BATTLESPACE JOURNAL

Summer 2022 **Volume 2022-2**




Air Land Sea Application Center

ALSA

Air Land Sea Application Center

BATTLESPACE JOURNAL

AIR LAND SEA BULLETIN

ALSA Staff

Director
Col Ian Bennett, USA

Deputy Director
CAPT Brian Solano, USN

Bulletin Editor
Maj Matthew Jackson, USAF

Editor
CAPT Brian Solano, USN

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

Publications Officer
Maj Eric Pederson, USAF

DIRECTOR'S COMMENTS

Welcome to the summer 2022 issue of the Battlespace Journal (BSJ). ALSA's fundamental reason for being is to promote interoperability and make the joint warfighter better. One of the ways to do this is by gathering the thoughts and ideas of subject matter experts, through articles, to highlight what matters to them with regards to tactical issues they face and present that in the journal.

The common theme across the articles in this issue of the BSJ is the necessity for the force to adapt to the changing dynamics of warfare and the corresponding technologies employed therein. Transformation and transition across all domains affect the demands requisite of the Department of Defense (DoD) in a near-peer fight today and in the future. Sharing lessons learned from past tactics, techniques, and procedures (TTPs) is vital for collective situational awareness and we do this through ALSA's engagements and written products.

We hope that you find the articles interesting and informative. We also hope that they make you think about the possibilities and continue the conversation on solving interoperability challenges across the joint force as well as with our Nation's allies and partners.

ALSA continues to evolve and to that end, we would like to welcome the United States Space Force as a full member of the Joint Actions Steering Committee, our governing board comprised of the doctrine centers of all five of our DoD Services.

ALSA itself will undergo a significant personnel transition this summer as we return teammates to the force and welcome aboard new members. This is a necessary but bittersweet process vital to ALSA's growth and development. We ask that you keep engaging ALSA and support us in our joint working groups for MTTPs, contributions to the BSJ, and host us in our engagements with your units and organizations at your duty locations. Likewise, if you happen to find yourself on the Langley side of JBLE, please let us know and we will be more than happy to give you the grand tour of what has been our home since 1975.

Habilis, Credibilis, Celeritas!

Sincerely,

IAN S. BENNETT Colonel, USA

Director

BRIAN J. SOLANO, Captain, USN

Deputy Director

- New ALSA Team Members: SSgt Jonathan Payne (IT support), Maj Matthew "ALF" Jackson (Air/Sea Branch), LTC Margret Stick (Land Branch), LTC Doug Willig (Land Branch), Lt Col Jordan "Itchy" Hrupek (Air/Sea Branch), MAJ Jeff Hackman (Land Branch), MAJ Matt Jensen (Land Branch), Col Joshua Biedermann (ALSA Director), COL Mike Reyburn (ALSA Deputy Director), and Bob Finn (Editor).
- Farewells: ALSA Team Members: LTC John Newman (retirement), Lt Col Nathan "Booster" Owen (PCS), Maj Evan "WAYST" Fillman (PCS), MAJ Jon Page (PCS), LTC Erik Jorgensen (PCS), Lt Col Tony "Cooter" Curtis (retirement), Col Aaron Clark (retirement), and COL Ian Bennett (retirement).

DOD CYBERSPACE: ESTABLISHING A SHARED UNDERSTANDING AND HOW TO PROTECT IT

US Cyber Command members work in the Integrated Cyber Center at the Joint Operations Center in Fort George G. Meade, Maryland, April 2, 2021. (Photo by: Josef E. Cole, USA)

By Maj Eric Pederson, USAF; MAJ Don Palermo, USA; MAJ Stephen Fancey, USA; LCDR (Ret) Tim Blevins, USN

> *We have no room for complacency and history makes it clear that America has no preordained right to victory on the battlefield.—Secretary James N. Mattis*[1]

As the joint force shifts its focus towards trans-regional, all-domain, multi-functional (TAM) strategic competition, nowhere are these concepts more relevant than in cyberspace. The cyberspace domain itself cuts across all physical domains (land, maritime, air, and space) and historic adversary cyberspace activity has generally been below the level of armed conflict. From a defensive cyberspace perspective, the threat to the Department of Defense (DOD) has never been greater. Cyberspace defensive joint force doctrine is still being developed, defensive cyberspace DOD authorities are not well known, and the U.S. and its allies do not have cyberspace supremacy (i.e. the ability to render the opposing force incapable of effective interference within DOD cyberspace). The full consequences of potential adversary cyberspace operations (CO) in the DOD are still being fully understood. Yet, there is a lack of shared understanding about cyberspace across the DOD and the joint force and even less understanding of how the DOD should protect its cyberspace. Despite a desire to understand cyberspace and to protect ourselves, a dearth of clear, concise guidance for the joint force has led to a lack of emphasis on cyberspace and cyberspace security in planning and operations. This article establishes a clear, shared understanding of DOD cyberspace, provides guidance to the DOD to protect its cyberspace, and illustrates current and

future efforts to improve DOD's cybersecurity.

CHANGING NATURE, CHARACTER OF WAR

The 2018 National Defense Strategy (NDS) and 2018 Joint Concept for Integrated Campaigning present the idea of global integration: arranging military actions in time, space, and purpose to address security challenges. Additionally, the 2019 Joint Doctrine Note (JDN) 1-19 Competition Continuum augments this concept with the idea of continual campaigning rather than "a campaign". Continual campaigning is when the joint force is continually competing and adapting in response to strategic conditions and policy objectives through different levels of cooperation, competition below armed conflict, and armed conflict. This is different from a traditional campaign designed around the idea that the world is either at peace or at war. Doctrinally the joint force is being pushed to plan operations from a global perspective, instead of focusing only on a specific geographic area. These concepts describe the approach required for the cyberspace domain. Actions in cyberspace, particularly defensive actions within DOD cyberspace, should not be viewed as a traditional force-on-force competition. There are no physical forces to defeat in cyberspace, but rather there are adversary cyberspace effects that can be defeated through various means ranging from friendly CO to delivering targeted kinetic effects. Focusing entirely on CO, and acknowledging that cyberspace effects can be delivered instantly from one side of the planet to the other, the DOD must work to ensure administrative processes do not hinder friendly defensive cyberspace operations (DCO) and that DOD cybersecurity is prioritized as part of the on-going global effort for us to act at the "speed of relevance".

TOO LITTLE, TOO LATE?

> *The Russians and Chinese are playing a long game to threaten the international, rules-based order…and they are doing this with actions below the threshold of armed conflict. They use information operations, troop movements, proxy fighters, propaganda, diplomacy, economic pressures, and threats to coerce countries.*
> *—Jim Garamone*[2]

Arguably, the DOD's established processes and bureaucracy are not suited to the fast-paced world of cyberspace. The first US Air force chief software officer, Nicolas Chaillan, who spent three years on a Pentagon-wide effort to boost cyber security, resigned late in 2021, arguing, "we do not have a competing fighting chance against China in 15 to 20 years".[3] The Chinese are heading for global dominance because of their advances in artificial intelligence, machine learning, and cyber capabilities, and that these emerging technologies were far more critical to America's future than hardware such as big-budget fifth-generation fighter jets such as the F-35.

> Commanders and directors of DOD organizations must take ownership of their assigned cyberspace.

Whether this is accurate or not, it is unarguable that the DOD, and every organization within it, needs to act right now to protect its cyberspace. Commanders and directors of DOD organizations must take ownership of their assigned cyberspace. If their DOD cyberspace is not adequately protected, the adversary will exploit it and may even achieve physical effects such as shutting down critical infrastructure or weapon systems, while ensuring any digital footprint is not attributable. Accurate reporting of the cybersecurity status of DOD cyberspace is critical. Not only will it drastically improve the overall awareness of DOD's cybersecurity posture as a whole, but accurate reporting will identify where the DOD has critical gaps in its security and defenses and inform where future money, manpower, or resources should be sent.

CYBERSPACE MISSIONS AND ACTIONS

There are three types of cyberspace missions: offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and Department of Defense information network (DODIN) operations (DODIN Ops); and, four types of cyberspace actions: attack, exploitation, security, and defense (Figure 1).

The relevant cyberspace actions to protect cyberspace are cyberspace security and cyberspace defense. The difference between cyberspace security and defense actions is that security actions are taken to *prevent* malicious cyber activity in order to ensure system availability, integrity, authentication, confidentiality, and nonrepudiation, whereas defense actions

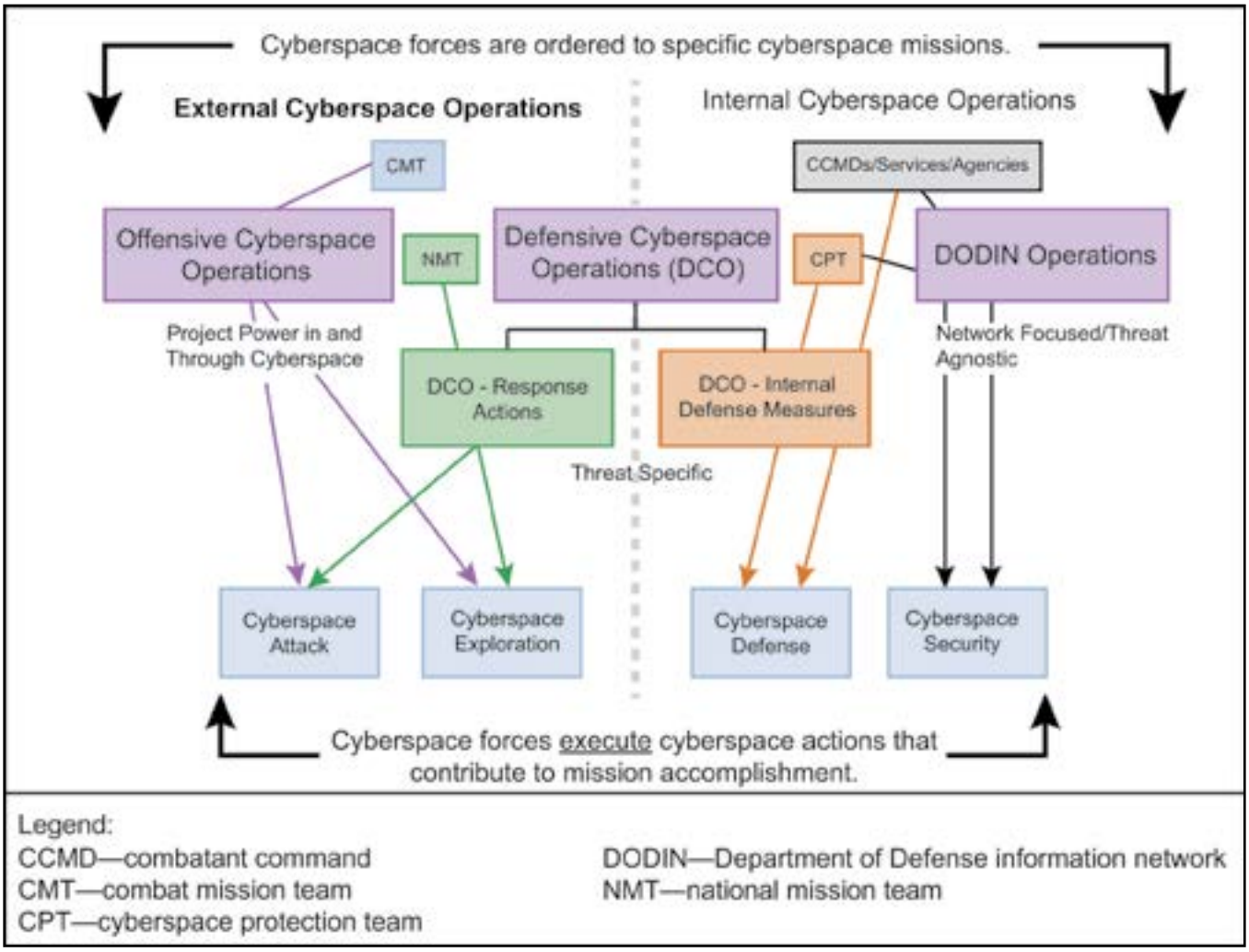


Figure 1. Cyberspace Operations Missions Actions and Forces.[4]

are taken to *defeat* the adversary in order to restore the system to a secure configuration.

