accessed March 6, 2019. https://www.hsdl.org/?view&did=439267.

[7] Nepa, Stephen. "Philadelphia Transportation Company (PTC) Strike." The Encyclopedia of Greater Philadelphia. 2015 Rutgers University. Accessed May 6, 2019. https://philadelphiaencyclopedia.org/archive/philadelphia-transportation-company-ptc-strike/

[8] Khamooshi, Arish. "Breaking Down Apple's iPhone Fight with the US Government." The New York Times. March 21, 2016. Accessed March 3, 2019. https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html?_r=0.

[9] Neily, Nicole. "How the Tech Sector United Against Justice Department Overreach | RealClearTechnology." Realcleartechnology.com. May 3, 2016. Accessed March 3, 2019. http://www.realcleartechnology.com/articles/2016/05/03/how_the_tech_sector_united_against_justice_department_overreach_1285.html.

[10] Goldberg, Jonah. "Why are We Ignoring a Cyber Pearl Harbor?" Los Angeles Times (Los Angeles, CA), June 16, 2015. Accessed February 21, 2019. http://www.latimes.com/opinion/op-ed/la-oe-0616-goldberg-china-cyber-hack-20150616-column.html#.

[11] Wallace, Ian. "The Military Role in National Cybersecurity Governance." December 16, 2013. Accessed March 13, 2019. https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/.

[12] Harrell, Brian. "The Private Sector is the Key to Success for the Department of Homeland Security." February 1, 2017. Accessed March 1, 2019. http://www.csoonline.com/article/3161793/security/the-private-sector-is-the-key-to-success-for-the-department-of-homeland-security.html.

[13] US Department of Defense. "Cyber Mission Force Achieves Full Operational Capability." May 17, 2018. Accessed March 1, 2019. https://dod.defense.gov/News/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/

Real-time cyber attacks, including information on the attack's origin, type, and target; the attacker's IP address, geographic location, and ports being used are displayed on the 275th Cyberspace Squadron's Norse attack map on 2 December 2017. (Photo by J.M. Eddins Jr.)

A HYBRID CYBER EMPLOYMENT MODEL:
PLAYING FUTBOL VS FOOTBALL

By CAPT Joshua Sanders, USN; LTC Albert Davis , USA; and Maj Thomas Moore, USAF

BACKGROUND

Military operations include synchronized effects in the cyberspace domain. Using cyberspace operations effectively is key to the United States' ability to compete against the identified priority challenges (i.e., Russia, China, Iran, Democratic People's Republic of Korea (DPRK), and violent extremist organizations (VEOs)).[1] Mastery in competing below the level of armed conflict enables the asymmetric military advantage necessary to attain superiority of the information environment. The challenges to meet this objective require leaders to make tough decisions when it comes to employment and management of the finite force. The current structure is not optimal for power projection and is unable to effectively provide the requisite support needed for global force integration and dynamic force employment. Looking at the evolution of the operational environment and gaining a better understanding of potential near-peer adversaries, suggests United States Cyber Command (USCYBERCOM) must change the paradigm from its current bifurcated operational structure (offensive and defensive) to a cross-functional approach where hybrid teams are developed with warriors possessing offense and defense skillsets needed to defeat evolving and emerging threats.

CURRENT STRUCTURE

Cyber forces execute operations to secure, operate, and defend the Department of Defense information network; defend the nation from attack; and provide cyberspace operations, as required, to combatant com-

manders.[2] In 2018, USCYBERCOM became a combatant command.[3] Heading the functional combatant command for the cyberspace domain, the commander is responsible for directing, synchronizing, and coordinating cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners.[3] USCYBERCOM's operational cyber force, or team, established in 2012, is the cyber mission force (CMF).[4] The CMF is comprised of three distinct mission teams, cyberspace protection teams (CPTs), combat mission teams (CMTs), and national mission teams (NMTs).[5] The CPTs focus on defensive cyber operations, while the CMTs and NMTs focus on offensive cyber operations.[5] In addition, there are combat support teams (CSTs) and national support teams (NSTs) who provide direct support to the mission teams.[5] The CMF operates at the strategic and operational levels.

Cyber forces execute operations to secure, operate, and defend the Department of Defense information network; defend the nation from attack; and provide cyberspace operations ...

For purposes of this article, the questions of structure and model are directly related to the teams who are at the tactical level and responsible for action. The tactical level is where the fight takes place.

Currently, the Services maintain administrative control of the CMF teams by providing personnel, training, and equipment.[5] However, while Services maintain operational control of their Service-retained CPTs, operational control of the majority of CPTs and all the CMTs and NMTs becomes the responsibility of other combatant commanders and the commander of the cyber national mission force (CNMF).[5] This regional alignment, as the current construct, hinders USCYBERCOM from combatting emerging threats.

Comparing the popular models provided by American football and European futbol, the existing structure suggests the CMF is a team that plays football while others play futbol. A CMF team is either offense or defense and, in this model, rarely will a team play both sides of the ball in the same game. If a team wishes to play the other side of the ball, the team must come off the field allowing another team to come onto the field to take their place. On the other hand, a futbol team is able, with a quick transition, to switch back and forth between offense and defense, making use of their own skills instead of having to

Service Components of USCYBERCOM[6]

leave the field in favor of another team with different skills. Is the football model, with only an offense or a defense on the field optimal to support today's dynamic threat? Should USCYBERCOM have a more integrated model with a defense-in-depth approach where offensive and defensive specialists can perform both functions and share the field being agile and responsive enough to contend with rapid changes in action?

Should USCYBERCOM have a more integrated model with a defense-in-depth approach ...

Make no mistake, cyber warfare is not a game. The intent of this metaphor is to understand how USCYBERCOM can more effectively and efficiently fight in the cyber domain. How USCYBERCOM chooses to play this game is the question. If they truly want to win, there must be enough flexibility to support emerging threats in cyberspace while working to combat the threats outlined in the National Security Strategy (NSS).[7] The team's organizational model must be optimal for power projection and be able to effectively provide the support needed for global force integration and dynamic force employment.

ADVANTAGES OF THE CURRENT STRUCTURE

The current structure proves to be advantageous to streamlining crew position training requirements, leading to crew position expertise. A team member knows exactly what training is needed to become certified and what capabilities to bring to the team. Solely focused on training and developing capabilities, the cyber professional becomes an expert.

A combatant commander provides priorities which become the teams' lines of effort. This provides teams clear direction and purpose.

Another advantage in using the current structure is the ability to meet each combatant commander's requirements. A combatant commander provides priorities which become the teams' lines of effort. This provides teams clear direction and purpose.

A final advantage is, teams can meet their training and capability requirements quickly. Having operators only specialize in one capability shortens the training pipeline. This allows teams to join the fight expeditiously to meet the needs of combatant commanders.

DISADVANTAGES OF THE CURRENT STRUCTURE

Given the finite amount of CMF resources, not all priorities are accomplished, especially if a combatant command has more priorities than it does CMF teams. The current construct employs 68 defensive and 40 offensive teams across the globe.[8] This becomes an issue if there are more requests for offensive cyber than defensive cyber. Some cyber operation priorities will need to "stay on the shelf" due to a lack of resources and capabilities.

Additionally, the existing structure does not provide flexibility to combat emerging threats because the team's focus is on a specific mission set. Since a team is stovepiped to either offensive or defensive cyber operations, it is unable to easily move between the two types of operations. Therefore, if an emerging priority requires offensive and defensive cyber capabilities, two teams (instead of one) must steer to that priority to meet the requirement while abandoning the previously assigned missions.

USCYBERCOM REAL-WORLD ACTIONS TOWARDS ENEMY ACTIVITIES—ONE WAY

A real-world example is Joint Task Force (JTF) Ares, stood up by USCYBERCOM in 2016 to combat Islamic State in Iraq and the Levant (ISIL) cyber threats.[9] ISIL, a VEO, is one of the five great power competitors designated in the NSS.[10] JTF Ares' charter is to create new digital weapons and deliver cyber effects in direct support of defeating ISIL on the offensive and defensive digital fronts in the United States Central Command (USCENTCOM) area of responsibility (AOR).[8] The JTF was formed from members of every type of CMF team by pulling team members from working their designated priorities. This was necessary because defensive and offensive capabilities are needed to combat ISIL.[8] Combining capabilities led to some growing pains while team members from

offensive teams had to learn what capabilities their team members from defensive teams brought to the fight. Initially, USCYBERCOM leaders only focused on cyber operations to combat the ISIL threat but later realized that just looking through the cyber lens was somewhat myopic at best.[8] This is because cyber has yet to fully integrate into the whole spectrum of military operations.

Based on USCENTCOM objectives and desired outcomes, cyber leaders realized they, as a community, must understand the capabilities throughout the entire combatant command and not only be fully integrated, but fully interoperable, to achieve maximum results on the battlefield. To achieve desired effects, cyber had to embed across all aspects of military operations including kinetic, nonkinetic, offensive, and defensive.[11] This requires coordination not only with military members in the USCENTCOM AOR, but with the Department of Homeland Security, the Department of State, nongovernment organizations; and, at times, international government organizations. JTF Ares supports the joint and coalition efforts to degrade and defeat ISIL and they continue to thwart ISIL operations by spreading messages and coordinating future operations with defensive and offensive cyberspace operations.[12]

JTF Ares monitored ISIL's growing capability to increase the use of social media focusing on recruiting and propaganda to radicalize and create a new generation of loyalists.[11] This is a modern-day approach that enabled ISIL to spread its ideologies throughout the world, specifically targeting a young, impressionable audience that is in tune with technology and cyber capabilities.[13] The combination of Facebook, Twitter, and YouTube allowed ISIL to spread their message to millions of would-be jihad extremists.[14] From millions of viewers, thousands of ISIL videos have received comments of support and uplifting the organization to illustrate that not only are they an organization that supports the greater good of society, but they also help protect innocent civilians.[12] Understanding the ISIL game plan allowed USCYBERCOM to respond with an integrated cyber team and plan to fight and win.

The structure and approach for JTF Ares focused on combatting a transregional threat in an environment with no boundaries that moves at the speed of the computing power.[15] This required an agile force to combat an astute adversary. JTF Ares is a diverse, agile, and integrated team of teams formed from all three distinct CMF mission teams, including members from defensive and offensive specialties.[16]

The structure and approach for JTF Ares focused on combatting a transregional threat in an environment with no boundaries that moves at the speed of the computing power.[15]

JTF Ares considered the sequence of events and actions that impacted the ability of ISIL to maneuver. They understood the offensive element of the effort started with assessing the readiness of the team, followed by effective execution with a purpose to minimize ISIL propaganda. The defensive effort required a ready force able to quickly identify any ISIL offensive maneuver and respond appropriately to ensure the team could continue to operate. Security established the boundaries the team used to differentiate what should or should not affect operations. The unique aspect of JTF Ares is, they executed all operations as one, integrated, unit. A synchronized series of actions by the JTF and interagency partners resulted in a decisive blow to the adversary.[17]

The approach directly correlates with the futbol metaphor where each cyber player was ready to press in a forward offensive approach and was able to quickly transition to a defensive position while keeping the ball in play. In cyberspace, the ball is always in play. Although, there is much room for improvement, leaders within USCYBERCOM feel the digital fight against ISIL and VEOs continues to improve and the cyber fight is vital, in the coming years, as we look at near-peer competitors and our ability to protect the homeland.[18] It is apparent that the ability to resurge and be adaptive and flexible enough in virtual space is paramount for the future of cyber.