Within a given cyberspace mission, different types of cyberspace actions can occur. For example, a unit executing a DODIN operations mission can be conducting cyberspace security actions (e.g. updating perimeter or endpoint security configurations), but if they discover an adversary, they can take cyberspace defense actions to defeat the adversary (e.g. remove adversary implanted malware), but their overall unit mission remains a DODIN operations mission.

DOD CYBERSPACE AND AUTHORITIES

The DOD cyberspace backbone is called the DODIN.[5] The DODIN is the biggest network in the world. It is composed of 44 different DOD components made up of service, agency, and combatant command constructed networks. The DODIN is DOD's classified and unclassified enterprise. Within each DOD component constructed network are thousands of subordinate networks, information technology equipment, tools and applications, weapon system technologies and data spanning across bases, posts, camps, and station levels.

The Defense Information Systems Network (DISN), managed by Defense Information Systems Agency (DISA), serves as the DODIN backbone. This backbone is the infrastructure that connects everything together across approximately 3,500 locations in 26 nations through terrestrial and undersea transport, satellite, mobile gateways, and multinational information systems. Each of the 44 DOD components owns a portion of the DODIN area of operation (DAO) and is responsible for protecting it. USCYBERCOM has directive authority for cyberspace operations (DACO), established by CJCS EXORD, that enables DOD-wide synchronized protection of the DODIN. DACO has been delegated to JFHQ-DODIN and provides authority to direct cyberspace operations related to global DODIN operations and DCO-IDM within each DOD component's DAO. (Figure 2).

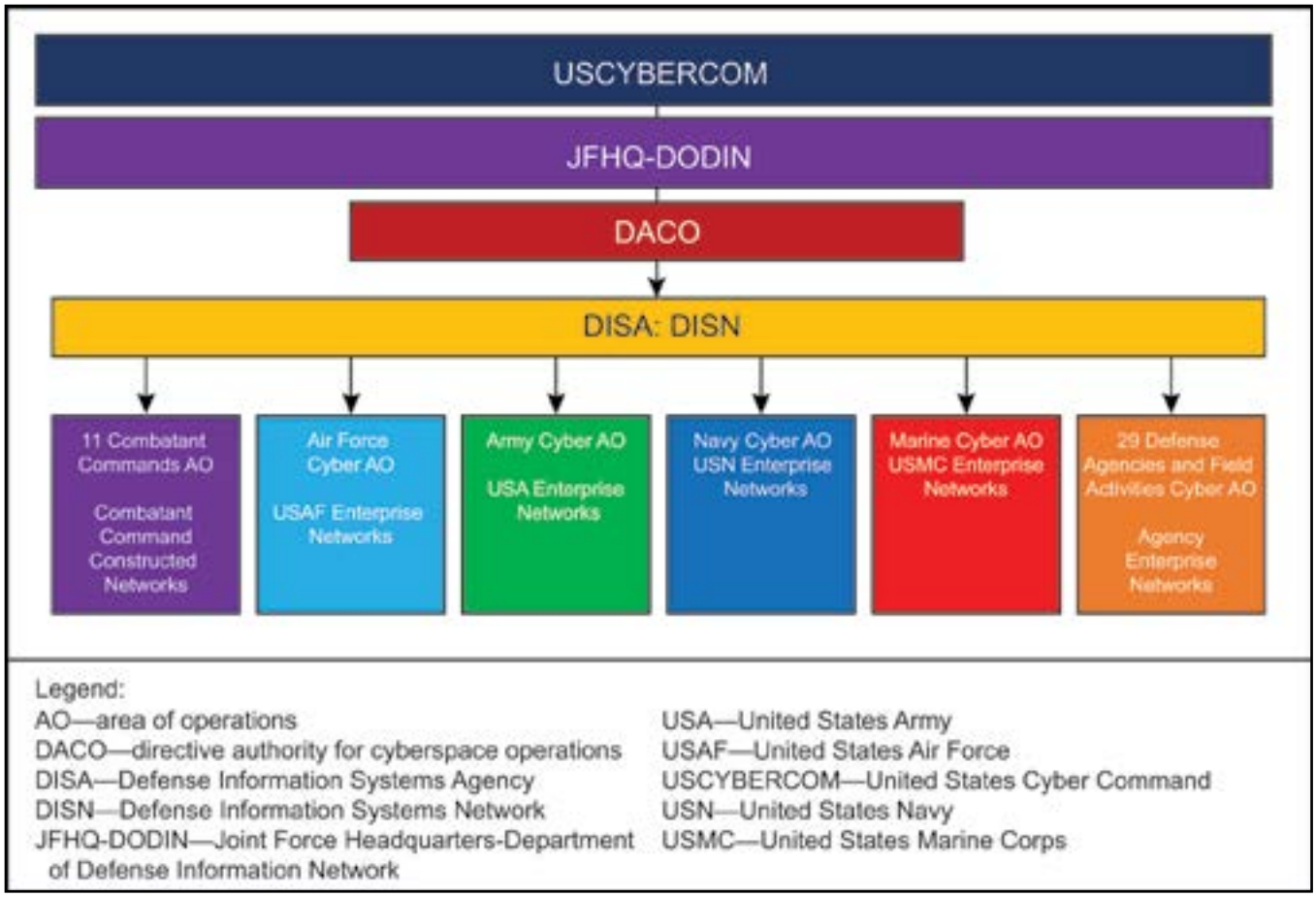


Figure 2. DACO Authority.[6]

JOINT CYBERSPACE ORGANIZATIONS, STRUCTURES, ROLES, AND RESPONSIBILITIES

There is a hierarchy based on roles and responsibilities (Figure 3) when it comes to protecting cyberspace as part of the joint force. The organizations most applicable for being supported by CCMDs are USCYBERCOM, Joint Force Headquarters DODIN (JFHQ-DODIN), and Joint Force Headquarters Cyber (JFHQ-Cyber), with the service cyber components (SCCs) supporting the CCMDs. Organizations within CCMDs that can provide cybersecurity expertise and support are cyber operations-integrated planning elements (COIPEs), joint cyber centers (JCCs), cybersecurity service provider (CSSPs), and network operation centers (NOCs). We will give a quick summary of these organizations as this will help you understand when we address the complications and solutions for CCMDs.

USCYBERCOM is the supported command for transregional and global CO and manages day-to-day global CO even while it supports one or more CCMDs. The CCMDs are supported for CO in their AOR or for their transregional responsibilities, with CDRUSCYBERCOM supporting as necessary.

JFHQ-DODIN which is a component command of USCYBERCOM is the organization that is responsible for securing, operating, and defending the DOD complex infrastructure of roughly 15,000 networks with 3 million users. JFHQ-DODIN leads unified actions across all DOD for DODIN operations and defeats, denies, and disrupts cyberattacks against the DODIN.

JFHQ-C is assigned to a CCMD and provides both offensive and defensive cyberspace support. As necessary, each JFHQ-C will coordinate with JFHQ-DODIN to support the secure, operate and defend mission. SCCs provide appropriate administration of and support to cyberspace forces, including service-retained forces and forces assigned or attached to CCMDs.

Each CCMD has DAO-level CSSPs and NOCs. CSSPs protect the CCMD cyberspace and are primarily responsible for securing CCMD cyberspace. NOCs configure, operate, extend, maintain, and sustain the CCMD cyberspace and are primarily responsible for operating CCMD cyberspace. Under current

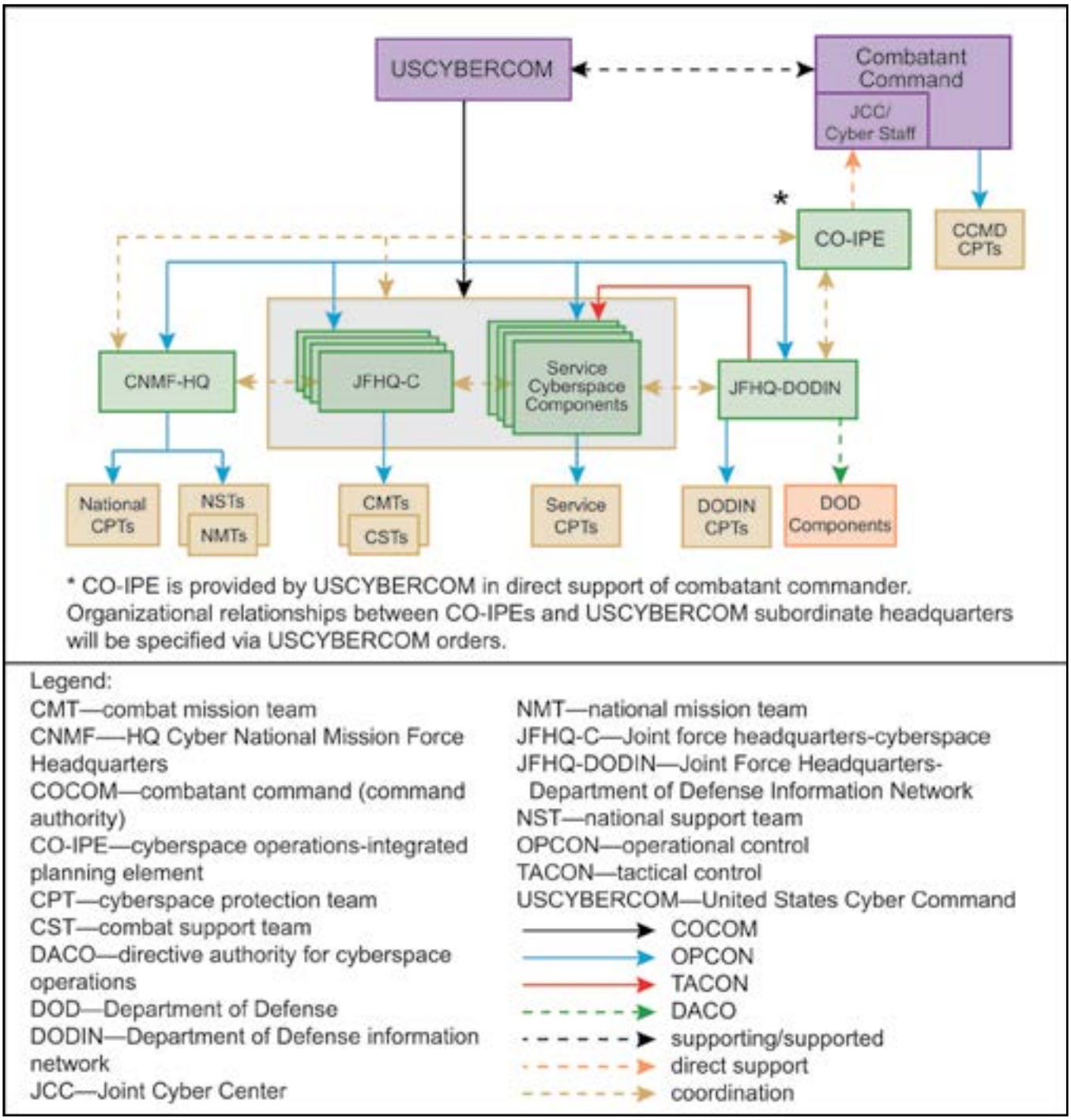


Figure 3. Routine Cyberspace Command and Control.

doctrine, securing cyberspace falls within the DODIN operations mission. Additionally, the joint force function of protecting cyberspace consists largely of cyberspace security actions, and when required, cyberspace defense actions.

WHY LIFE IS COMPLICATED FOR COMBATANT COMMANDS

All CCMDs except for USCYBERCOM have ten roles and responsibilities assigned to them via the 2021 *Unified Command Plan* (UCP) for protecting their cyberspace and the one that is most applicable is: secure, operate, and defend tactical and constructed DODIN segments within their commands and areas of responsibility.

Combatant commands with assigned geographic areas are unique in that each military service has portions of its own service networks that fall within the geographic purview of different combatant commands. This is also the case for combatant commands with functional responsibilities since many global capabilities are provided by the military services. CCMD-constructed networks are limited

to the local CCMD services such as network share points or shared drives and are likely very small when compared to the service enterprise networks within the CCMD AOR. The CCMD-constructed networks are the only portion of the DODIN that the CCMD is directly responsible for. Yet, the services have their own network operating independently within the CCMD AOR and, therefore, the CCMD is unaware of all activities that could have an impact on their current and future operations.

The CCMD-constructed networks are the only portion of the DODIN that the CCMD is directly responsible for.

THE WAY FORWARD

There are three straightforward, but fundamental, steps that CCMDs and DOD organizations need to take to protect their cyberspace:

1. **Take Ownership:** Determine what portion of DODIN cyberspace the CCMD is responsible for. A CCMD should go to its COIPE, JCC, CSSP, and NOC to obtain its operationally assigned cyberspace from JFHQ-DODIN. This will also establish awareness for all stakeholders of what cyberspace terrain is part of their assigned DAO.

2. **Report Cybersecurity Status:** Report the consolidated cybersecurity status to the CCMD commander and to JFHQ-DODIN. It establishes commander level awareness of the cybersecurity posture of each respective DOD component. This vastly improves component awareness of potential operational impacts from a cyberspace perspective. By also sharing this information with JFHQ-DODIN, this establishes awareness of the DOD's cybersecurity posture, DOD-wide. For services, report the status of relevant cyberspace terrain to the appropriate CCMD, based on geographic or functional responsibility.

3. **Identify all MRT-C and KT-C:** Identify what cyberspace terrain is relevant from a mission commander standpoint. Often, there are pieces of cyberspace terrain that are critical for mission or network function that are not obvious (e.g. a lone server in a random unprotected closet that all operational data passes through). The process of identifying this terrain requires both *technical understanding* and *knowledge of the commander's missions*. This then translates into a critical task for CSSPs. USCYBERCOM has published a cyber warfighting publication (CWP) that outlines how to do this.[8] In a nutshell, it simply involves following a mission's data path across networks. Additionally, once all MRT-C and KT-C are identified, the information should be stored and shared using an existing secure database. This step is critical to inform cyberspace defensive planning and operations. As this process matures, cyberspace planners will know what MRT-C and KT-C must be protected throughout all phases of the various scenarios in joint force plans and operations.

CURRENT AND FUTURE CYBERSECURITY EFFORTS

There are other efforts to modernize cybersecurity within the DOD (and the federal government as a whole) that are relevant to CCMDs and all DOD organizations. These include:

- Standardizing network sensors (e.g. perimeter and endpoints sensors) and their deployment within each DAO and across the DODIN

- Standardizing data aggregation at local (local network log/data collection), regional (base/camp/post/station collection), and enterprise (big data) levels, as well as what data is fed to higher echelons

- Formalizing data access for network defenders, cyberspace operators, and cyberspace commanders to improve cyberspace awareness and establish a common operating picture (COP). This will result in increased cyberspace command and control and decrease DOD security incident response times.[9]

- Adopting cybersecurity best practices such as implementing zero trust architecture,[10] accelerating movement to secure cloud services, enhancing software supply chain security, and streamlining cybersecurity to drive data analytics for identifying and managing cybersecurity risks.[11]

- Adopting standardized cybersecurity reporting practices such as the DOD cybersecurity analysis and review (DODCAR) methodology and cyber threat framework that provide effective, and read-

ily digestible, cybersecurity risk information.[12] This nests with industry governance, risk, and compliance (GRC) best practices that improve current DOD compliance operations and ensure operationally focused assessments augment compliance, rather than replace them, ensuring additional risk is not created.

- Updating contract language with DOD partners in a timely manner to address current cybersecurity issues such as enabling cybersecurity-related information sharing across the DOD and limiting/governing cleared defense contractors (CDC) remote access into the DODIN.

PROTECTING DOD CYBERSPACE, NOW AND BEYOND

The stage is set to successfully consolidate multiple cybersecurity efforts. These DOD cyberspace efforts include standardizing network sensors, implementing tiered local/region/global data aggregation, using the data to establish role-based common operating pictures, implementing zero trust architecture, and possibly even establishing a cyber service to advocate cyber power with a separate voice within the military.

> ... DOD cybersecurity efforts have moved away from localized efforts and expertise, and transitioned to established cybersecurity standards across the DOD.

The end state of all these initiatives is that DOD cybersecurity efforts have moved away from localized efforts and expertise, and transitioned to established cybersecurity standards across the DOD. Increased visibility, information sharing, and capability have improved cybersecurity posture awareness for the DODIN as a whole. All DOD organizations share cyberspace information and intelligence securely, and cyberspace is fully incorporated into joint force planning and operations.

CASE FOR A CYBER SERVICE

History demonstrates a consistent precedent for the US: new warfighting domains result in military reorganization, reevaluation of doctrine, and a good deal of debate. A new service emerges to ensure that warfighting in the domain receives the necessary focus for education, training, recruiting, doctrine development, force generation, and as a leading voice in the ongoing discussion of that domain at the strategic, operational, and tactical levels. Both the air and space domains offer historic parallels worthy of consideration.

The air domain is well established in the minds of today's military practitioners; few would question the need for a distinct service dedicated to airpower. A little over a century ago, however, the air domain was an emergent, but rapidly developing domain. Establishing a separate service in the air domain was not instantaneous or without controversy: creation of the US Air Force was gradational, spanned two world wars, and was marked by resistance from within the Army and Navy. Now the Air Force has its own identity, service culture, technology, tactics, and strategy. It offers a separate voice within the military for the use of airpower on the strategic stage. Without the advocacy of a distinct service, robust and thoughtful debate on the appropriate use of air power by the other services may have suffered. Although the existence of a separate Air Force is no longer controversial, its creation was often characterized by resistance from within the military amidst advocacy from civilian political pressures.

Unlike the air domain, the space domain is expanding as a realm of competition nearly simultaneously with another domain: cyberspace. Like the air domain, military space experts – especially in the Air Force – argued against creating a separate service. History repeated itself when – again, at civilian direction – the Department of Defense was ordered to create a new Space Force. In just a few years, Air Force Space Command's General John Raymond went from being an opponent of the Space Force to its first Chief of Space Operations![13]

Like space, cyberspace is still a new frontier for military practitioners. Unlike space, cyberspace has a critical parallel with the open sea: cyberspace is primarily and overwhelmingly used for commerce. Cyberspace is a "wild west" with a low barrier to entry where both nations and criminals can exploit it for their own ends. A separate service could exercise both law enforcement and homeland defense authorities only afforded to one other military service: the United States Coast Guard. Like the Space Force's "No

Day Without Space", a Cyber Force with authorities that parallel the Coast Guard's Title 14 USC would support national strategy and protect our homeland from the disastrous consequences of "A Day Without Cyberspace". A dual identity (military and law enforcement) and alignment under the Department of Homeland Security allow a separate cyber service to protect our nation's global infrastructure from state actors who will be indistinguishable from criminal threats.

CONCLUSION

The DOD cyberspace is only going to continue expanding at an exponential rate utilizing the latest and greatest technology to meet the ever-growing demands for more information from commanders while conducting warfare. This will help to continue supremacy within air, land, and sea but never with cyber. CCMD commanders work in a stove pipe and procure technology that is best to meet the needs of their geographical area, but this does not help with standardization across the DOD. Since the US has experienced successful and harmful cyber-attacks on the critical infrastructures, protecting the DOD cyberspace from adversaries is more important than ever. But do we have an adequate level of protection and shared understanding of our cyberspace and does our current structure work for the foreseeable future. We have only created a band-aid solution and pieced together the infrastructure with the cheapest possible solutions. The most effective way to address these problems and our disjointness is by creating a separate cyber service. Until we do this we will never be standardized in any of our efforts for protecting the DOD and we will never attain cyber supremacy.

END NOTES

[1] "Secretary Mattis Remarks on U.S. National Defense Strategy," January 19, 2018, C-SPAN, video, 49:06, https://www.c-span.org/video/?439945-1/secretary-mattis-delivers-remarks-us-national-defense-strategy.

[2] Garamone, Jim, "Global Integration Seeks to Buy Leaders Decision Time, Increase 'Speed of Relevance'," DOD News, July 2, 2018, https://www.defense.gov/News/News-Stories/Article/Article/1565240/global-integration-seeks-to-buy-leaders-decision-time-increase-speed-of-relevan/.

[3] Manson, Katrina, "US has already lost AI fight to China, says ex-Pentagon software chief," Financial Times, October 10, 2021, https://www.ft.com/content/f939db9a-40af-4bd1-b67d-10492535f8e0.

[4] Figure 1: Cyberspace Operations Missions, Actions, and Forces. Source: Joint Chiefs of Staff, Cyberspace Operations, JP 3-12 (Washington, DC: Joint Chiefs of Staff, 2018), II-13, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

[5] Defense Information System Agency Joint Force Headquarters Department of Defense Information Network, Capabilities: Connecting and Protecting the Warfighting in Cyberspace, 2019, https://www.disa.mil/-/media/Files/DISA/Fact-Sheets/DISA-Capabilities.ashx#:~:text=DISA%20Voice%20Services%20provide%20reliable,voice%20and%20voice%20messaging%20services.&text=Virtual%20Private%20Network%20(VPN)%20provides,through%20various%20means%20and%20modes.

[6] Created by MAJ Don Palermo (USA).

[7] Figure 3: DOD Cyberspace C2. Source: Joint Chiefs of Staff, Cyberspace Operations, JP 3-12 (Washington, DC: Joint Chiefs of Staff, 2018), IV-13, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

[8] U.S. Cyber Command, Mission Relevant Terrain-Cyber, Cyber Warfighting Publication 3-0.1, 20 August 2021

[9] Russel, W. William, Defense Acquisitions: Joint Cyber Warfighting Architecture Would Benefit from Defined Goals and Governance, GAO-21-68, (Washington, DC: Government Accountability Office, 2020)

[10] Pomerleau, Mark, "The Pentagon is moving away from the Joint Regional Security Stacks", C4ISRNET, November 1 2021, https://www.c4isrnet.com/it-networks/2021/11/01/the-pentagon-is-moving-away-from-the-joint-regional-security-stacks/.

[11] Joseph R. Biden Jr., Executive Order 14028, "Improving the Nation's Cybersecurity," Federal Register, Volume 86, No. 93, May 17 2021

[12] Office of Management and Budget, Federal Cybersecurity Risk Determination Report and Action Plan (Risk Report), (Washington, DC: Office of Management and Budget, 2018), https://www.hsdl.org/?view&did=811093.

[13] Raymond, John W., "We Need to Focus on Space, We Don't Need a Space Corp," Defense One, July 20, 2017, https://www.defenseone.com/ideas/2017/07/we-need-focus-space-we-dont-need-space-corps/139360/.; Raymond, John W., "How We're Building a 21st Century Space Force," The Atlantic, December 20, 2020, https://www.theatlantic.com/ideas/archive/2020/12/building-21st-century-space-force/617434/.