THE RIGHT CHOICE

Commander, USCYBERCOM is charged with employing the force to meet re-

Unidentified Sailors stand watch in the Fleet Operations Center at the headquarters of US Fleet Cyber Command/ US 10th Fleet on 27 September 2018. (Photo by MC1 Samuel Souvannason, USN)

quirements and execute the mission.[19] The best use of the force, for prior commanders, focused on defense, which has more players.[20] Defense alone is not enough.[19] The current commander, United States Army General Paul Nakasone, stated "the best defense is a strong offense".[21] Given the threats and the state of play in the cyber domain, General Nakasone, has even gone as far as to suggest the need for a Seal Team Six-type model for the cyber force.[20] This would be a force that is flexible, agile and has the appropriate authorities to respond to emerging high-level threats at a moment's notice.[20] It is necessary to restructure the current teams to an integrated model establishing a hybrid team that is made of teammates with offensive and defensive skills. This would provide a force that is ready to respond to any threat without having to dismantle multiple teams to make it possible, as in the JTF Ares example.

The new, integrated model for the cyber teams is flexible and adaptive to emerging missions. With the current CMF structure, a team must break into smaller elements to respond appropriately. A team requires a full spectrum, multi-domain approach, with offensive and defensive capabilities, to effectively respond to threats. This new, dynamic approach will ensure cyber forces integrate with the full spectrum of military operations. Unity of effort among all elements of military power is the goal for effective execution at strategic, operational, and tactical levels.

The new, integrated model for the cyber teams is flexible and adaptive to emerging missions.

DISADVANTAGES TO THE NEW STRUCTURE

The cost of a restructure and the time needed to perform the restructure are not ideal. USCYBERCOM must spend time for planners to determine the new team structure including crew positions, crew training requirements, and combatant command source reallocation. Planners have invested a lot of time and work already to analyze the current structure, and with the proposed restructure, USCYBERCOM must factor in additional time, money, and resources.

Given current fiscal constraints, adding an additional cost to an already resource

constrained budget is not ideal or optimal. However, for each hybrid team member, USCYBERCOM will get a two-for-one capability. This will be beneficial for future fiscal years.

A final disadvantage is the new model contradicts the command and control principle of simplicity. According to Joint Publication 1, *Doctrine for the Armed Forces of the United States*, simplicity is defined as having a clear delineation of responsibilities and authorities.[22] Authorities differ between offensive and defensive cyberspace operations. A team performing offensive and defensive cyber will operate under expanded authorities according to their mission. This is not an issue for current planners because the teams' authorities are clear, based on whether they are offensive or defensive. This issue will need to be considered by planners as the structure evolves to an integrated model.

ADVANTAGES TO A NEW STRUCTURE

The CMF is made of 133 teams. Some believe there are not enough teams.[23] However, a restructure of the current teams will meet the needs of combatant commanders' cyber missions without having to grow the CMF force. The hybrid team will be able to work offensive and defensive cyber lines of effort. The new model is a force multiplier. Additionally, the model will answer the global integrators' need to apply dynamic force employment of the cyber force to meet requirements without altering team structure. This moves USCYBERCOM from playing football to futbol, that is, from having attackers (offense) and defenders (defense) to having only midfielders (offense and defense).

In military operations, synchronization among all elements and from all warfighting domains is paramount prior to and during execution.

In military operations, synchronization among all elements and from all warfighting domains is paramount prior to and during execution. Considering the speed of cyberspace, timing is always a critical component. Given that defense and offense do not coexist, there is the basic challenge of providing requested support. With the current model, the defensive operators may have to wait for the offensive operators to arrive with their assets before adequately responding to an incident.

For defensive team members, identifying an incident rapidly is critical to their successful diagnosis and response actions or, in worst case, that of the offensive special operators. When there is an offensive maneuver, there must be an equally responsive defense ready to posture networks and secure critical infrastructure from retaliation. Time, again, is of the essence. Eventually, as with time, there are the readiness and resources questions that surface with the proposed model. Cyber teams are finite, therefore, they must be employed in the most effective and efficient manner to guarantee mission success.

CONCLUSION

Services will continue to operate as force providers to the CMF to introduce the new, integrated model. The current construct proves inefficient and incapable of handling today's cyber challenges. Teams outside JTFs remain unintegrated. The current model is one that supports a federated rather than an integrated team of teams.[24] A bifurcated model is inefficient, resulting in valuable time and synergy lost, which impacts the success of military operations.

Looking at the evolution of the cyberspace operational environment and gaining a better understanding of potential near-peer adversaries, it seems imperative that USCYBERCOM adopts an integrated and dynamic approach to the fight in cyberspace. To do so, the CMF must adopt a cross-functional approach to defeat emerging threats rather than a bifurcated offensive and defensive approach.

According to former Commander, USCYBERCOM, Admiral (Ret) Mike Rogers, "Cyber is an operational domain". Adopting an operational approach to cyber warfare is the key to successful integration and the mastery of full-spectrum military operations.[25] Adopting the proposed model will enhance cyber team effectiveness and produce a dynamic team capable of providing full-spectrum support when called to the field. The teams called "cyber warriors" are the best in the world. They fight every day to protect this country's vital interests. Whether the teams are fight-

ing on the offensive or defensive side, they are on the same team, the CMF. Cyberspace will always be a contested environment, with little to no chance of superiority. However, with an agile and ready force the United States will be ready to maintain the advantages of movement and maneuver in the cyber domain.

"While we cannot ignore vital cyber defense missions, we must take this fight to the enemy, just as we do in other aspects of conflict."[26]

General Paul M. Nakasone, Commander, USCYBERCOM

END NOTES

[1] "National Security Strategy." December 2017.

[2] "Joint Publication 3-12: Cyberspace Operations." June 8, 2018.

[3] US CYBERCOM website. Accessed February 1, 2019. https://www.cybercom.mil/About/History/.

[4] Army Cyber, Accessed February 1, 2019. https://www.goarmy.com/army-cyber/timeline-of-army-cyber.html.

[5] Pomerleau, Mark. "Here's how DOD organizes its cyber warriors." Fifth Domain. July 25, 2017. Accessed February 1, 2019. https://www.fifthdomain.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors/.

[6] Lange, Katie. "Cybercom: How DOD's Newest Unified 'COCOM" Works." Department of Defense. October 12, 2018. Accessed March 9, 2019. https://www.defense.gov/explore/story/Article/1660928/cybercom-how-dods-newest-unified-cocom-works/.

[7] "National Security Strategy." December 2017.

[8] Pomerleau, Mark. "Here's how DOD organizes its cyber warriors." Fifth Domain. July 25, 2017. Accessed February 1, 2019. https://www.fifthdomain.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors.

[9] Lamothe, Dan. "How the Pentagon's cyber offensive against ISIL could shape the future of elite US Forces." The Washington Post. December 16, 2017. Accessed February 1, 2019.

https://www.washingtonpost.com/news/checkpoint/wp/2017/12/16/how-the-pentagons-cyber-offensive-against-ISIL-could-shape-the-future-for-elite-u-s-forces/?noredirect=on&utm_term=.1783dbdfa1a2.

[10] "National Security Strategy." December 2017.

[11] Martelle, Michael. "Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War against ISIL." National Security Archive. August 3, 2018. Accessed March 1, 2019. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil.

[12] Martelle, Michael. "Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL." National Security Archive. August 3, 2018. Accessed March 1, 2019. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil.

[13] Prajuli, Wendy A. "On social media, ISIL uses fantastical propaganda to recruit members." December 4, 2017. Accessed February 1, 2019. http://theconversation.com/on-social-media-ISIL-uses-fantastical-propaganda-to-recruit-members-86626.

[14] Byers, A. & Mooney, T. "Winning the Cyberwar Against ISIL: Why the West Should Rethink Its Strategy." May 5, 2017. Accessed February 15, 2019. https://www.foreignaffairs.com/articles/middle-east/2017-05-05/winning-cyberwar-against-ISIL.

[15] Lamothe, Dan. "How the Pentagon's cyber offensive against ISIL could shape the future of elite US Forces." The Washington Post. December 16, 2017. Accessed February 1, 2019. https://www.washingtonpost.com/news/checkpoint/wp/2017/12/16/how-the-pentagons-cyber-offensive-against-ISIL-could-shape-the-future-for-elite-u-s-forces/?noredirect=on&utm_term=.1783dbdfa1a2.

[16] Silverman, D., Collins, T., & Fussell, C. "Team of Teams: New Rules of Engagement for a Complex World." Published May 12, 2015.

[17] Byers, A. & Mooney, T. "Winning the Cyberwar Against ISIL: Why the West Should Rethink Its Strategy." May 5, 2017. Accessed February 15, 2019. https://www.foreignaffairs.com/articles/middle-east/2017-05-05/winning-cyberwar-against-ISIL.

[18] Moon, M. "The Pentagon is developing cyber warfare tools to fight ISIL." Engadget. July 16, 2016. Accessed February 1, 2019. https://www.engadget.com/2016/07/16/pentagon-joint-task-force-ares/.

[19] US CYBERCOM website. Accessed February 1, 2019. https://www.cybercom.mil/About/History/

[20] Zurkus, K. "Playing cyber defense is not enough to win: Sometime offensive attacks are a necessary part of the game." CSO. December 7, 2016. Accessed February 1, 2109. https://www.csoonline.com/article/3146642/playing-cyber-defense-is-not-enough-to-win.html.

[21] Farran, Lee. "US Hacker Squads Constantly on the Attack in New Cyberwar Strategy." Real Clear | Life. February 2019. Accessed February 1, 2019. http://www.realclearlife.com/military/u-s-cyber-squads-are-under-constant-attack-and-what-we-are-doing-about-it/.

[22] Joint Publication 1, Doctrine for the Armed Forces of the United States, July 12, 2017.

[23] Cohen, Rachel S. "CYBERCOM Chief: 133 Cyber Teams Will Be Insufficient as Adversaries Improve." Air Force Magazine. February 14, 2019. Accessed February 1, 2019. http://www.airforcemag.com/Features/Pages/2019/February%202019/CYBERCOM-Chief-133-Cyber-Teams-Will-Be-Insufficient-as-Adversaries-Improve.aspx/.