MANEUVER COMBAT AND THE INTEGRATION OF AIR FORCE SPECIAL WARFARE: LEVERAGING TACP EXPERTISE AGAINST A NEAR-PEER THREAT

An USAF special warfare mission support Airmen conducts small unit tactics at Joint Base Elmendorf-Richardson, Alaska, June 17, 2020. (Photo by: SrA Jonathan Valdes Montijo, USAF)

By Capt Cameron Urquhart, USAF

> *Tomorrow's Airmen are more likely to fight in highly contested environments and must be prepared to fight through combat attrition rates and risks to the nation that are more akin to the World War II era than the uncontested environment to which we have since become accustomed. The forces and operational concepts we need must be different. Our approach to deterrence must adapt to the changes in the security environment.*
>
> *Charles Brown, Jr., Gen, USAF*
> *Chief of Staff of the Air Force*[1]

THE FUTURE FIGHT

General Brown echoes what the Air Force enterprise has realized for the last several years. We are not postured for the next fight against a near-peer threat such as China or Russia. The tactical air control party (TACP) under the newly minted Air Force special warfare (AFSPECWAR), must transition from a community that focuses primarily on close air support (CAS), multi-domain command and control (C2) functions during Phase III operations, to a career field that can be doctrinally relied on from the onset of Phase I operations who answers the needs of the combined force air component commander (CFACC), keeping in line with the chief of staff's new directives.

TACPs can longer rest on their laurels of liaison and terminal control alone, they must acknowledge the struggles that our nation faces in the next conflict. The Air Force developed a map for the

TACP weapon system in the latest *AIR FORCE SPECIAL WARFARE (AFSPECWAR) TACTICAL AIR CONTROL PARTY (TACP) WEAPON SYSTEM VISION 2030*. In this four-page document, the USAF Deputy Chief of Staff states that: "The TACP weapon system (WS) is not currently postured to provide 'joint lethality in contested environments'… from the tactical to strategic planning level as laid out in the National Defense Strategy …the improved TACP WS will provide effective air-minded integration to joint elements to enable stand-in sensors, link stand-off shooters, and provide all domain effects for joint commanders."[2] This battle-hardened community of joint terminal attack controllers (JTACs) must evolve to be joint partners in all domains; kinetic and non-kinetic subject matter experts across the all-domain spectrum.

EVOLUTION OF TACTICS FROM COUNTERINSURGENCY (COIN) OPERATIONS TO NEAR-PEER THREATS

For the last two decades, the United States military has fought a COIN war in the Middle East which has equated to, among other things, the use of precision strike against insurgents in mostly uncontested environments. As General Brown illustrated in his strategic approach, *Accelerate Change or Lose*, the Air Force needs to learn how to fight in an environment akin to the Second World War. For special warfare TACPs that means internalizing the Army's ground scheme of maneuver and refining how they can integrate fires that do not have the requirement for JTAC employment. Annex 3-03, Counterland Operations, states that since World War I, "Airpower added a synergistic element to conventional ground forces because of its ability to attack behind enemy lines and support offensive breakthroughs …Airpower has proven invaluable in supporting friendly ground maneuvers by diverting, disrupting, delaying, or destroying an enemy's operational military potential."[3]

The joint force fundamentally understands that airpower plays a pivotal role from the start of a major engagement. The Air Force as a whole, however, lacks the ability to successfully integrate into the ground scheme of maneuver as well as an understanding for battlespace geometry. The terms forward line of own troops (FLOT), fire support coordination line (FSCL), coordinated fire line, and phase lines are joint doctrinal terms that must be added to the Air Force's lexicon. TACPs are uniquely suited to be the lynchpin due to their ability to integrate from the company level through the corps providing both terminal control, liaison capabilities, and C2 across all domains. "The TACP WS should integrate not only with traditional air, land, and sea-based capabilities, but also cyber and space capabilities to provide the full suite of joint all-domain operations to defeat future adversaries in a highly contested and denied environment."[4]

> … the necessity to balance CAS, air interdiction (AI), and strike coordination and reconnaissance (SCAR) is paramount.

In a conflict with a near-peer threat, the necessity to balance CAS, air interdiction (AI), and strike coordination and reconnaissance (SCAR) is paramount. TACPs' bread and butter is CAS, which is defined as air action by aircraft against hostile targets that are in close proximity to friendly forces and require detailed integration of each air mission with the fire and movement of those forces. This form of fire support is best suited between the FLOT and FSCL and differs greatly from AI which is defined as air operations conducted to divert, disrupt, delay, or destroy the enemy's military surface capabilities before it can be brought to bear effectively against friendly forces, or to otherwise achieve objectives that are conducted at such distances from friendly forces that detailed integration of each air mission with the fire and movement of friendly forces is not required. (Annex 3-03, *Counterland Operations: AI Fundamentals*). AI and SCAR do not require a JTAC to deploy munitions, but at the tactical level, the TACP is essential in collecting data across multiple domains and funneling it to the appropriate agencies to ensure that the joint force commander's (JFC) objective is achieved. At the operational level (corps staff) and during Phase I/II, TACPs are crucial in integrating fires long of the FSCL and aiding AI and SCAR to peel back layers of integrated air defense systems (IADS) by being the connective tissue between the air operations center (AOC) and the ground maneuver elements, ultimately allowing an increase in air superiority and a permissive environment.

During the early phases of a major conflict, TACP operators would be vital acting as the connec-

An A-10 Thunderbolt II from the 190th Fighter Squadron executes a show of force during a training exercise with the 124th Air Support Operations Squadron and Brazilian Air Force tactical air control party specialist at the National Training Center, Fort Irwin, California, June 12, 2019. (Photo by: SrA Mercedee Wilds, ANG)

tive tissue, linking the tactical and operational levels. Currently, TACPs are manned from the battalion level, through the corps/joint air component coordination element, with additional personnel at the AOC. No other career field has the same representation of personnel at so many echelons during combat operations. As the Air Force moves into the all-domain fight, TACPs are already strategically poised to fill the gap with the their newly minted TACP integration unit type code layout that include all-domain subject matter experts, but above all else, they have the knowledge base of how to integrate crucial information for both the air and ground war. Ideally, AFSPECWAR operators will be the premier ground tactical C2 entity, projecting an advanced mesh network from within the anti-access area denial (A2AD) threat environment.[5] This will be done through a combination of increasing manning at echelons above the division to aid in coordination and integration, as well as sending operators into the threat zone and controlling kinetic and non-kinetic fires.

RAMIFICATIONS FOR THE JOINT FORCE, AND THE LIMITATIONS THAT MUST BE ADDRESSED

As mentioned in the previous section, special warfare TACPs will be crucial during Phase I and II of a conflict to integrate the Air Force component commander's objective with the land component commander's to achieve the joint force commander's goals within the area of operation (AO). During the first phase of an operation, the Air Force's primary concern is disrupting military centers of gravity, degrading the enemy's IADS, and disrupting enemy forces deep behind enemy lines before those maneuver elements can make their way into the corps AO (once ground forces are in the AO). One of the key limitations to this balancing act in the joint environment is understanding each branch's definition of "the deep fight".

The FSCL is the key term when delineating between each branch's deep fight and JP 3-09, *Close Air Support*, defines the fire support coordination line

best; "The FSCL delineates coordination requirements for the joint attack of surface targets, while also facilitating the expeditious engagement of targets of opportunity beyond the coordinating measure, this applies to all fires of air, land, and maritime-based weapon systems using any type of munition against surface targets"[6]. The air component views the FSCL as a restrictive fire support coordination measure when regarding the area short of the coordination measure. The joint force air component commander (JFACC) cannot employ fires short of the FSCL without coordination with the joint force land component commander (JFLCC). The FSCL is a significant consideration during interdiction operations. The FSCL is primarily used to establish C2 procedures for planning and execution purposes.

Understanding how the FSCL impacts the battlefield is vital to the TACP mission at the corps level because it helps in delineating CAS, AI, and multi-domain operations. As we look forward to a near-peer fight, this dedication to integrating fires across all domain spectrums will be one of the main factors that reduce friction within the joint operations. For starters, this means TACPs need to revamp their approach to joint exercises at locations such as the National Training Center (NTC) and the Joint Readiness Training Center (JRTC); and Warfighter Exercise (WFX) participation. Instead of focusing on the liaison and control as it pertains to CAS, AFSPECWAR operators have to start integrating joint all-domain command and control functionality into the fight. Using all domain control teams (ADCTs) and deep strike reconnaissance teams (DSRTs) within the scenarios and more importantly, teaching the army echelons how that capability will achieve the ground commander's effect.

HOW SPECIAL WARFARE PLAYS IN FUTURE WARFARE THROUGH THE JAGIC AND FIRES INTEGRATION

The joint air-ground integration center (JAGIC) is the result of decade long Army-Air Force integration effort led by Air Combat Command's Joint and Combined Integration Directorate. At its core, the JAGIC takes an air support operations center (ASOC) crew and integrates it with the division's staff making a current operations integration center (COIC). The COIC is comprised of the ASOC, division TACPs, fire support element, C2, air and missile defense (AMD), and aviation personnel. The JAGIC is responsible for integrating air-to-ground effects within the division battlespace, as well as managing the air asset collocation amongst the subordinate brigades. The Joint Force Quarterly article, Bridging the Gap from Coordination to Integration, sums up the role of the JAGIC best as; "… collocates the decision-making authorities from the land and air components with the highest levels of situational awareness, that is, the senior air director and deputy fire support coordinator…This arrangement also ensures support of JFACC objectives and intent and requirements of the JFC."[7]

The JAGIC is a crucial war-fighting function in terms of major combat operations against a near-peer threat and though the liaison and control mission of the TACP will not change, there is the potential to build on the all-domain aspect and keep the WS in line with the 2030 vision. Using the TACP C2 construct, under the JAGIC AO, we can employ TACP DSRTs, comprised of 4-6 personnel, including 2-3 Army Scouts and 2 JTACs. During Phase III operations and while supporting a ground maneuver element, the purpose of this team would be to deploy short of the FSCL within the division's "deep area" and collect targeting information to either action on with air-to-ground munitions or surface-to-surface fires, effectively extending the reach of both air and surface capabilities, as well as extending the all-domain network beyond the FLOT. The DSRT would be an extension of the JAGIC and report their findings directly to the COIC to help degrade and attrite those enemy maneuver elements before reaching the FLOT.

THE AIR FORCE'S ACE IN THE WHOLE

Agile combat employment (ACE) is the Air Force's solution to how it will extend its capability in a near-peer fight. Not only projecting air power beyond the FSCL, but maintaining air superiority to achieve the CFACC's objectives. Under the ACE construct, fighter wings will push their aircraft to forward air refueling points (FARPs) much in the same manner that brigade combat teams (BCTs) employ their organic

Agile combat employment (ACE) is the Air Force's solution to how it will extend its capability in a near-peer fight.

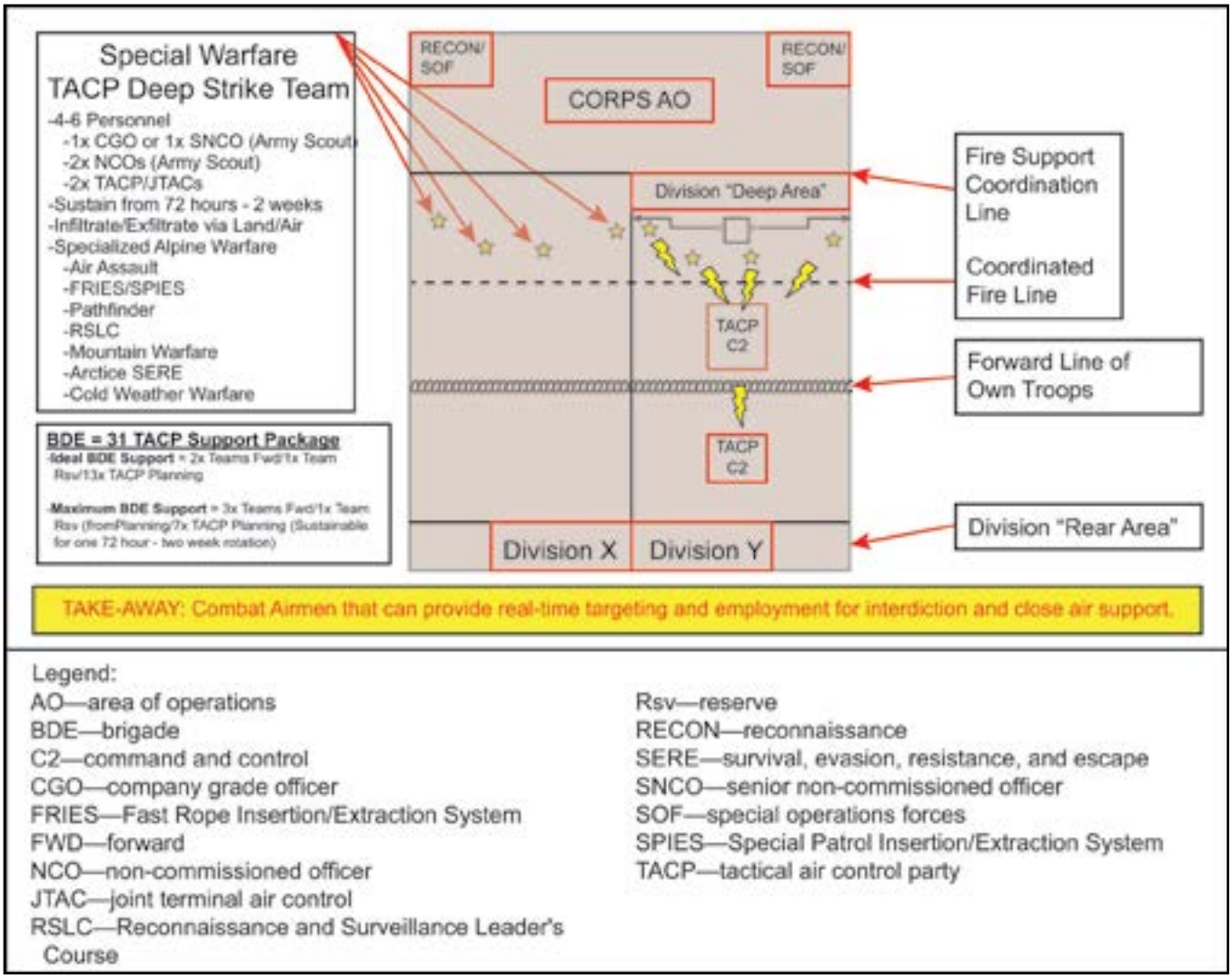


Figure 1. Example of Deep Strike Team within a Division Battle Space.

rotary wing assets. "ACE operations require greater risk acceptance throughout the chain of command. ACE involves higher risk activities like integrated combat turns, specialized fueling operations, or wet wing defueling to maintain momentum. Operations inside an adversary's integrated air defense system, landing sites operating with limited defenses, short notice dispersal operations, etc., may also be necessary."[8]

This configuration allows the fighter wing to keep its assets closer to the fight instead of returning to its established airfield. With the Air Force leaning towards the ACE concept and the Army working on building the multi-domain task force (MDTF) within Indo-Pacific Command (INDOPACOM), TACPs are in a unique position to align themselves with the MDTF's long-range fires supporting the JFACC during the initial stages of a major conflict and then focusing on the JFLCC's objectives once ground forces are in the area of operation. The white paper titled "*Disaggregated TACP C2 Mission Network Capability*" briefly touches on this new opportunity known as the DSRT, which was previously touched on in the last section. Under ACE within Pacific Air Forces, special warfare TACPs are part of the ADCT. Whereas the DSRT is best utilized as an extension of the division for shaping targets before they hit the FLOT (Figure 1), the ADCT is co-located at the main operating base and forward operating stations and is responsible for the C2 structure (datalink, voice communications) as well as limited ASOC functions such as sortie allocations for the fighter wing.[9]

This would be a major change to the TACP's concept of fighting in a major operation. Instead of JTACs only deploying during the Phase III operations to support a ground maneuver echelon, they would be stepping into the fight earlier to facilitate the JFACC's success in Phase I and II operations.[10] As stated earlier in this paper, TACPs are uniquely suited to integrate with all facets of combat operations and

more so within the forward operating cluster, through a standard theater air control system style footprint that would be adapted to support ACE operations. The headquarters element would be centralized with the wing operations center at the main operating base, facilitating reach back to the AOC while ensuring C2 redundancies to the forward station locations. Capitalizing on this structure, TACPs will have small ADCT teams that can rapidly deploy to as many as six forward operating locations to provide a litany of capabilities such as conducting landing zone operations for fixed and rotary-wing aircraft, maintaining C2 from mission type orders received from the main base of operations, precision strike, and integration capabilities.

CONCLUSION

As the TACP community transitions to the newly minted AFSPECWAR moniker and looks to the next near-peer fight, the community must transition from a CAS-only mindset to a multi-domain C2 functionality, keeping in line with the chief of staff's new directives. This evolution will be achieved through the creation of the ADCT and DSRTs that will aid in the Air Force's ACE by creating a datalink network within the A2AD environment and providing kinetic and non-kinetic fires. Moreover, as TACPs continue to accumulate all domain expertise, they have to increase the manning of personnel above the division level to include representation at the AOC to successfully integrate all of the capabilities required in a joint fight to achieve the JFACC and JFLCC's objectives.

END NOTES

[1]Brown, Charles, Jr., "Strategic Approach: Accelerate Change or Lose," pg 3.

[2] Deputy Chief of Staffs. "Air Force Special Warfare (AFSPECWAR) Tactical Air Control Party (TACP) Weapon Systems Vision 2030." Pg 2.

[3] Lemay Center for Doctrine Development and Education, Annex 3-03 DAF Counterland Operations. 21 Oct 2020

[4] Chief of Staffs. 2030 Vision, pg 2.

[5] Hairfield, Capt Austin. "TACP Participation in the Air Force's Advanced Battle Management System (ABMS) On-Ramp DEMO #2". Wheeler AAF, HI. 15 Oct 2020.

[6] Joint Publications 3-09.3

[7] Caraway, Troy. Green, Robert. Neal, Curtis. Bridging the Gap from Coordination to Integration. Pg 98.

[8] Lemay Center for Doctrine Development and Education, Annex-3-99 DAF Role in Joint All-Domain Operations (JADO), Key Considerations for Agile Combat Employment (ACE).

[9] Rings, Maj Nathan. "Disaggregated TACP C2 Mission Network Capability". White Paper, Wheeler AAF, HI, Nov 2020.

[10] Holmes, Maj Gen James. "Air Combat Command Tactical Air Control Party Command and Control Concept of Employment". 10 Jun 2020.

TACP Wraith Challenge competitors from the 9th Air Support Operations Squadron execute a target-talk-on with an AH-64D Apache Longbow, April 22, 2021, at Fort Bliss, Texas. (Photo by: Capt Faith Brodkorb, USAF)

COMMAND, CONTROL, AND COMMUNICATIONS IN THE SOUTHWEST PACIFIC AREA CAMPAIGN (1943-45): A RETROSPECTIVE TO INFORM FUTURE C2 AND COMPETITION IN THE INDO-PACIFIC

A US Navy Sailor checks communications as the phone and distancing line signalman on the forecastle aboard the Ticonderoga-class guided-missile cruiser USS Antietam (CG 54) before a dual underway replenishment on July 22, 2020. (Photo by: MC3 James Hong, USN)

By BG Jan C. Norris, USA and Maj Jared L. Towles, USMC

Communications are seldom mentioned in official dispatches or noted in historians' accounts unless they fail.[1] Comms constitute the weapon placed in the hands of the commander to accomplish the mission, just as the rifle is placed in the hands of an infantryman.[2] The Southwest Pacific Area (SWPA) theater liberation campaign (1943-45) led by GEN Douglas MacArthur demanded innovative communications solutions given the vast distances, jungle terrain, and archipelagic landscape in support of maneuver. Not since that campaign has the United States had such a force presence in the region.

The current DOD and Indo-Pacific strategy calls for a dynamic forward posture and presence in Southeast Asia, South Asia, and Oceania (formerly the SWPA). While the communication challenges and operating environment remain largely unchanged, advanced 21st-century communication technologies will only be as effective as the sophisticated adversarial threat capabilities built to deny them. This retrospective intends to provide context for command and control, and communications for future competition and conflict (if required) in the South Pacific to maintain a free and open Indo-Pacific.

Drawing directly from Center of Military History Publication 10-18 (Signal Corps: The Outcome, mid-1943 through 1945, 1966), the following historical narrative and excerpts capture the SWPA campaign command and control and communications environment.

From Signal Corps ref) Tropical combat in the Southwest Pacific placed Army communications and

the Signal Corps in an environment similar to that of adjacent Pacific Ocean areas. Jungle conditions, excessive heat, and rain sorely strained Signal Corps men and their equipment. Great distances over water required sole dependence upon heavy-duty long-range radio. Actions under Allied and amphibious commands demanded close coordination of signalmen, signal procedures, and signal equipment in co-operation with the Navy, the Marine Corps, and often with British and Dominion forces. These circumstances of military operation were common to the South and Central Pacific as well as to SWPA, but in its organizational structure and manner of operation, SWPA differed. If the Pacific war was principally the Navy's war, Army conforming therewith, SWPA provided an exception. The SWPA staff was primarily Army, not Navy. The naval commander of the Seventh Fleet that supported SWPA, in Morison's words, was seldom admitted to General MacArthur's strategic staff discussions; he was simply told that the General intended to land at such a place on such a date, and the Navy must see that their movement to the objective was properly covered.

Whatever unified command there was in SWPA existed at the top only, in the commander in chief himself, General MacArthur, and in his staff relations. There was in SWPA no joint organization that reached down into the task forces and island commands, as it did in the South and Central Pacific. There were no joint communications centers in SWPA, and no joint units such as Joint Assault Signal Company (or JASCO which later became USMC ANGLICO), until the assaults upon the Philippines. Each participating service maintained its own communication centers and kept its circuits separate for its own sole use. Coordination was accomplished, below MacArthur's GHQ, by co-operation and consent.[3] General HQs SWPA had taken form in MacArthur's hands during the spring of 1942 in Australia. Head of the Signal Section and the Chief Signal Officer, SWPA, was Brig. Gen. Spencer B. Akin. Akin had departed from Corregidor in March 1942 and accompanied MacArthur to Australia.

He remained the chief signal officer for SWPA throughout the war and beyond, through all the subsequent moves and redesignations of MacArthur's command, from Australia to Tokyo and until his appointment in 1947 as the Chief Signal Officer of the Army in Washington, D.C.