[24] Stanley A. McChrystal, David Silverman, Tantum Collins, and Chris Fussell. "Team of Teams : New Rules of Engagement for a Complex World."

[25] Garamone, Jim. "US Cyber Command chief discusses importance of operations." DOD News, Defense Media Activity. April 15, 2015. Accessed February 1, 2019. https://www.arpc.afrc.af.mil/News/Article-Display/Article/585122/us-cyber-command-chief-discusses-importance-of-operations/

[26] Nakasone, Paul M. "A Cyber Force for Persistent Operations." Joint Forces Quarterly. 1st Quarter 2019. Accessed March 7, 2019. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf.

TWENTY-FIRST CENTURY ISR TACTICS:

GROUND TO AIR SIGNALING THROUGH QR CODES

Unidentified Airmen perform remotely piloted aircraft operations at Creech Air Force Base, Nevada on 1 October 2015. (Photo by TSgt Nadine Y. Barclay, USAF)

By Maj John Long, USAF; Maj Amy Long, USAF Reserve; Capt Kasey Vaughn, USAF; TSgt Andrew Patry, USAF

BACKGROUND

Air Force leadership is actively pursuing human-machine paring as a method to rapidly collect, exploit, and communicate enemy presence and activity without active human control.[1] The Air Force is the right branch to lead this development because of its preponderance of intelligence, surveillance, and reconnaissance (ISR) assets, dedicated command and control (C2) weapon systems, and the corps of liaison officers embedded with joint Services' tactical warfighting staffs. The communications architecture to enable C2 autonomous collection will be taxed, possibly beyond the current capacity. The time is right to begin experimenting with ISR platforms as machine communicators through using Quick Response (QR) codes and imagery collection assets. Developing them can offer more tools to primary, alternate, contingency, and emergency (PACE) communication plans in the event voice communications or radio command links are disrupted by incidental or deliberate events.

Using QR codes and imagery assets may enable human-machine pairing for human-to-human communication (like passing information from tactical units to higher headquarters). With enough success, pairing QR codes and ISR collection opens the door for a variety of machine-to-machine communication strategies using codes to directly task autonomous collection, combat effects systems, or logistics tracking mechanisms. Developing QR signaling techniques would bring strengths and vulnerabilities, but there are ways to mitigate the vulnerabilities in combat scenarios.

WHY QR CODES?

A QR code is a high contrast image designed to store alphanumeric information. It is readable around 360 degrees, from multiple angles of observation and (by design) does not blend in with the environment. Unlike free-space lasers, QR codes can be pieced together if weather or urban obstacles interrupt a clear line of sight.[2] This means, airborne sensors can read the QR code from any point in their

orbit, from any angle, and construct the code from a broken collection. If weather, foliage or urban obstacles interrupt the line of sight, the message can still be received and understood. The sensor altitude would only matter if the pixel resolution is greater than the pixel of the QR screen. The QR code's easy recognition for human eyes, and readability by machine scanners, supports its application beyond a variety of commercial applications and can be adapted to similar military reconnaissance elements of information.

... QR codes can be pieced together if weather or urban obstacles interrupt a clear line of sight.[2]

The processing power required for QR scans is simple enough to fit on virtually any modern digital imagery sensor. Smart phone processing capabilities exceed the minimum requirements for scanning QR codes; so, military sensors, from the tactical to national levels, could be modified to interpret and transmit QR information. Since the processing requirements are minor, QR code interpretation can happen on the platform itself without requiring reachback support from advanced architecture and human exploitation. The two main ways QR signaling for military actions are beneficial: human-to-human communication and human- or machine-to-machine tasking.

The first is includes QR code and ISR collection assets as options for PACE plan development to promote human-to-human communication through the machine sensors. This means a human on the ground generates a QR code for an airborne sensor to collect. This is nothing more complicated than a technologically empowered, ground-to-air signaling (GTAS) technique (or QR-GTAS), replacing hand signals and flags with QR screens or projections.[3] After the QR-GTAS is read by the airborne sensor, a few simple processes can translate the scan into an alphanumeric output for the flight crew. Imagine an MQ-9 or F-16 pilot reading the next priority on the heads up display after the full motion video sensor pod spotted a coalition position with a QR-GTAS. The sensor would do all the work, and it would not matter if the pilot and ground-based tactical controller had effective voice communications. Two humans are making all the decisions, in this example, but they are relying on machine processes to encode and decipher the content.

Employing QR-GTAS for human-to-human communication also extends beyond dynamic C2 processes. Although ISR or strike coordination would need significant confidence, QR-GTAS could begin with benign experiments using airborne ISR as 21st-century carrier pigeons. If short-range radio or internet relay communication fails, QR-GTAS can pass situation reports for logistics or personnel status or updates to the enemy order of battle from ground-based scouts. This would look similar to commercial QR code usage for geocaching, banking, shipping, and automatically linking the user to a targeted web address.[4]

Once ISR collection of QR-GTAS gains enough confidence in human-to-human communication, it will be an easy transition to machine-to-machine communication. The United Postal Service already employs drones to deliver packages by flying an autonomous

CASEVAC 9-Line

Line 1: Landing zone (LZ) coordinates using an 8-digit grid system
Line 2: Call sign and frequency used by the unit at the LZ
Line 3: Patient priority status and patient count
Line 4: Special equipment
Line 5: Number of patients by type for aircraft configuration
Line 6: Security at the LZ
Line 7: Methods used to mark the LZ
Line 8: Patient's nationality
Line 9: Contamination with nuclear, biologic, or chemical weapons

A sample QR image generated to store and display the information in a casualty evacuation 9-Line. This information was generated for this article using the website http://GoQr.me, and the information is encrypted at no charge to the user.

route.[5] The parallel is direct. Combat outposts with a functional QR-GTAS capability could signal to an airborne or spaceborne ISR collection asset and automatically request a resupply. Instead of relying on humans, phones, or email, requests can be made across the battlefield in a single ISR mission. The Global Hawk, for example, can survey 40,000 square miles in a day.[6] At the same time, a drone is conducting reconnaissance and surveillance against the enemy it can be communicating logistics tracking mechanisms and preloading tasks to delivery drones.

The same programming required to read QR-GTAS for logistics can be applied to combat effects. A drone understands the grid coordinates and a specific action to apply, the difference between a resupply or munition is only a change in the payload. This is especially pertinent in combat scenarios involving drone swarms (i.e., autonomous drones of modular capability, size, and mission).[7] Swarms are poised to create a new form of unmanned warfare, replacing human-intensive remotely piloted aircraft like the MQ-9 with alternative control schemas. Swarm technology is still in the nascent stages, but the hardening mechanisms include looking for ways to enhance the swarm's resistance to electronic warfare. In a situation where autonomous, weaponized drone swarms are prevented from radio wave based commands, QR-GTAS could provide an option for trained, equipped and aligned joint terminal attack controllers to pass the same information and restrictions in a format machines are prepared to read and obey.

SECURING THE QR SIGNAL

There are some limitations. Adopting QR-GTAS only works for two-way transmissions when paired with other domains. For example, if the signaler on the ground presents a QR-GTAS to an airborne ISR asset for collection, the ISR asset would only be able to return the information using alternate delivery methods. Airborne sensors offer the opportunity to use many mechanisms of information warfare to deliver a response, but digital "dead-drops" on commercial internet service should not be overlooked. This is because the QR-GTAS could include a uniform rescource locator (URL) for a password-locked web page. In this digital "dead-drop", coalition forces could access the information with two methods of authentication: the URL address and the password, each sent through different mechanisms. Each time QR-GTAS is used, commanders should form a risk-to-gain calculation before making a decision. However, timing the transmissions, orienting the QR-GTAS to certain cardinal directions, or other encryption methods could be developed.

One consideration for secure QR-GTAS could be a variety of encryption techniques. Even civilian-sector QR codes allow using some encryption.[8] Focusing the QR-GTAS skyward offers some communications security for the ground-based signaler, but additional encryption methods are available if military users employ more than the visible spectrum. Infrared and hyperspectral imaging could tease out additional layers of information or employ military deception techniques if certain signaling stations are at risk of compromise.[9] Simple QR codes work with electronic ink, like electronic book screens. Organic light-emitting diodes (LEDs) produce thousands of colors and projectors could turn any command tent or building into QR-GTASs of varying sizes. Producing encrypted messages can be as easy as multiplexing the visible code against other, deliberately false messages, or as complicated as broadcasting several conflicting messages across the visible and infrared spectra simultaneously. In other words, the ground-based signaler and the airborne machine have all the parts and software they need to succeed today. Employment feasibility is limited to the creativity of the involved teams.

AIRPOWER IS EVOLVING

Now is the right time to test and develop QR-GTAS. While the Air Force develops robust artificial intelligence programs to process the sensing grid, it is also fusing cyber warfare and ISR career fields into an "information dominance" hybrid.[10] This merges intelligence professionals, communications officers, and information warriors.[11] These changes include grouping officers into promotion categories and fusing the 24th and 25th Air Force to merge the ISR and Cyber C2 mechanisms under unified leadership.[12] Put another way, the Air Force is merging talent and resource management systems to develop the future of how ISR, cyber systems, and coalition communications work against peer adversaries.

The Air Force's new information warfare professionals will continue to train, deploy and fight alongside the other element that should request this capability: Air Force Special Warfare (AFSW). Including combat search and rescue, close air support, and special reconnaissance missions, AFSW's tactical air control parties are rebranding their mission set to include multidomain C2.[13]

Combining the multidomain C2 with a resilient ISR command, control, and communication capability is overdue. The best place to make this change is with the Air Force's multidomain ISR professionals located alongside land domain warfighters, the tactical air control party's ISR liaison officers.[14]

The Air Force already identified the weapon system, allocated the people, and assigned the mission to ensure success within the ISR dominance flight plan. Updating tactical GTAS through QR signaling provides a tool to help achieve all these goals. Since most of this technology is available commercially, off the shelf, the techniques could be developed by private citizens or Service members with the technical proficiency to begin the work. The ground domain warfighters need to acknowledge the requirement and initiate entrepreneurial research, development, and experimentation. Doing this now can shape the way Air Force ISR and human-machine communication works in tactical scenarios against peer adversaries.

END NOTES

[1] Deputy Chief of Staff, A2 Intelligence Surveillance and Reconnaissance, Headquarters Air Force - A2, "Next Generation ISR Dominance Flight Plan: 2018-2028" 24 Jul 2018: 9,

[2] O'Neill, Mark. "What is a QR Code and How Does it Work?" Small Business Trends. 12 Feb, 2019. https://smallbiztrends.com/2015/05/what-is-a-qr-code.html Accessed on 7 Sept 2019.

[3] Training Circular (TC) 3-21.60 / Field Manual (FM 21-60), Headquarters, Department of the Army, Washington D.C., 17 March 2017. 3-1 and 3-25

[4] G.F., "Why QR Codes are on the Rise," The Economist, Nov 2017. URL: https://www.economist.com/the-economist-explains/2017/11/02/why-qr-codes-are-on-the-rise accessed on 6 Sep, 2019.

[5] Burns, Stephen. "Drone meets delivery truck." Longitudes: Navigating the trends of tomorrow. 22 Feb, 2017. URL: https://www.ups.com/us/es/services/knowledge-center/article.page?kid=cd18bdc2 Accessed on 5 November 2019.

[6] Limer, Eric. "U.S. Air Force Drone Crashes in California Starting Small Wildfire." Popular Mechanics. 22 June 2017. URL: https://www.popularmechanics.com/military/news/a27044/global-hawk-drone-crash/ Accessed on 5 November 2019.

[7] Kallenborn, Zachary. "The Era of the Drone Swarm is Coming, and we need to be ready for it" Modern War Institute. 25 October 2018. URL: https://mwi.usma.edu/era-drone-swarm-coming-need-ready/ Accessed on 6 Nov, 2019.

[8] Pearson, Jordan. "Encrypted QR Codes could Keep Devices Safe from Hackers," Motherboard: Tech by Vice. 27 February 2015. URL: https://www.vice.com/en_us/article/8qxed5/encrypted-qr-codes-could-keep-devices-safe-from-hackers Accessed on 6 November 2019.

[9] No Author listed. "Hyperspectral Remote Sensing" http://www.csr.utexas.edu/projects/rs/hrs/hyper.html Accessed on 6 November 2019.

[10] Deputy Chief of Staff, A2 Intelligence Surveillance and Reconnaissance, Headquarters Air Force - A2, "Next Generation ISR Dominance Flight Plan: 2018-2028" 24 Jul 2018: 9

[11] Losey, Stephen. "Farewell, Line of the Air Force: Massive officer category broken out into six groups," The Air Force Times. 21 October 2019. URL: https://www.airforcetimes.com/news/your-air-force/2019/10/21/farewell-line-of-the-air-force-massive-officer-category-broken-out-into-six-groups/ 6 November 2019.

[12] MSgt Steve Stanley, "ACC Commander holds town hall about 24th, 25th Air Force Merger," Air Combat Command Public Affairs, Joint Base San Antonio, TX. 11 July 2019. URL: https://www.jbsa.mil/News/News/Article/1901621/acc-commander-holds-town-hall-about-24th-25th-air-forces-merger/ accessed on 6 Sep 2019.

[13] No author listed. URL: https://afspecialwarfare.com/afspecwar-overview/ Accessed on 6 November 2019.

[14] Haley, Jaylan; Long, John; Sidwell, Melissa. "Resilient Command and Control of Airborne Intelligence Assets in the Theater Air Control System: a Contested, Degraded, Multi-Domain Imperative" Small Wars Journal. 27 April 2019. URL: https://smallwarsjournal.com/jrnl/art/resilient-command-and-control-airborne-intelligence-assets-theater-air-control-system Accessed on 6 November 2019.

MULTI-DOMAIN OPERATIONS: EXPANDING BATTLEFIELDS

An aerostat is prepared to launch during Cyber Blitz 19. The experiment/exercise pairing gave more than 30 organizations from across the Army, Navy, and Air Force a realistic first look at how the intelligence, information, cyber, electronic warfare and space battalion, or I2CEWS BN, could fight and win as part of a multi-domain task force. This photo was taken on 29 August 2019. (Photo by Edric Thompson)

By Maj Kimber Nettis, USAF (with contributions from Col Lori Winn, USAF)

"The Air Force, in conjunction with fellow joint warfighters, must adapt our thinking and culture to be able to seamlessly shift between domains, components, and regions to create high velocity, precision warfighting effects to satisfy the joint force commander's mission needs."

—Air Force MDO Implementation Plan 2018[1]

ABSTRACT

The operational environment in which United States (US) forces fight has changed. According to the 2018 National Defense Strategy (NDS), strategic competition among enemy states is the nation's number one threat.[2] The shift away from violent extremist organizations has led to grey-zone warfare, threats to civilian sectors from cyber-attacks, and threats to US military readiness through multiple domains.

This article seeks to guide readers through changes within the operational environment, driven by new technologies and threats, requiring multi-domain operations (MDO). In addition, it discusses the defensive side of multi-domain command and control (MDC2) based on the current operational test of the Mission Operations Group at Wright-Patterson Air Force Base (WPAFB), Ohio.

In recent years, the Department of Defense (DOD) turned its attention to the growing need for MDO. The NDS states, to "compete in this complex and contested security environment, the US must be prepared to operate across a full spectrum of conflict, [and] across multiple domains at once."[3] The US military Services took this guidance and began implementing differing forms of MDO operations. As the Air Force senior mentor for MDC2, Lieutenant General (Ret) Norman Seip, stated, "the goal of MDO operations is to create complex, simultaneous dilemmas …

for the enemy."[4] To do this, Service members must realize how the operational environment has changed (with the rise of space and cyber technologies) and how these changes affect access to information. Also, military members must realize battlefields now extend back to the home front, which presents new challenges requiring new solutions.

Some have argued[5, 6, 7], the DOD currently executes MDO and this is just a new Pentagon buzzword meant to elicit additional funding. This article looks at how warfare has evolved and why US forces should build new MDO doctrine. Additionally, it presents a framework to better understand basic MDO concepts when building offensive and defensive objectives at the tactical and operational levels of war.

The main impetus for change in how a military conducts warfare is based, largely, on changes in technology.

THE EVOLUTION OF WARFARE

The main impetus for change in how a military conducts warfare is based, largely, on changes in technology. When new technology is introduced, forces must adapt the scheme of maneuver and update their doctrine and tactics, techniques, and procedures to account for the new technology. This brief history on the evolution of warfare covers the main changes in doctrine sparked by changes in technology.

Since early wars, battles have been linear. One army lines up against another and draws swords, spears, or muskets and fights until one has decidedly triumphed. When one side was smaller or less capable of fighting in this traditional manner, guerilla warfare emerged as a balancing maneuver with tactics that included ambushes, sabotage, and raids. Then a change in technology (namely, machine guns) sent armies into trenches.

According to Nicholas Murray, "Trench warfare proliferated when a revolution in firepower was not matched by similar advances in mobility, resulting in a grueling form of warfare in which the defender held the advantage."[8] Trench warfare became known as a symbol of the futility of war, often leading to stalemates with high casualty rates.[9]

Then there was a change in technology and doctrine. During World War I, the Germans focused on the scheme of maneuver by implementing trench infiltration tactics while the British and French focused on technology by developing tanks to achieve victory.

Coming out of Vietnam, the US Army based its main fighting doctrine on the Air Land Battle.

Coming out of Vietnam, the US Army based its main fighting doctrine on the Air Land Battle. At that time, General Donn Starry was sent to Israel to understand the Yom Kippur War because the tempo, speed, and proliferation of new weapons was different from anything previously seen. He saw the importance of fighting an integrated air and land battle and how antitank, guided missiles changed battlefield tactics. He said, "the Army we have today, coming out of Vietnam, is not the Army we need going into the future."[10] General Starry took the lessons learned from the Yom Kippur War and started what is known as the Army's Big Five Modernization Program, which also inspired the Air Force's investment into stealth and precision standoff weapons.[11]

Doctrine changed again when the US encountered new threats, such as violent extremist organizations (VEOs). Since 2003, the US has faced, primarily, irregular warfare. Irregular warfare is described as "a violent struggle among state and nonstate actors for legitimacy and influence over the relevant populations."[12]

As the US was focused on VEO threats across the globe, a new form of warfare began to emerge. The reemergence of near-peer competitors brought about a need to focus on MDO as adversaries used new tactics, domains, and technology to threaten the US. These near-peer adversaries have contested the US in every domain, while increasing the speed of warfare through new technologies (such as artificial intelligence and hyper-sonic weapons). This increased speed of warfare leads to a decrease in time and space for leaders to make critical decisions.

MDO is the newest doctrine to emerge

from the DOD to counter near-peer threats. MDO is "a concept that the joint force can achieve a competitive advantage over a near-peer adversary by presenting multiple, complementary threats that require a response thereby exposing adversary vulnerabilities to other threats. It is the artful combination of multiple dilemmas, rather than a clear overmatch in terms of any particular capability that produces the desired advantage."[13] In other words, it is a way to provide effects in timing and tempo with which the enemy cannot compete.

One may wonder how MDO is different from fighting as a joint force. After all, the Goldwater-Nichols Act of 1986 was the fix to the inter-Service rivalry experienced during the Vietnam Conflict and the failed hostage rescue attempt in Iran in 1980.

Previously, MDO was more single domain focused, with coordinated effects and archaic command and control (C2) processes. Today's operations are layered or synchronized, but not fully integrated. The authorities for space and cyber forces are retained, largely, at the strategic or national level, while authorities for air operations remain at the operational level. Situational awareness capabilities are not designed to provide an integrated understanding of the complete battlespace spanning all domains, and C2 constructs do not provide the necessary agility to synchronize effects.[14]

Organizations, such as Air Force Warfighting Integrating Capability (AFWIC), are looking at how military leaders make decisions at a pace and scale equal to a near-peer competitor and how to create a common operating picture which connects the right sensor to the right processor and, ultimately, to the right shooter. Also, they are working to ensure the right systems and people are in place for MDC2 and distributed C2.

The Army has created its first unit to combine long-range targeting, hacking, and jamming and space to support the move to MDO. The unit is called intelligence, information, cyber, electronic warfare, and space (I2CEWS). The I2CEWS unit was stood up at Fort Lewis-McChord, Washington.[15]

Before discussing domain considerations, it is worth identifying the current doctrine held by one of the US' top competitors. Russia uses what has been termed "hybrid warfare" which combines conventional, irregular, political, and information warfare. Dr. Francis Hoffman, a distinguished research fellow at the National Defense University in Washington, DC, states that hybrid threats are adversaries who employ a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the same time and in the same battlespace to obtain their political objectives.[16] Russia uses new information warfare tactics (such as meme warfare) to create chaos among populations (such as in the US). Also, Russia has been identified in several election meddling campaigns including Ukraine's, France's, and the US'.[17]

Russia also includes using tactical nuclear weapons in its overall doctrine called "New Generation Warfare". This whole-of-government approach seeks to "manipulate the adversaries' perception, maneuver its decision-making process, and influence its strategic behavior while minimizing (compared to the industrial war era) the scale of kinetic force use".[18]

DOMAIN CONSIDERATIONS

After reviewing warfare evolution and the need for MDO, looking at the domains is necessary to set a foundation and ascertain where operations are occurring. The traditional five domains are air, sea, land, space, and cyberspace. Jared Donnelly and Jon Farley, Air Command and Staff College professors in Montgomery, Alabama, state that a definition of "domain" is in order as we are starting to see how nonphysical domains are having real effects on missions.[19] They recommend the definition of a domain given by Jeffrey Reilly, the Director of the MDO Strategists Concentration at Air Command and Staff College. He defined it as "a critical macro maneuver space whose access or control is vital to the freedom of action and superiority required by the mission".[20] It is an area into which one must have access and in which one can make effects. It does not have to be physical.