General Akin sought in every way to ensure the success of any operation, moving equipment and personnel as

Figure 1. Major General Akin arrives at Hollandia.

the immediate needs of the situation might require. Whenever he took direct action, he did so in conformity with the wishes of the local commander while informing the GHQ chief of staff. In SWPA operations, the GHQ chief signal officer first arranged for and supervised the necessary signal coordination and cooperation of the several participating forces to the end that confusion, waste, and duplication might be minimized. General Akin gave the highest Army commander in combat areas the responsibility (while providing to him the needed equipment and troops) for the installation and maintenance of major communications facilities. The highest Army commander in most SWPA operations (apart from the conquest of the Lae-Salamaua area by the end of 1943 in which a large number of Australian forces bore the brunt of combat) was General Krueger, commander of the Sixth Army (sometimes called the ALAMO Force). Krueger's signal officer throughout the Pacific war was Col. Harry Reichelderfer.[4]

Colonel Reichelderfer later said in summarizing these and other SWPA signal experiences that each element-Navy, Sixth Army, AAF, SOS-had certain missions, and each, he emphasized, used its own communications. The only joint circuits that they employed were limited to naval gunfire support and to air support communications during the landing phase of an operation. The SWPA command system "worked very well," Reichelderfer told an Armed Forces Staff College audience in 1947, "and I liked the way we did it."[5]

Amphibious assaults, requiring the closest possible contact between air, sea, and ground forces, depended heavily upon radio, the only means of communicating under the circumstances, beyond the reach of ear or eye. The radio blueprints for each action were necessarily complex and extensive. The communications plans for the amphibious portion of an operation, Reichelderfer recalled, "always culminated in a conference prior to the issuance of the necessary field or operation orders which was attended by representatives of GHQ, SOS, Sixth Army, the Navy, and the Air Force." Individual conferences for each of the many actions in the New Guinea area took one or two days. Later on, preceding the large-scale Leyte and Luzon landings, the conferees took much more time. Every detail fell under scrutiny. Frequencies were assigned. Communications procedures and plans for coordination were formulated. The decisions at which the conferees arrived went into the signal annexes of the operation instructions and into the field orders of the troop units.[6]

Conditions under which Signal Corps men worked in SWPA were frequently wretched-wretched for the men, whether laying and maintaining wire or working in message centers, and wretched for the equipment also. The steaming heat often rendered life equally difficult indoors and out. "Imagine," Colonel Reichelderfer commented, "what the in¬ side of a six-ton van, housing nine radio operators ... felt like, completely closed up [under blackout conditions] with the temperature and humidity both in the nineties." Even at that, the communicators perhaps had it a bit better facilities of the Sixth Army, General Krueger himself noted that "priority was given to the message center." He thus underscored the vital importance of the communications links in the isolated circumstances of jungle warfare in the Pacific. He listed as next in priority cooking and eating arrangements, and, last, the shacks and tents for his own headquarters personnel.[7]

The region and its peculiarities directly affected communications. The assignment of radio frequencies that had succeeded farther south failed badly in the scene of these actions. Colonel Reichelderfer found that "frequencies which worked perfectly over the comparable distances at 10 degrees south latitude both day and night, would not function at all at night and were erratic in the daytime in the vicinity of 6 degrees south latitude. A great deal more experience and data on radio propagation," he reported to the Washington headquarters, "will be necessary before the solution will be fully satisfactory." Even Safehand Airplane Courier Service suffered from the climate. Intended to operate on a daily schedule, it could not. Often the couriers and their message pouches had to sit out hours and even days of violent weather. "As this is being written," Reichelderfer commented, "no airplane has arrived or taken off from the airstrip serving this headquarters for three days, because of torrential rainstorms."[8]

Despite transmission troubles, radio was succeeding in carrying Army messages. Ten days after the last of the three landings, Colonel Reichelderfer reported, "the Army is operating a total of 24 high-powered radio circuits. Twelve of these circuits are at the rear echelon and seven are at the Command Post." Small radios worked well, within the recognized limitations

Figure 2. Signal supply dump, white beach, Leyte.

imposed by the jungle (the dense vegetation absorbing radio waves, reducing the range of the sets).[9]

"The SCR-300 radio sets," he reported further, "have proved to be a godsend in amphibious operations for ship-shore communications and shore party communications."

Before the end of 1942, as operations against the enemy began in the island and ocean areas northward from Australia, amphibious communications became necessary, and General Akin outfitted a Signal Corps fleet, a flotilla of small vessels equipped with radio. At first, they served in a small way as relay ships from forward areas to headquarters in the rear. Their function soon expanded, however, till they took aboard the forward command post communications facilities. The little aggregation became the Army's CP fleet.[10]

The small communications ships proved so useful in amphibious actions that Army elements in SWPA operations continually competed to obtain their services. Army commanders preferred them to Navy communications ships, or AGC's. For one thing, Navy AGC's were hard to obtain for Army operations. For another, Navy AGC's tended to stay too far offshore, and they tended to depart from the vicinity of land combat as soon as possible. The naval commander of a large AGC was always mindful of enemy suicide boats and planes and he would generally, come darkness, move his ship out several miles from the beach, too far to provide the close communications support that Army elements ashore very much needed.[11] *None could deny that these ships served the Army well. Their temporary use to ensure communications so vital to overall success, during the crucial hours and difficult first days of an amphibious action, entirely justified all the effort that went into them.*

General Akin himself had no doubt of the value and necessity of Army communication ships in SWPA combat. On 21 March 1944, he set up in GHQ SWPA Signal Section a separate Seaborne Communications Branch to plan for extensive communications afloat and to provide a more adequate CP fleet.

Signal supply in the SWPA, as anywhere else, needed good planning and adequate training of the personnel. There was no time for either. Nowhere else did the signal depots serving overseas experience so many moves and vicissitudes as in SWPA over the thousands of miles of sea and jungle terrain that stretch from Australia to Tokyo. Bad as were these unavoidable difficulties, there were exasperating moves of depot locations made within a single area. There were sharp differences between the views and objectives of signal supply officers at a base and the signal officers at the front. The former, reported Colonel Strasburger, signal officer of the XIV Corps at Bougainville (SOPAC) in mid-1943, sought for his base large quantities of supplies, the need for which was not so much immediate as anticipatory. The signal officer of a tactical unit, however, wanted only a minimum of general supplies but a maximum of whatever was needed to meet immediate requirements.[12]

However much of the equipment may have been stored in the rear base depots, not enough of it got into the hands of the troops forward. Such was the complaint of the 162d Infantry Regiment after its operations in the Sala Maua area of New Guinea late in the summer of 1943. "At no time," the regiment complained, "was a sufficient supply of all signal items on hand." The thing the men wanted was an ideal that could never be realized-"a completely equipped signal dump and repair section . . . in operation as near to the action as deemed feasible."[13]

(Author) The Southwest Pacific Theater liberation Campaign and elements of command, control, and communications described here do not reflect the current state of competition for the Theater Army and Joint Force in the Indo-Pacific. We are not at war, do not have the same force presence forward (yet), nor are the resources fully committed to executing a like campaign of 'competition'. The terrain, climate, and operating environment are unchanged. The ability to command and control is as critical as ever and communications remain the foundational weapon systems for enabling C2. In the coming years, forces operating and competing in the South Pacific will certainly encounter similar communications challenges as MG Akin and his subordinate Signal Officers faced supporting maneuver, supplying and enabling Commanders across an archipelagic landscape. Unlike GEN MacArthur's SWPA GHQ task organization in 1943, any future competition/fight will undeniably be an integrated 'joint and coali-

U.S. Marine transmissions system operators with 10th Marine Regiment, 2d Marine Division set up a Dipole antenna as part of the High-Frequency (HF) Competition at Camp Pendleton, California., July 13, 2021. (Photo by: Pfc. Sarah Pysher, USMC)

United States Army National Guard Soldiers and Airmen move swiftly through the Cyber City area of operation as Blue Team defenders during the Cyber Shield 2016 exercise at Camp Atterbury, Indiana, April 20, 2016. (Photo by: SGT Stephanie A. Hargett, USA)

tion' fight across all echelons, across all domains, and with supporting joint and all domain communication systems. Exercising, experimenting and rehearsing in these geographic areas at scale will validate existing and developing communications capabilities.

By reflecting on lessons learned in SWPA, Signal/Cyber forces have an opportunity to better prepare and enable Theater Army and Joint Force goals for competition in the Indo-Pacific. Limitations and challenges from weather, vegetation, and terrain, and the vast distances are still significant challenges to communications in the Pacific Theater and we are amiss to think that our technological advances in digital and radio communications will make these limitations trivial. The planning of communications was scrutinized because of the complexity of the operations. Deliberate planning with all our end-user organizations must carry the same importance.

Commanders and small units must have layered communication plans that range from digital to denied (either by terrain and weather, or enemy actions). These communications should include:

1. Digital Channels
2. Line of Sight (LoS) and LoS relay
3. High-Frequency comms (HF)
4. And mission-type orders when no communication is possible

Finally, the Signal Corps had to figure out HF radios, antennae theory, and radio wave propagation during combat. These skills and art have been largely lost in the US military and should be reinvigorated so we are not learning it again under duress. HF still remains the only form of electronic communication that does not need a relay system.

END NOTES

[1] Center of Military History Publication 10-18 (Signal Corps: The Outcome, 1943-1945, 1966), page 13.

[2] Ibid, page 17.

[3] Ibid, page 238.

[4] Ibid, page 243.

[5] Ibid, page 244.

[6] Ibid, page 244.

[7] Ibid, page 247.

[8] Ibid, page 252.

[9] Ibid, page 252.

[10] Ibid, page 261.

[11] Ibid, page 261.

[12] Ibid, page 269.

[13] Ibid, page 269.

MANEUVER, MODERNIZATION, AND THE SECOND NAGORNO-KARABAKH WAR

Azerbaijani forces stand in formation for the opening ceremony of exercise Rapid Trident, Yavoriv, Ukraine, Sept. 3 2018. (Photo by: Pfc. Andrea Torres, ARNG)

By Andrius Bivainis (Lithuania)

Eastern and Western perceptions of military affairs surface in the region of South Caucasus, a historic crossroad of multiple cultures and worrying parties[1] and erupted into a full-scale war between Armenia and Azerbaijan in the fall of 2020 over a region called Nagorno-Karabakh, the mountainous enclave between two countries for which both nations maintain their cultural, national, and strategic claims. Prolonged military build-ups, defense coalition initiatives and military modernization are the backdrops for what is now called the Second Nagorno-Karabakh War. This article offers an assessment of the military campaign conducted in a six-week war period. The first part of the article elaborates on maneuver, terrain, and command and control. The second part highlights the decisive role of military modernization.

GRADUALLY CHANGING QUALITIES OF WARFARE

The region of Nagorno-Karabakh historically has become a source of rivalry between the two nations[2] and extended interests from the regional actors Russia and Turkey[2]. The European Union also sought to influence the region through the Eastern Neighborhood initiatives. Some broader repercussions of this war have become evident. They are worth assessment in terms of qualities of warfare. The term "qualities" in this article is referred to as "a qualitative category to describe relevant differences in military conduct between two parties at war". Qualities of warfare of the Second Nagorno-Karabakh War should be discussed by highlighting the following aspects: command and control, tenants of maneuver warfare, flexibility of tactics, and the joint capabilities of the armed. The quality of the command and control is a key capability that can disrupt or enhance operational tempo in contemporary warfare. The practical implications and theoretical works of the US Air Force colonel John Boyd laid a solid background.[2]

The Second Nagorno-Karabakh War has highlighted two of the most important competing factors of Command and Control (C2) capabilities: reliability of secure communications and sensors' integration into data sharing. For the Azerbaijanis, continuous upgrades of armed force's capacities also included communications technology. During the war Azerbaijani armed forces conducted synchronized flanking maneuvers through southern and northern grounds towards Nagorno-Karabakh.[3] Given the

steep elevation and reduced line of site of the area, the capability to control maneuver on two avenues of approach would suggest a more robust, timely paced C2 capability on their side. Integration of surveillance and reconnaissance sensors data into tactical decision cycle assisted advancing Azerbaijani forces. Research suggests[4] that technology supplied by Turkey and Israel led to enhanced situational awareness of Azerbaijani forces and rapid decision making at various tactical levels.[5]

Armenian forces were eager to fight on the defensive and hold prepared defenses across elevated areas.[6] That operational choice led to the preparation of deliberate defensive positions with a more static, landline and short distance communication capacity.[7] The setup of pre-planned defenses was ineffective when confronted by rapidly advancing and direct strike supported Azerbaijani units and the Arminian forces were unable to adjust C2 for a mobile defense.[8]

Therefore, the second quality of warfare became evident, highlighting tactical differences between two adversary forces. The Second Nagorno-Karabakh war showed different conduct of the maneuver warfare. The campaign fought by the Armenians was based on a static deliberate defense. That concept was developed due to the need to protect dominant high grounds in Nagorno-Karabakh provinces. Those areas have been controlled by Armenian forces since 1996. Meanwhile, Azerbaijani forces' relied on offensive maneuver in this steep terrain and required rapid displacement and movement to provide continuous support of integrated direct and indirect fire systems. Conduct of this offensive campaign was a tactically demanding task given the restricted avenues of approach of Nagorno-Karabakh. A limited space for maneuver of weapon systems and the increased need to overwhelm the adversary with fires effects was the essential tactical challenge. It has turned out that the success in handling this challenge caused the breakthrough advantage.