A sixth domain has been under consideration due to the rise in information operations. It is the cognitive domain. General Robert Brown, Commander of US Army Pacific,

stated that the cognitive domain should not only be considered a domain but, in his opinion, it is the most important domain.[21] The cognitive domain is becoming more important with the introduction of space and cyber technologies because these have exposed the populace to more sources of information, making the traditional gatekeepers inadequate and making it easier for any actor, state or nonstate, to effect this domain. The traditional gatekeepers, such as CNN or the Wallstreet Journal, are being outpaced by information shared on Twitter, Facebook, and other social media platforms.

A sixth domain has been under consideration due to the rise in information operations.

A good example of how the cognitive domain is becoming more critical can be seen in the book, *War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century*. The author, David Patrikarakos, describes how Twitter is the main source of vital, timely information in the Russian-Ukrainian conflict. Patrikarakos is a reporter on the front lines of the conflict and consistently gets his most up-to-date information from Twitter users. There are pros and cons when it comes to this kind of speed for receiving information. Patrikarakos writes about seeing the vastly different reports from the pro-Russian and pro-Ukranian sides. As a journalist, he is concerned about writing the facts about a situation, yet he sees false information "re-tweeted thousands of times".[22] He said, "It wasn't propaganda I was witnessing, it was the reinvention of reality. And social media was at its heart".[23] Patrikarakos also stated that he saw a "mass enlistment" that included noncombatants and civilians.[24] These new participants in the operational environment can have real effects on the battlefield.

The enemy realized, a long time ago, it cannot compete with the US in a battle of military might, therefore, other means of competition became the ways to win the battle of resources and power. Patrikarakos said, "I began to understand that I was caught up in two wars: one fought on the ground with tanks and artillery and an information war fought largely, though not exclusively, through social media. And, perhaps counterintuitively, it mattered more who won the war of words and narrative than who had the most potent weaponry."[25]

The enemy realized, a long time ago, it cannot compete with the US in a battle of military might, therefore, other means of competition became the ways to win the battle of resources and power.

An example of how social media can change a battlefield is found in a recent article entitled, "With Just $60 and Internet Access, Researchers Found and Tracked NATO [North Atlantic Treaty Organization] Troops and Even Tricked Them into Disobeying Orders".[26] The author, Ryan Pickrell, illustrates the importance of a commander realizing the entirety of the operating picture. "Researchers with NATO's Strategic Communications Center of Excellence used open-source data (primarily social media) to identify 150 soldiers, locate multiple battalions, track troop movement, and persuade service members to leave their posts and engage in 'undesirable behavior' during a military exercise".[27] The researchers were red team members, however, the adversary can be anyone with internet access and a cause.

THE EXPANDING BATTLEFIELD

Due to new technologies, state and nonstate actors can have tremendous impacts on US technology and military operations from anywhere in the world. The necessary technology costs little and is readily available to anyone. Not only can the enemy have an impact throughout an area of operations (AO), but can hit American soil. Patrikarakos explains the extended battlefield as follows.

> "Unconventional forces may strike in grey-zone operations long before conventional troops officially go to war, if they ever do. The first blow may be struck by proxies (like the Russian-backed Ukrainian rebels), deniable forces (like the 'Little Green Men' in Crimea or Chinese state-owned fishing vessels in the South China Sea), non-

military government agencies (like the Chinese Coast Guard), or 'lone wolves' inspired to act by social media but with no connection to the enemy. It may come from cyber-attacks, whose origin is notoriously hard to figure out, and which may involve months or years of careful preparation but take effect in seconds."[28]

The video, "Evolving Threats to Army Installations in a Complex World", produced by the US Army, explains how the enemy can stop troops or demoralize them before they leave the US or their home installation. If the enemy is successful, the troops will never make it to the battle across the world or, when they do, will be at a huge disadvantage.[29]

Figure 1 is from the Army's "Operational Framework Six Physical Spaces".[30] It shows the traditional concept of the understood battle space (from Rear to Deep), includes the Strategic Support Area and Operational Support Area (blue space), and the Deep Maneuver Area and Deep Fires Area (red space). The military is beginning to realize, through new technologies, the safe haven of home base (or just being in the US) is no longer safe. A state or nonstate actor has the means to accomplish effects that could cripple the US. Some examples are:

- State actors who attack critical infrastructure from across the world.
- Nonstate actors who attack space systems or jam Global Positioning Systems.
- A lone wolf flying a commercial drone over a military base with explosives and blowing up munition areas (such as was seen in Ukraine in 2017).
- An Islamic State sympathizer who attacks water supply systems in the US.

The US Army has begun seeing installations as, not only strategic support areas, but close areas that must be guarded. Also, five Air Force bases, including Wright-Patterson in Ohio, have initiatives to protect bases from new multi-domain threats and have reached out to the community to become involved in various exercise scenarios. Communities are

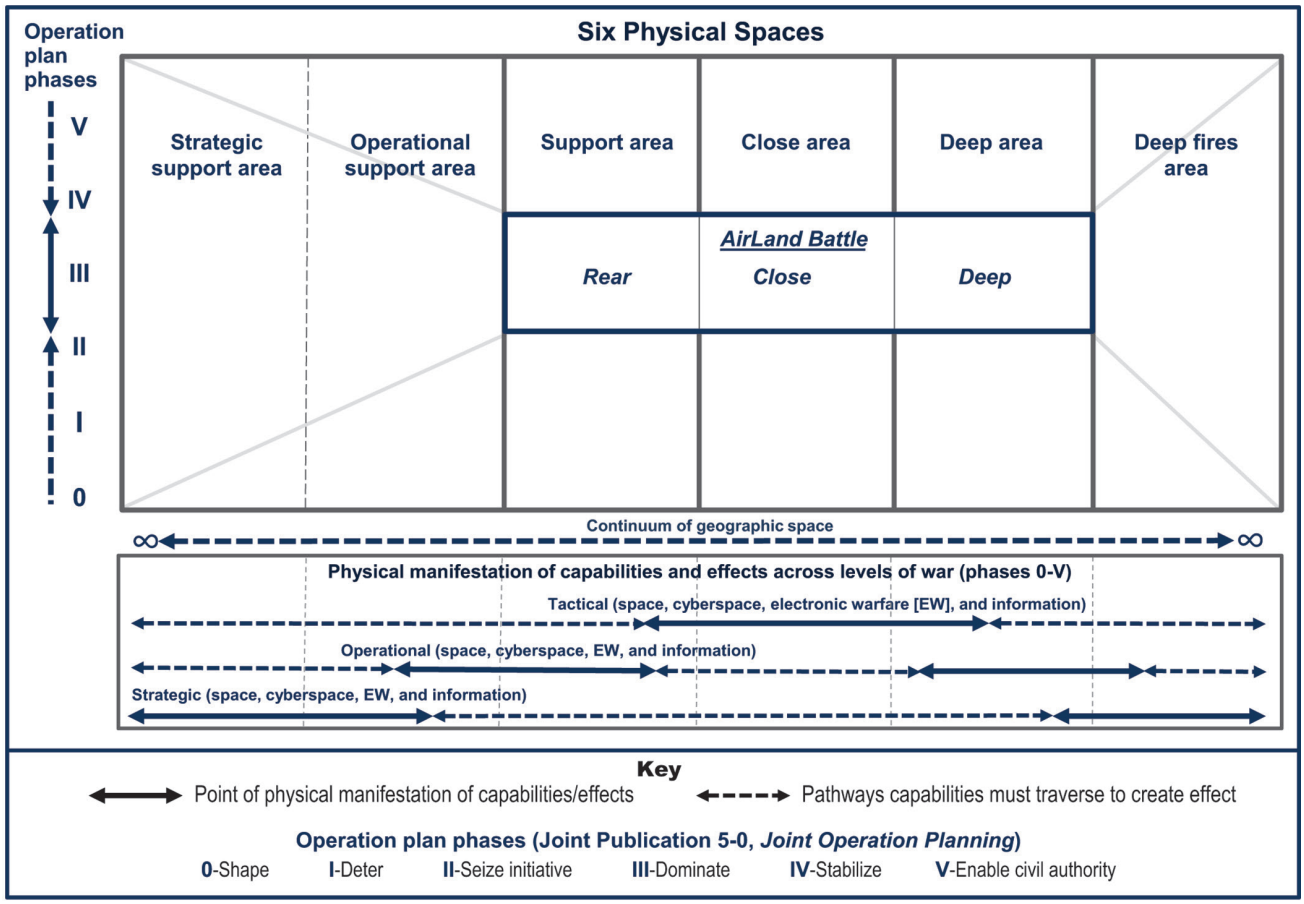


Figure 1. The Army's Operations Framework Six Physical Spaces (Courtesy of General David Perkins, USA (Ret))

important to protect and include in exercises because strikes on the civilian sector can impact on-base readiness. Of course, DOD agencies must determine the best organizations with whom to partner and work out associated legalities when involving nongovernmental entities. The 2019 Cyber Guard Exercise combined US Cyber Command, National Guard, and commercial enterprises to solve cyber threats. More of this type of integration will be required as new threats emerge.

Great strides have been made in securing the US' critical infrastructure and key resources through the Department of Homeland Security. However, the concept of seeing home installations as part of the battleground is new, especially for the Air Force.

DEFENSIVE MDO

WPAFB is leading the charge in realizing the installation's role in MDO. While most of the Air Force is focused on MDO at the operational level (i.e., using MDC2 offensively), WPAFB is focusing on using MDC2 defensively.

The 88th Air Base Wing, under Wing Commander, Colonel Thomas Sherman, is reshaping the wing structure to support defensive MDC2 at the installation level. Just as an air operations center relies on the C2 structure to support air war operations, an installation's security relies on a well-established C2 system under one commander.

Colonel Lori Winn, the 88th Mission Operations Group (Provisional) Commander stated, "the Air Force must see the installations as warfighting platforms like an aircraft carrier [from which] capabilities are launched. Our nation is hemorrhaging intellectual information and certain installations are critical when it comes to deploying passengers and cargo to the AO."[31]

The effort at WPAFB is two-fold. It involves a new organizational structure called the Mission Operations Group and a new fusion function for C2, called the Installation Command and Control Cell.

WPAFB is conducting a trial in which the existing Communications Group has been rebranded the Mission Operations Group (Provisional) with two assigned squadrons (i.e., the 88th Operations Support Squadron and 88th Communications Squadron), two attached squadrons (i.e., the 88th Security Forces Squadron and 788th Civil Engineer Squadron) and one attached staff agency (i.e., Wing Information Protection). This organizational alignment creates a single, multi-domain group (air, land, and cyber) focusing on installation protection and defense and ensuring a safe, secure, and resilient installation protecting and defending people, critical infrastructure, and information. At the conclusion of this trial, the wing will assess the results and determine courses of action.

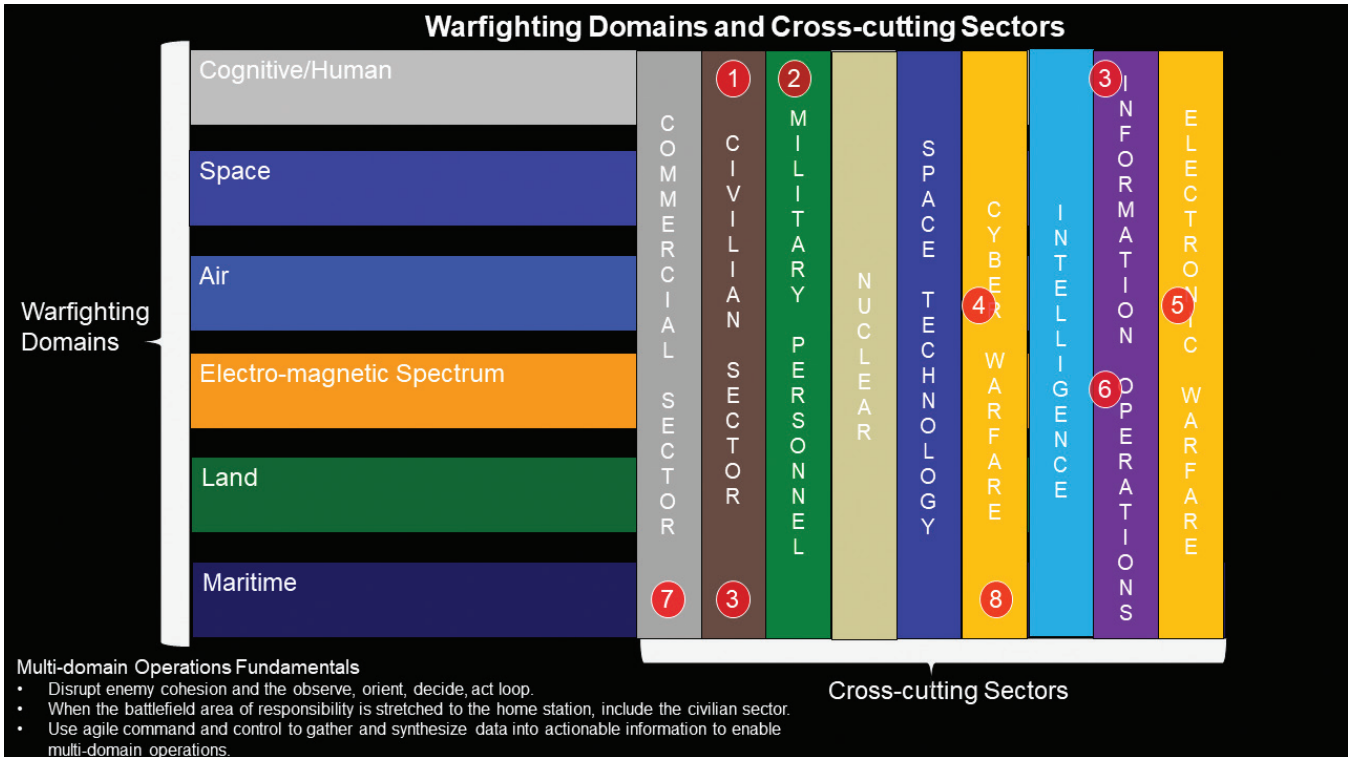
The second experiment at WPAFB is fusing all the base's operations centers (i.e., the base defense operations center, airfield management operations, fire dispatch, and cyber intelligence operations center) to create whole-of-installation situational awareness. This enables the wing commander to receive timely and accurate information concerning what is happening on the base. Also, WPAFB is the perfect place to exercise this new C2 structure because it hosts high-level events, such as the Air Force Marathon and annual senior leaders' Corona Top meeting, requiring integrated security and coordination.

In a complex world with evolving multi-domain threats, the outcome of experiments at the five bases will help shape the future of installation defense.

MDO FRAMEWORK

The framework (figure 2) was created to help identify cross-cutting sectors affecting all domains. This framework is used in various applications and has proven beneficial to understanding MDO concepts and is useful to commanders and planners at various levels. Also, the framework was made into a chart to educate students participating in a deterrence course at Barksdale Air Force Base, Louisiana, falling in line with General Goldfein's comments at the 2019 Air Force Association event, that MDO is the "new deterrence".[32]

The examples in figure 2 are for planners to consider offensive and defensive options as they relate to military objectives. The touchpoints are labeled in red and show how MDO operations affect cross-cutting sectors in multiple domains. The touchpoints should link directly to a defined military objective to achieve a commander's intent.



Planners need to think offensively and defensively. Answering the following questions and reviewing comments can help planners adjust their way of thinking, especially when considering many of the answers are synergistic.

Circle 1: (This regards election legitimacy.) Was the United States (US) attacked during the last presidential election? Could the US have defended against possible attacks better? Could the US influence foreign elections to oust an opposition party? Would this be a good use of the domain? What other legal and ethical matters bear discussion in this regard?

Circle 2: How can the US use social media to effect military personnel? What information can the US Government learn from its posts and interactions? Can the US have effects on the battlefield by targeting personnel using social media?

Circle 3: (This relates to moving a carrier strike group (CSG).) How does the American public react to the movement of a Chinese aircraft carrier? How does the US hope to influence the thoughts of the enemy population if America moves a CSG near another country's shores?

Circle 4: Can the US steal, degrade, or destroy enemy aircraft via a cyber attack?

Circle 5: What aircraft can jam an enemy's radar, enabling other operations to take place unnoticed? How can the US prepare to defend against electronic warfare attacks?

Circle 6: (This concerns adjusting the content of an online news site to sway the readers away from their group's fundamental beliefs.) Have any of the US' websites been hacked? Does the US ever hack the enemies' sites? (The US can affect the electro-magnetic spectrum and cognitive domains through information operations.)

Circle 7: The 2017 NotPetya virus attack on A.P. Moller-Maersk is an example of how the commercial sector impacts other domains. The ransomware shut down the world's largest shipping conglomerate (which is responsible for 1/5 of the world's shipping capacity).[33] A.P. Moller-Maersk is used by the Department of Defense. How vulnerable is the US to this type of attack?

Circle 8: What if the US does not have time to move a CSG, can the US steal one? Does the US have any vulnerabilities on its systems?

Figure 2. MDO Framework with touchpoint examples labeled in red.

CONCLUSION

The US military uses the language of "winning hearts and minds" but tends to lean toward the "warheads on foreheads" method of war. The reason for this lies within the processes by which war is conducted. It is easier to put a munition on a target than conduct a well-coordinated information operations campaign. Future commanders need to realize the full potential of their nonkinetic and kinetic options. The problem is, there is not a sufficient process in place, or technology available, for fully integrating kinetic and nonkinetic operations. The joint targeting cycle and kill chain need to be updated to include a seamless integration of new domains for future MDO conflicts.

Future commanders need to realize the full potential of their nonkinetic and kinetic options.

Understanding the current environment and how it has expanded domains will help military leaders make informed decisions that move toward the right technologies to fuse the disparate pieces. Each domain can have a tremendous effect on the superiority of other domains. The first steps are recognizing, defining, and building authorities and tools for use in the additional domains. Looking at a new framework to see how the domains and cross-cutting sectors interact helps commanders and planners build MDO objectives to exercise for the next war. MDO requires an understanding of one's own domain and a desire to bridge the gaps to other domains to achieve dominance over the enemy's ability to do the same. There is no need for a substantial reorganization, instead, there is a need for considerable force reeducation. All military members, especially planners, need to expand their perspective beyond current domains and into emerging cyber and space domains. Furthermore, better tactical and operational linkages across sectors need to exist to enable a rapid, dynamic response to future events.

The past paradigm of joint education focused on integrating land, sea, air, and space. The new paradigm must reconsider the sector approach, using capabilities that provide cross-domain effects simultaneously. The military must create complex problems for the enemy while defending against new tactics being demonstrated in hot spots around the world.

Understanding the current environment and how it has expanded domains will help military leaders make informed decisions that move toward the right technologies to fuse the disparate pieces.

Service members must continue to explore home-station vulnerabilities and how the battlefield has enlarged to encompass US communities and units supporting the AO. The US can maintain superiority on the battlefield by extending the enemies' battlespace and presenting challenges in all domains simultaneously. This may require restructuring or rethinking operations but, in the end, the one who adapts is the one who wins the war.

Disclaimer: The views expressed are those of the author and do not necessarily reflect the official policy or position of the Department of the Air Force or the US Government

Major Kimber Nettis is the Deputy Director for the Cyber Professional Continuing Education Program in the School of Strategic Force Studies at the Air Force Institute of Technology at Wright-Patterson Air Force Base. She holds a Master of Arts in Homeland Security and a Master of Arts in Christian Ministry.

END NOTES

[1] *Air Force Multi-domain Operations Implementation Plan* (Washington DC: The Pentagon, 2018)

[2] *National Defense Strategy* (Washington DC: Office of the Secretary of Defense, 2018).

[3] *Ibid.*

[4] Lt Gen (Ret) Seip, Norman, "Multi-Domain Operations", Speech for Cyberspace 200 Course, Air Force Institute of Technology, January 30, 2019.

[5] Michael Spirtas, Toward One Understanding of Multiple Domains, C4ISRNET, May 1, 2018

[6] Colin Clark, Multi-Domain Operations: Insights from Lockheed Martin, Breaking Defense, September 18, 2019

[7] Sydney Freedberg Jr., All Services Sign on to Data Sharing-But Not to Multi-Domain, Breaking Defense, February 8, 2019

[8] Murray, Nicholas, *The Rocky Road to the Great War: The Evolution of*

Trench Warfare to 1914, (Potomac Books, Washington DC, 2013).

[9] Griffith, Paddy, *Battle Tactics of the Western Front—The British Army's Art of Attack 1916–18*, (Yale University Press, 1996).