A limited space for maneuver of weapon systems and the increased need to overwhelm the adversary with fires effects was the essential tactical challenge.

The success of the fire support integrated maneuver has brought overwhelming enabling effects for Azerbaijani forces. In this war tanks and armored infantry fighting vehicles were hunted as valuable targets and the neutralization and destruction of these targets significantly downgraded Armenian capabilities.[9] Fire engagement at longer distances were more successful on Azerbaijani side. For the Second Nagorno-Karabakh War tanks were less the agile hunters and more the hunted targets.[10] The success of hunting down Armenian tanks was implied by their tactical choices in the defense. The case of Nagorno-Karabakh has demonstrated that the advantage of maneuver is not based solely on unshakable tactics and exploitation of surrounding terrain. Although that could have been estimated as an operational guarantee on Armenian side.[11]

Military practice from that war suggests that the success of maneuver warfare would be highly dependent on integrated combat support capabilities.[12] Western views of maneuver warfare is based on technological enhancements. There are two examples suggesting that the technology-enabled form of maneuver warfare was more effective during the Second Nagorno Karabakh war. The first is the dominance of UAVs as an integrated weapon system and their effectiveness against armor targets.[13] The second is the integration and use of C2 capabilities. Azerbaijani maneuver was covered by outreaching UAV capability and target data transmission. This is a modern quality of deliberate and dynamic maneuver that requires extended situational awareness and rapid target elimination with all available weapon systems. This effectiveness of Azerbaijani offense suggests that the Second Nagorno-Karabakh War has brought broader implications for the changing understanding of warfare. In those high grounds deliberate defense on dominant terrain supported by massive artillery has met with rapid maneuver supported by increased situational awareness and precise strike capabilities. The later set of war fighting options has gained a winning hand.

The initial outcomes of the war suggested a more devastating fire and maneuver to be applied by Azerbaijani forces. Initial battle damage assessments indicated that Armenia lost about 6 times more tanks and about 16 times more artillery pieces, never mention the destruction of air defense positions by integrated surveillance and strike capabilities of Azerbaijani forces.[14] Tactical outcomes of that war suggest

that advanced maneuver supported by technological capabilities has spared some additional troops for Azerbaijani forces to implement additional offensive in the north[15] and conduct an astounded light force maneuver to retake the highland town of Shusha.[16] The success at Shusha had a broad operational effect as Armenian positions were disrupted and military units were forced to abandon high ground defensive positions. Soon after Shusha fell, the Armenian prime minister declared the agreement to start negotiations for the cease fire. Thus, the takeover of historical Shusha town brought a decisive tactical victory for Azerbaijani forces.

THE DECISIVE ROLE OF MODERNITY

The overview of gradual changes of qualities of warfare suggests that Azerbaijani side was well prepared and technologically advanced. The comparison of C2 capabilities, maneuver warfare execution and joint interaction suggests that those were the main qualities exploited during the Second Nagorno-Karabakh War. Practical achievements on Azerbaijani side also suggest that technologically advanced military forces have more flexibility of where and for what to task infantry. That was the driving factor enabling their offensive maneuver on two different avenues of approach. As the war over Nagorno-Karabakh has shown, the pure role of the infantry is still essential for consolidation of the gains.

The Second Nagorno Karabakh War was different from the first one. The outstanding difference was the usage of modern technology that provided a significant dominance for Azerbaijani side. This finding suggests that there are a few key lessons to be learned from the Second Nagorno-Karabakh War. Firstly, there is an increased need to have a reliable and adaptive decision cycle in contemporary war campaign. That decision cycle needs to be agile and resilient despite of environment features, operational changes, and adversary effects.

The second lesson suggests that armor formations need to be protected and exploited more thoroughly. Danger to armor maneuver is comes from terrain obstacles, mine fields and concentrated fire power of adversary and armed Unmanned Aerial Vehicles (UAVs). As Gen. James C. McConville, Chief of Staff of the U.S. Army, has suggested, unmanned aerial vehicles should be estimated as a new improvised explosive device type of threat for the next ten years.[17] Thus, the enablement of maneuver warfare implies a two-fold solution for protective armor maneuver. Dispersed, fast and coordinated maneuver forms one way for solution, as technological innovation for early detection and neutralization of selective type of aerial platforms leads to important supplementary role.

The third lesson indicates the importance of the joint approach to the application of military forces. During the Second Nagorno-Karabakh War two different war fighting capabilities have collided. The outcome of this war reassures that there is no second place in the contemporary war. More than that, this war teaches us that the joint force employment based on speed, range and convergence provide victorious achievements. The contemporary warfare has become a competition based on joint capabilities of irregular warfare elements, regular forces, and combat support empowered by educated, well trained specialists. All needed elements must be addressed seriously in order to adjust and build-up contemporary war fighting capabilities.

CONCLUSIONS

Southern Caucasus became an illustrative case of how different qualities of warfare can compete on the contemporary battleground. The campaign over Nagorno-Karabakh was waged between two forces with different operational visions. Azerbaijan have forced a deliberate extension of armed force capacities, in cooperation with Turkey and other partners have strived for a better trained force that would manage advanced technology. Meanwhile, Armenia has concentrated on quantitative capabilities of weapon systems positioned to dominate and defend key high grounds of Nagorno-Karabakh.

It turned out that the qualities of warfare based on rapid communication, enhanced maneuver and integration of precise strike capabilities has played a winning part in this war. This suggests that the Western way of war based on technological de-

... the qualities of warfare based on rapid communication, enhanced maneuver and integration of precise strike capabilities has played a winning part in this war.

velopments and joint force capabilities has been adjusted by Azerbaijani forces. Thus, the modernity had a decisive impact in this war.

Observations provided in this article are worth further considerations. That is due to two reasons. First, the fate of Nagorno-Karabakh is not fully determined and might cause additional escalation in the future. Second, the outcomes of this war are examined by regional powers, Russia being one of them. NATO allies should not disregard the Second Nagorno-Karabakh war but pay a sufficient attention to qualities of warfare demonstrated there. This is a helpful case analysis that could assist in strategic decisions of how to adjust and improve war fighting capabilities aimed at confronting near-peer competitors.

END NOTES

[1] Kazemzadeh F., *The Struggle for Transcaucasia: 1917-1921*, New York: Philosophical Library, 1951.

[2] Osinga F., "The Enemy as a Complex Adaptive System: John Boyd and Airpower in the Postmodern Era", Olsen A., ed., *Airpower Reborn: The Strategic Concepts of John Warden and John Boyd*, Maryland, Naval Institute Press, 2015, p. 48-54.

[3] *Nagorno-Karabakh War Analysis*, Lithuanian Land Force Command Staff, G2 Intelligence Analysis Branch, Vilnius, December 2020.

[4] Shaikh S., Rumbaugh W., "The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense", Center for Strategic and International Studies, December 2020, https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense, 2021 07 29.

[5] Mirza H., Presentation of Azerbaijani tactical solutions and aspects of war, Conference of the Nagorno-Karabakh War Analysis, Vilnius: Lithuanian Military Academy, March 2021.

[6] *Nagorno-Karabakh War Analysis*, Lithuanian Land Force Command Staff, G2 Intelligence Analysis Branch, Vilnius, December 2020.

[7] Mirza H., Presentation of Azerbaijani tactical solutions and aspects of war, Conference of the Nagorno-Karabakh War Analysis, Vilnius: Lithuanian Military Academy, March 2021.

[8] *Nagorno-Karabakh War Analysis*, Lithuanian Land Force Command Staff, G2 Intelligence Analysis Branch, Vilnius, December 2020.

[9] *Nagorno-Karabakh War Analysis*, Lithuanian Land Force Command Staff, G2 Intelligence Analysis Branch, Vilnius, December 2020.

[10] Reynolds N., Watling J., "Your Tanks Cannot Hide", RUSI Defense Systems publication, https://rusi.org/explore-our-research/publications/rusi-defence-systems/your-tanks-cannot-hide, 2020 03 20.

[11] Remler P., Giragosian R., et al, "OSCE Minsk Group: Lessons from the Past and Tasks for the Future", OSCE In-sights Vol. 6, Baden-Baden: Nomos, 2020, https://doi.org/10.5771/9783748922339-06;

[12] Gordon M., Gen. Trainor B., *Cobra II. The Inside Story of the Invasion and Occupation of Iraq*, Pantheon Books, New York, 2006; Rayburn J., Sobchak F., eds., *The U.S. Army in the Iraq War: Surge and Withdrawal 2007-2011*, Vol. 2, Strategic Studies Institute, U.S. Army War College, 2019.

[13] Watking J., Dr., "The Key to Armenia's Tank Losses: The Sensors, not the Shooters", RUSI publication, https://rusi.org/explore-our-research/publications/rusi-defence-systems/the-key-to-armenia%E2%80%99s-tank-losses-the-sensors-not-the-shooters, 2020 06 20.

[14] *Nagorno-Karabakh War Analysis*, Lithuanian Land Force Command Staff, G2 Intelligence Analysis Branch, Vilnius, December 2020.

[15] Ibid.

[16] Kramer A., "Azerbaijan Claims Capture of Key Town in Nagorno-Karabakh", New Yok Times, 8 November 2020, https://www.nytimes.com/2020/11/08/world/europe/nagorno-karabakh-azerbaijan-shusha.html?searchResultPosition=3, 2021 07 25.

[17] General James McConville: "Not Fighting the Last War Better", Western Way of War, Podcast Series, Episode 58, 5 August 2021, https://rusi.org/podcasts/western-way-of-war/episode-58-general-james-mcconville-not-fighting-last-war-better.

ARMY AIRSPACE MANAGEMENT DURING LARGE-SCALE COMBAT OPERATIONS

A group of four AH-64E Apache helicopters arrive after a four-day journey to Hunter Army Airfield, Georgia on July 16, 2021. (Photo by: Sgt. Savannah Roy, USA)

By CW3 Christopher Cronen, USA and CW3 Michael Rich, USA

INTRODUCTION

The Air Defense Airspace Management/Brigade Aviation Element (ADAM/BAE) is a critical combat multiplier for Army brigade formations during large-scale combat operations (LSCO). Airspace is a finite resource which is under the purview of the joint commander, yet the number of airspace users utilized in the brigade area of operations continues to grow at an exponential rate. The ADAM/BAE remains uniquely situated to provide airspace management of the growing number of airspace users required for success against a peer competitor in LSCO.

DEVELOPMENT OF THE ADAM/BAE

The need for trained and equipped Army airspace managers has been identified throughout the rise of the air domain, but was made most apparent during the early days of Operation Iraqi Freedom. In 2004, at the direction of Chief of Staff of the Army General Peter Schoomaker, the Army transformed the brigade combat teams to incorporate additional fires, command and control, and sustainment capabilities.[1] The newly transformed Army brigade combat teams would incorporate new equipment and organizations, combining different units from various Army branches and warfighting functions under a single brigade commander. These units brought new capabilities with them, in the form of indirect fires from the direct support field artillery battalions, and the RQ-7 Shadow unmanned aerial system (UAS) from the attached military support company, among others.