[10] General Brown, Robert, "Multi-Domain Operations", Future Warfare, Perception Man, 2019, https://www.youtube.com/watch?v=ahdSysH_pGw

[11] Goure, Dan, *A New Joint Doctrine for an Era of MDO, RealClear Defense*, October 11, 2019, https://www.tradoc.army.mil/Publications-and-Resources/Article-Display/Article/1987883/a-new-joint-doctrine-for-an-era-of-multi-domain-operations/

[12] The Irregular Warrior, 4 October 2015

[13] Taylor, Curt and Kay, Larry, *Putting the Enemy Between a Rock and a Hard Place: Multi-Domain Operations in Practice*, Modern War Institute, August 27, 2019, https://mwi.usma.edu/

[14] 705th Training Squadron, 13O Initial Skills Training Curriculum, 2019.

[15] Freedberg Jr., Sydney J. and Clark, Colin, *Breaking Defense, Hack, Jam, Sense, and Shoot: Army Creates 1st Multi-Domain Unit*, January 24, 2019.

[16] Hoffman, Francis, US National Defense University.

[17] Mueller III, Robert S., Report On The Investigation Into Russian Interference In The 2016 Presidential Election, Washington, DC, March 2019. https://www.justice.gov/storage/report.pdf

[18] Adamsky, Dmitry, "*Cross Domain Coercion: The Current Russian Art of Strategy*," Security Studies Center, 2015.

[19] Jared Donnelly and Jon Farley, *Defining the "Domain" in Multi-Domain, Over the Horizon*, September 17, 2018, https://othjournal.com/2018/09/17/defining-the-domain-in-multi-domain/

[20] Reilly, Jeffrey, OTH Video: Beyond the Theory – A Framework for MDO, April 13, 2018, https://othjournal.com/2018/04/13/oth-video-beyond-the-theory-a-framework-for-multi-domain-operations/

[21] General Brown, Robert, "MDO", Future Warfare, Perception Man, 2019, https://www.youtube.com/watch?v=ahdSysH_pGw

[22] David Patrikarakos, *War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century*, (Basic Books: New York, 2017), 2.

[23] Ibid.

[24] Ibid.

[25] Ibid., 3.

[26] Ryan Pickrell, "With Just $60 and Internet Access, Researchers Found and Tracked NATO troops and Even Tricked Them Into Disobeying Orders," Business Insider, February 19, 2019, https://www.businessinsider.com/officials-tricked-nato-troops-into-disobeying-orders-with-social-media-2019-2

[27] Ibid

[28] David Patrikarakos, *War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century,* (Basic Books: New York, 2017), 4

[29] Office of the Deputy Assistant Secretary of the Army (Strategic Integration), Trending Threats: Driving the Next Evolution for Our Military Installations, October 16, 2017, https://www.army.mil/article-amp/195390/trending_threats_driving_the_next_ev

[30], David G. Perkins, *Multi-Domain Battle: Driving Change to Win in the Future, Military Review* (Army University Press, Jul-Aug 2017), p 10.

[31] Col Lori Winn, Speech for AFCEA, Installation Mission Assurance and MDO, January 17, 2019

[32] Goldfein, David, Air Force Air, Space, and Cyber Conference, September 17, 2019, https://www.youtube.com/watch?v=wyQG29uiiy8

[33] Andy Greenberg, The Untold Story of NotPetya, The Most Devastating Cyberattack in History, *Wired*, September 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

ADDITIONAL REFERENCES

Major Albert Harris III, Air and Space Power Journal, Preparing for Multi-domain Warfare, Fall 2018, Pgs 45-61.

Brian Willis, Over the Horizon, MDO at the Strategic Level, Sept 17, 2018, https://othjournal.com/2018/03/02/multi-domain-operations-at-the-strategic-level/

Department of the Air Force, Memorandum for all Commanders and HAF Staff, Multi-Domain Command and Control (MDC2) Implementation Plan, June 25, 2018.

Sydney J. Freedberg Jr., Breaking Defense, No Safe Place in Next War: The Army's Expanding Battlefield, September 22, 2017

Major Albert Harris III, Air and Space Power Journal, Preparing for Multi-domain Warfare, Fall 2018, Pgs 45-61.

Brian Willis, Over the Horizon, MDO at the Strategic Level, Sept 17, 2018, https://othjournal.com/2018/03/02/multi-domain-operations-at-the-strategic-level/ <https://othjournal.com/2018/03/02/multi-domain-operations-at-the-strategic-level/>

Department of the Air Force, Memorandum for all Commanders and HAF Staff, Multi-Domain Command and Control (MDC2) Implementation Plan, June 25, 2018.

Sydney J. Freedberg Jr., Breaking Defense, No Safe Place in Next War: The Army's Expanding Battlefield, September 22, 2017

MULTI-DOMAIN WARFARE OFFICER, THE 13O

United States Air Force's multi-domain warfare officers will wear multi-domain warfare officer wings on their uniforms, shown in the photo taken on 18 October 2019. The new career field will be the air component's core manning and provide continuity, breadth, and depth of experience at the operational level of war. (Photo by Shelton K. Keel)

By Col Francisco M. Gallei, USAF

BACKGROUND

On June 25, 2018, the Chief of Staff of the Air Force (AF) released the AF's Multi-Domain Command and Control (MDC2) Implementation Plan. This plan details how the AF will enhance its command and control (C2) capabilities, and is distinct from the draft *Joint MDC2 Campaign Plan*. The implementation plan and the National Security Strategy, "clearly articulate why we must rapidly prepare for a peer fight". To do so requires "harnessing the vast amount of information joint and allied sensors gather, fusing it quickly into decision-quality information, and creating effects, simultaneously, for any domain or component from anywhere in the world".[1]

Historical analysis of C2 assignments highlighted, 90% of officers with a C2 tour never accomplished a second C2 tour, and those with more than one C2 tour were not deliberately developed. Critically, the numbers of air operations center (AOC) directors, division chiefs, and deputy division chiefs with prior AOC experience is less than 10%.[2] At the end of 2017, the MDC2 enterprise capability collaboration team (ECCT) (a temporary AF organization stood up to examine the best way to fill a capability gap once it is identified), found two critical gaps. The first is institutional competency to "employ military forces" at the operational level of war, and the second is the lack of a method to deliberately develop "operational-level breadth" and expertise in joint and multi-domain operations planning.[3] These critical gaps are direct results of how the AF mans and provides resources for air components.

The AF's *MDC2 Implementation Plan* has three lines of effort (LOE): C2 operating concepts, advanced technology, and support structures for C2. One of the tasks within the support structures for C2 LOE is developing and establishing "an operational-level C2 ca-

reer field (13O) including all activities needed for effective career-field management".[4]

THE DEFINITION OF A 13O

The new 13O operational-level C2 career field members are known as multi-domain warfare officers. The 13O students will receive training in operational art and design and integrating multi-domain capabilities, up to the special access program/special technical operations level to lead the AF in key warfighting positions at the AF (and joint) operational level of war C2 enterprise. Specifically, the training provides personnel "principles, methods, and practices pertaining to joint organizational structures, operational command and control architectures, joint planning processes and execution, and multi-domain capabilities and employment considerations".[5]

The 13O students will receive training in operational art and design and integrating multi-domain capabilities, up to the special access program/special technical operations level to lead the AF in key warfighting positions at the AF (and joint) operational level of war C2 enterprise.

The 13Os will be the air component's core manning, providing continuity, breadth, and depth of experience to the operational level of war. At the air-component level, they will not only develop air-component plans but will integrate and plan with joint forces. This includes planning with joint and coalition liaisons (such as a battlefield coordination detachment; special operations, naval aviation, Marine Corps aviation, and AF liaison elements; and area air and missile defense centers) assigned to the air component, particularly the AOC. Additionally, they will be closely tied to, and planning with, their higher headquarters (whether it is a combatant command or a joint task force). Multi-domain operations is about integrating potential capabilities from the start of the planning process to its execution; and it is, inherently, joint.

The initial implementation plan has 13Os filling positions at the air-component level. The AF will work with the combatant commands to determine their needs and assign 13Os to headquarters based on those needs.

WHAT 130S DO IN THE FIELD

The 13Os are expected to lead component and joint planning efforts by providing commanders plans to optimize multi-domain capabilities and create multiple dilemmas for the enemy, regardless of their joint, coalition, or interagency partner affiliation. As experts in joint planning and multi-domain capabilities, they will be able to help the commander "visualize" multiple battlespaces and facilitate rapid decision making. They will have continued exposure from operating at the operational level of war through multiple assignments. This will create officers with breadth and depth in operational-level C2 based on experience versus the "touch and go" process of the past.

Not everyone at the air component will be a 13O, however, 13Os will be the core cadre. Other Air Force specialty codes (AFSCs) will continue to be part of the air component to bring current tactics, techniques, and procedures and ideas to the operational level of war. The other critical AFSCs bring their experiences and currency in air, space, and cyberspace operations to ensure new ideas are integrated into planning and executing multi-domain operations. As the core cadre, however, 13Os will fill critical positions as AOC team chiefs; division chiefs/directors; deputies; and, eventually, as AOC commanders.

Upon selection and IST completion, 13Os will spend the remainder of their AF careers at the operational level of war C2 enterprise.

Those selected to become 13Os undergo a 20-week initial skills training (IST) course conducted twice a year by the 705th Training Squadron (TRS), 505th Test and Training Group, 505th Command and Control Wing (CCW), Hurlburt Field, Florida. TRS' functional and career field manager, with a separate development team, selects the board and provides guidance to shape future 13O leaders. Two cross-flow boards, selecting 25 students for each class, are expected annually. Primarily, the boards will target senior captains and

majors. Upon selection and IST completion, 13Os will spend the remainder of their AF careers at the operational level of war C2 enterprise.

The career field is expected to consist of approximately 550 senior captains and field-grade officers from a diverse background of operations and select support career fields. In addition to the 13O IST Course at Hurlburt Field, Air Command and Staff College, Multi-domain Operational Strategist program graduates have an opportunity to cross flow. There will be a limited number of direct-entry opportunities for individuals who have the requisite knowledge, skills, and abilities based on experience.[6]

HOW TO APPLY

The two boards, conducted in the spring and fall, are preceded with a personnel services directory message from the AF Personnel Center. Successful, multi-domain operations requires a broad range of foundational experience and tactical expertise. The following are eligibility criteria. Applicants must be:

1. Rated or nonrated operations AFSCs (11X, 12X, 13X, 14X, or 17X).
2. Mission ready/combat mission ready in a combat mission design and series (or equivalent combat system (e.g., space-based infrared system or AC-130, distributed common ground system) for at least 36 months.
3. Rated officers with 96 operational flying-duty-assignment months (gate 1 complete) (long-term duty not involving/including flying will be considered on a case-by-case basis). Air Force Instruction (AFI) 11-401, Aviation Management. Rules and restrictions apply.
4. Worldwide deployable ("limited" is acceptable depending on the specific restriction).
5. Top secret/special compartmented information eligible.

Select support officers will be considered. All those selected will incur a 2-year active duty service commitment in accordance with AFI 36-2107, Active Duty Service Commitments.[7]

OUTPLACEMENT

The first class of students began training at the 505th CCW on May 28, 2019 and graduated from the 20-week IST course on October 9, 2019. The first 27 students were assigned to the geographic AOCs (603rd, 607th, 609th, 612th, 613th), 505th CCW, 614th Combined Space Operations Center, and the National Defense Space Center. In addition to sending newly minted 13Os to the aforementioned locations, it is expected they will receive assignments to the 601st AOC and the newly created 616th Operations Center. Future graduates will be placed in other functional operations centers, on air component staffs, at geographic and functional combatant commands, and in other operational headquarters that desire officers steeped in operational art and design who can seamlessly integrate and execute multi-domain and joint capabilities.

The class that began January 2020 will be the first total-force-integration class with students from the National Guard.

Col Francisco M. Gallei is the Commander of the 505th Test and Training Group at Hurlburt Field, Florida.

END NOTES

[1] CSAF Implementation Plan, 25 June 2018.

[2] 13OXX Roadshow Slide Presentation, November 2018.

[3] MDC2 ECCT Force Development Working Group (FDWG) Phase I Gap Analysis Paper, unknown date.

[4] CSAF Implementation Plan, 25 June 2018.

[5] Plan of Instruction (Technical Training) Multi-Domain Warfare Officer. POI: R3OBR13O1 01A (PDS Code: 999). 505th Command and Control Wing, 505th Training Group, 705th Training Squadron, 28 May 2019.

[6] Bullet Background Paper on 13O Crossflow Program, Col Jeff Burdett, unknown date.

[7] Multi-Domain Command and Control Officer (13OX) Selection Board—Call for Nominations, PSDM 18-97, 10 December 2018.

Air Control Communication

The newly developed Air Control Communication multi-Service tactics, techniques, and procedures (MTTP) publication (dated November 2019) establishes communications tactics, techniques, and procedures (TTP) for tactical (TAC) command and control (C2) to manage air operations and control airspace and aircraft. It also establishes TTP for force packaging and direct air support coordination, air-to-air (A/A) communication, A/A intercepts, threat A/A warning, threat surface-to-air warning, and air-to-surface communication. This MTTP publication applies to all TAC C2 airspace control elements and warfighters conducting air operations in areas of responsibility (AORs) managed by the joint force commander (JFC) and overseen by the airspace control authority (ACA) in accordance with the JFC-signed airspace control plan (ACP) and airspace control order (ACO). Operational and exercise planners can use this publication to inform the ACP, ACO, the special instructions, area air defense plan, and rules of engagement for an AOR.

Joint All-domain Command and Control (JADC2):

ALSA's top research priority is joint all-domain command and control (JADC2). The Multi-domain Command and Control (MDC2) Campaign Plan was released in August 2019 to develop joint, integrated, multi-domain solutions to provide operational and tactical warfighters agile and resilient command and control (C2) and battle management capabilities. Its scope is to provide near term and midterm efforts to develop capabilities at the operational level, and below. These capabilities are needed to complete kill chains via any sensor, shooter, or C2 node and build the capability to synchronize hundreds of kill chains in multiple hours, regardless of domain or functional ownership.

Each Service is working its technological input into the JADC2 infrastructure by holding joint working groups, planning conferences, and operational vignettes ensuring their solution integrates with the joint solution. Also, the Services are coming together and working on a joint solution.

The Doolittle Games, lead by the Air Force Warfighting Integration Center (AFWIC) and hosted by the Curtis E. LeMay Center for Doctrine Development and Education in February 2019, is a good example of how the Services are integrated. The event had 54 players from each Service and some coalition partners (e.g., Canada, The United Kingdom, and Australia). The purpose of the games was to test and refine the Air Force's concept, developed by AFWIC, for distributed JADC2 as a joint node able to complete distributed kill chains while under attack (even during degraded communication scenarios).

Let ALSA know how we can get involved.

Dynamic Targeting/Dynamic Rescue

National Defense Strategy shifted focus from counterinsurgency operations to peer competitions. To better compete, the National Defense Strategy tasks forces with aligning people, resources, and readiness to win against peer adversaries in all domains.

As ALSA prepares to rewrite its Personnel Recovery MTTP publication, the focus is shifting from recovery forces having freedom of maneuver and clear communications across the battle space towards peer combat. This is where recovery forces are contested in all domains and must work jointly to set the conditions for a successful recovery. These forces must posture to provide enduring support while continuously tracking multiple isolated personnel across the battlefield. The emphases on contested domains and multiple isolated personnel are the overarching themes as doctrine evolves.

ALSA challenges all personnel recovery experts to overrule the status quo and redefine the emerging TTP needed for successful recovery operations in peer contested spaces.

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**	16 JUN 17	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: Revision**
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: Current**
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: Current**
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: Current**
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: Current**
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: Current**
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: Current**
BIOMETRICS *Multi-Service Tactics, techniques, and Procedures for Tactical Employment of Biometrics in Support of Operations* **Approved for Public Release**	6 MAY 16	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: Revision**
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: Current**
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: Current**
EO *Multi-Service Tactics, Techniques, and Procedures for Unexploded Explosive Ordnance Operations* **Distribution Restricted**	15 JUL 15	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: Current**
NONLETHAL WEAPONS (NLW) *Multi-Service Service Tactics, Techniques, and Procedures for the Tactical Employment of Nonlethal Weapons* **Distribution Restricted**	13 FEB 15	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: Revision**
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**
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**	20 JUN 18	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: Revision**
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**	30 JUN 14	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: Revision**

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

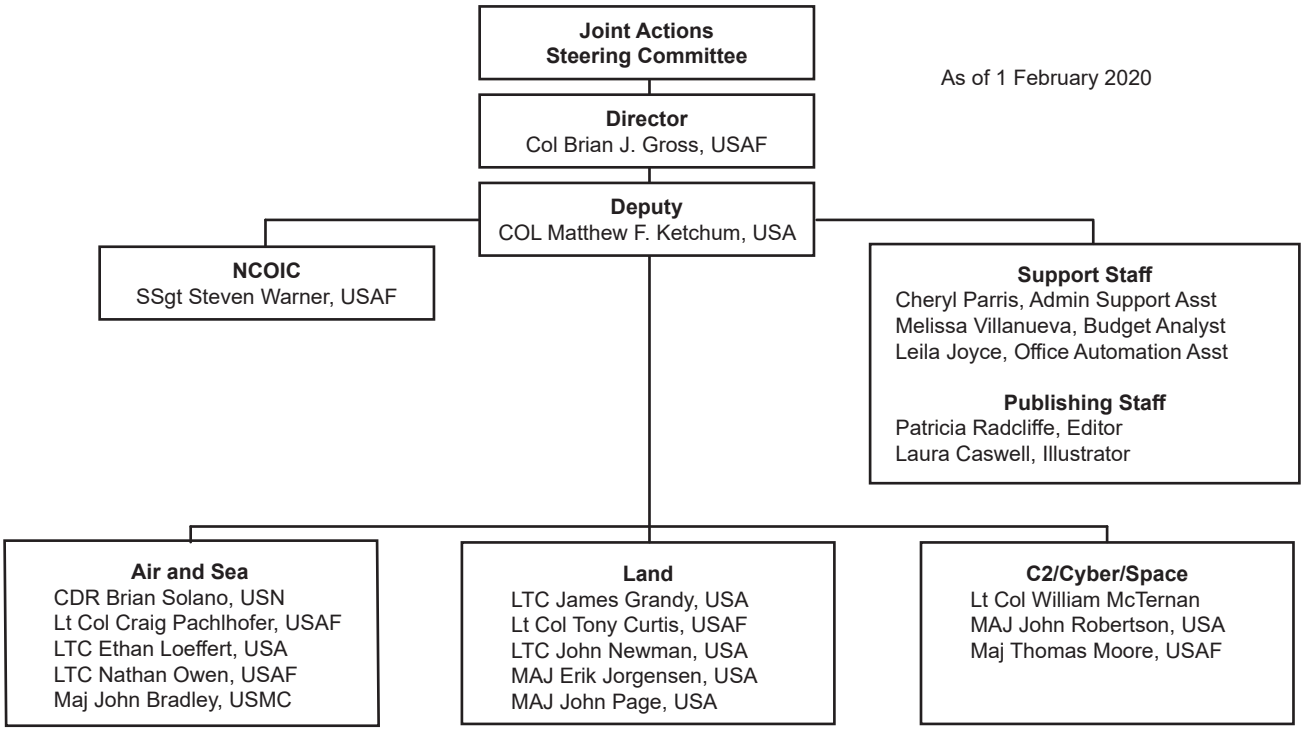
Submissions must:

- 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
Summer 2020	1 March 2020	alsaA@us.af.mil (757) 225-0967
Winter 2021	1 October 2020	alsaB@us.af.mil (757) 225-0964
Summer 2021	1 March 2021	alsaC@us.af.mil (757) 225-0903

ALSA ORGANIZATION



ALSA JOINT WORKING GROUPS

Date	Publication	Location	Point of Contact
1-5 June 20	CF-SOF	Joint Base Langley-Eustis, VA	Land Branch alsaB@us.af.mil
1-5 June 20	SCAR	Nellis AFB, NV	Air/Sea Branch alsaA@us.af.mil
1-5 June 20	Kill Box	Nellis AFB, NV	Air/Sea Branch alsaA@us.af.mil
13-17 June 20	CF-SOF	Joint Base Langley-Eustis, VA	Land Branch alsaB@us.af.mil
18-21 August 20	Personnel Recovery	Joint Base Langley-Eustis, VA	Air/Sea Branch alsaA@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
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 nulti-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

MG Douglas C. Crissman

Director, Mission Command Center of Excellence

MajGen William F. Mullen

Commanding General, Training and Education Command

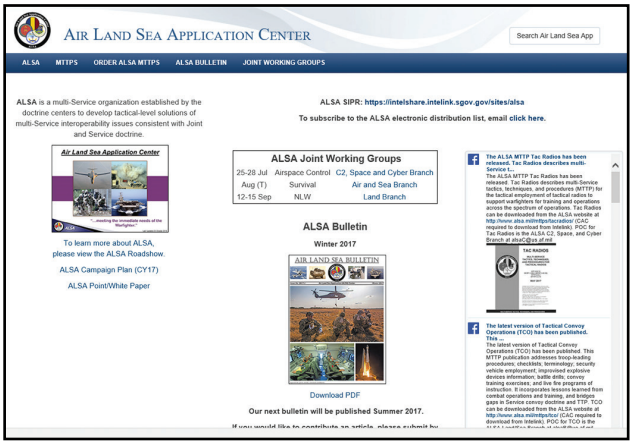
RADM John F. Meier

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



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