Other airspace users that required dedicated airspace management continued to develop during this period as well. Small UAS systems, such as the RQ-11 Raven, were fielded and issued to units at the company, troop, and battery level to provide low-echelon intelligence support.[2] Cyber-electromagnetic activities were employed throughout the battlefield, which could potentially impact airspace and required coordination to utilize. Aviation task forces were em-

ployed to support the brigade combat teams (BCT), offering reconnaissance, attack, lift, and assault capability to deployed maneuver forces.[3]

The newly transformed BCTs brought a lot of versatility and flexibility to the fight, but required dedicated airspace managers to ensure that these new capabilities could be integrated and synchronized in a safe and efficient manner. The ADAM/BAEs filled that gap during the counterinsurgency (COIN) years of Iraq and Afghanistan, providing airspace management for counterfire missions, medical evacuation, UAS employment, air assault operations, and planned fire missions.[4]

BRIGADE AIRSPACE MANAGEMENT DURING LSCO

In its current incarnation, the BCT ADAM/BAE is a small team, consisting of air defense and aviation personnel and equipment. Each ADAM/BAE varies in terms of personnel and equipment, depending on the type of brigade it is designed to support (an armored BCT has a different ADAM/BAE setup compared to a field artillery brigade, for instance). While the composition of each ADAM/BAE varies, there are generally anywhere from 8-12 personnel, with little to no overlap in terms of personnel expertise.[5] For instance, there is only one air defense officer, one air mission survivability officer, and one airspace control sergeant. The small size and lack of redundancy in skill sets highlights the critical need to ensure cross-training of disciplines occurs between ranks (officer/enlisted) and branches (air defense/aviation).[6]

The small size and lack of redundancy in skill sets highlights the critical need to ensure cross-training of disciplines occurs between ranks (officer/enlisted) and branches (air defense/aviation).[6]

While the ADAM/BAE may be small in size with no redundancy in terms of skills or experience, it is well equipped to provide air defense, aviation, and airspace management expertise to the supported brigade. The air defense component of the ADAM/BAE consists of an air defense officer, a command and control systems integrator warrant officer, and enlisted battle system operators with the military occupational specialty (MOS) of 14G. These personnel provide the expertise needed to plan and synchronize air and missile defense operations with brigade's scheme of maneuver. The air defense personnel, using the organic air defense command and control systems in the ADAM Cell shelter, are able to integrate with the joint datalink network in order to provide external sensor coverage, air track data, and aerial situational awareness to the brigade staff and subordinate units.

The aviation personnel within the BAE includes rated aviators, specifically the brigade aviation officer, deputy brigade aviation officer, and an air mission survivability officer. Ideally, these positions should be filled by aviators from across the full spectrum of Army rotary-wing aircraft (i.e. Apache, Blackhawk, and Chinook) so there is experience with all Army aviation mission sets (attack, reconnaissance, lift, and assault). However, these personnel assignments are not generally manned with this goal in mind. The aviation branch enlisted personnel consists of aviation operations sergeants (MOS: 15P) and airspace control sergeants (MOS: 15Q). The aviation operations sergeant produces and processes air mission requests providing needed aviation support to brigade operations for all aviation tactical, enabling, and sustaining tasks (screen, attack, reconnaissance, air assault, air movement, aeromedical evacuation, and C2 support).[7] The airspace control sergeant provides airspace management expertise and operates the Tactical Airspace Integration System (TAIS) C2 system in support of brigade airspace activities.

The requirement for the brigade to manage airspace users in the brigade area of operations during LSCO relies on the combined expertise of both air defense and aviation personnel within the ADAM/BAE section. While planning operations, this unique pairing of air defense and aviation personnel allows for planning of airspace use, development of the airspace control appendix to the operations annex, and analysis of airspace usage to identify, determine, and resolve conflicts. In the current operations fight, the ADAM/BAE monitors airspace usage, provides immediate airspace coordinating measure requests (ACMREQs) for airspace usage that conflicts with current operations, and executes near-real-time management of Army airspace users.

To manage Army airspace users in the brigade area of operations during LSCO, the ADAM/BAE utilizes procedural control. Due to the decentralized nature of Army operations, procedural control is the Army's preferred airspace methodology[8], as it relies on the dissemination and distribution of previously-agreed upon orders and procedures. The ADAM/BAE utilizes tactics, techniques, and procedures (TTP), standard operating procedures (SOP), planned airspace coordination measures (ACM), and their developed airspace control appendix to help plan, coordinate, synchronize, and integrate airspace users operating in support of the brigade.

A well-planned and well-rehearsed unit airspace plan utilizing procedural control will allow for the timely synchronization of decentralized airspace users to support the warfighter and minimize conflicts during current operations. Timeliness is always a consideration during combat operations, as any delay will result in degradation of desired effects. For this reason, it is imperative that brigade airspace plans need to be as free of conflict as possible when developed, built, and submitted for use in the airspace control order. While airspace conflicts are inevitable, they should be identified and mitigated during the planning phase to minimize their impact and allow for brigade resolution of these airspace conflicts during current operations.

If brigade airspace conflicts cannot be resolved internally, however, the airspace conflict must then be elevated to the division joint air-ground integration center (JAGIC) for resolution. The JAGIC, consisting of an Army division aligned with an Air Force air support operations center (ASOC), is a current operations TTP that arranges Army and Air Force personnel for the purpose of controlling division-assigned airspace. The intended purpose of the JAGIC is to support division-level current operations through the rapid execution and clearance of joint fires and airspace deconfliction.[9]

While the JAGIC TTP enables decision-making authority to provide for responsive air-ground operations supporting the division commander's scheme of maneuver, the JAGIC's success is reliant on subordinate brigades planning airspace and managing airspace users appropriately. A poorly constructed brigade unit airspace plan that leads to airspace conflict requiring JAGIC resolution will slow down the pace of LSCO. Slowing the pace of LSCO will hinder planned and dynamic fires, UAS employment, and aviation operations at the brigade, thereby allowing the enemy to exploit friendly inaction. The division must then allocate JAGIC resources, time, and effort to resolving airspace conflicts that could have been prevented with proper planning. This diversion of resources and time reduces the division's capability to rapidly execute joint fires in support of division operations.

Oklahoma Army National Guard soldiers conduct their required Additional Flight Training Period (ATFP) hours with the RQ-7 Bravo or "Shadow" at Muldrow Army Heliport in Lexington, Oklahoma, Jan. 29, 2018. (Photo by Staff Sgt. Jason Lay, USARNG)

INTEGRATION OF BRIGADE AIRSPACE USERS DURING LSCO

The ADAM/BAE's chief responsibility is to provide airspace management of brigade airspace users to support the commander's scheme of maneuvers while preventing fratricide and maximizing combat power. The main task supporting this responsibility is the requirement to identify and determine airspace users and their requirements.[10] Brigade organic airspace users and external airspace users operating in support of the brigade are found across the six Army warfighting functions, and must be fully synchronized and integrated in order to fully support brigade operations. This synchronization of airspace manage efforts across all six warfighting functions (movement and maneuver, fires, intelligence, protection, sustainment, and command and control) masses combat power at the decisive place and time and is vital to success in LSCO.

Chief among airspace users in the movement and maneuver warfighting function is Army aviation, which includes the rotary wing missions of attack, reconnaissance, lift, and assault. The combat aviation brigade (CAB) in a LSCO environment will likely be employed as a maneuver formation by the division commander. It is unlikely that the CAB will be broken down to battalion-sized task forces to support the brigade combat team, similar to what was experienced in Iraq and Afghanistan. While the CAB will probably be used as a maneuver element for the division, the firepower and tactical mobility provided by Army rotary-wing aircraft are not replicated anywhere else in the Army footprint. The ADAM/BAE (and brigade aviation officers in particular) must be proactive in requesting the rotary-wing assets they need to support brigade operations.

Other movement and maneuver airspace users in the brigade footprint that must be managed and integrated into the unit airspace plan include those at the company level. Small UAS, such as RQ-11 Ravens, will be employed to support low-level intelligence collection for the company, and if not planned for and executed appropriately, will put other airspace users (specifically low-flying manned aircraft) at greater risk. However, ADAM/BAE airspace managers that are too cautious and put up burdensome restrictions to employing small UAS may be denying a critical capability to company commanders. Mortars are similar in concept to small UAS, in that they should be responsive to the company commander in order to maximize combat power during LSCO but must be integrated appropriately to mitigate risk to other airspace users.

Within the fires warfighting function, field artillery is the preponderance of airspace users within the brigade area of operations. To support maximum combat power in a LSCO environment, brigade airspace plans should be built to emphasize a permissive fires environment while providing protective control measures for friendly aircraft operating within the brigade area of operations.

> Maneuver Short-Range Air Defense (M-SHORAD) is making a return to the contemporary battlefield and must be integrated within the brigade area of operations as well.[11]

Maneuver Short-Range Air Defense (M-SHORAD) is making a return to the contemporary battlefield and must be integrated within the brigade area of operations as well.[11] With tactical air defense units operating in close concert with other friendly manned airspace users while hostile aircraft are present, there must be additional emphasis on air-ground coordination in order to prevent fratricide. The potential for a friendly aircraft getting shot down by friendly air defense fires will remain high if not properly addressed during planning. These should incorporate airspace coordination measures for aircraft returning from forward positions, positive identification procedures, and rules of engagement for air defense forces. For aviation considerations, aviator check-in procedures to friendly air defense units must be incorporated as well.

The intelligence warfighting function brings unique capability to the brigade formation. Brigade tactical UAS assets, such as the RQ-7 Shadow, provides intelligence collection capability to the brigade commander but requires special integration requirements. Their range, speed, and altitude often puts them in the vicinity of low-flying aircraft within the brigade area of operations. Additionally, the lack of real-time situational awareness of environmental considerations on the remote-piloted aircraft requires

additional buffer space between itself and other manned airspace users.

Protection and sustainment warfighting functions possess their own airspace management integration criteria. While not traditional airspace users, chemical, biological, radiological, and nuclear (CBRN) and engineer effects (to include mine-clearing activities and explosive ordnance disposal) can potentially affect airspace usage within the brigade area of operations. The sustainment warfighting function includes several capabilities that require ADAM/BAE airspace managers to effectively integrate into brigade operations during LSCO. Among these are low-cost, low-altitude (LCLA) resupply drops, a cost-effective means of providing resupply across the LSCO battlefield.[12] "Ring routes," employed by the division to resupply brigades via lift rotary-wing in the forward area, traverse across subordinate boundaries in the division area of operations and require close coordination to ensure they are deconflicted from both SHORAD fighting positions and employed field artillery batteries.

> A poorly trained and undermanned ADAM/BAE will result in an inability to integrate critical capabilities ...

Trained, equipped, and proficient airspace managers at the ADAM/BAE are required to integrate all these capabilities from across the warfighting functions. A poorly trained and undermanned ADAM/BAE will result in an inability to integrate critical capabilities such as artillery, mortars, UAS, and M-SHORAD, directly impacting that brigade's ability to fight. The capabilities listed above are merely the current capabilities. As technology continues to develop and improve, other airspace users will emerge to support brigade operations in the LSCO arena. Directed-energy weapons are being tested for future use to support the brigade's counter-UAS mission.[13] Advances in artificial intelligence, miniaturization, UAS development, and other manned and unmanned platforms will greatly increase the number of airspace users that require detailed synchronization and integration in the brigade footprint.[14]

ADAM/BAE AIRSPACE PLANNING

The ADAM/BAE relies on detailed planning in order to integrate and synchronize as many airspace users as possible to support the brigade commander's scheme of maneuver. LSCO airspace planning requires the ADAM/BAE to coordinate airspace users and airspace user requirements from across warfighting functions, staff elements, and adjacent and subordinate units. A means to achieving this is the airspace control working group (ACWG).[15] The purpose of the ACWG is to synchronize contributions and requirements of all airspace users to best support the brigade commander's operations. Identification of airspace users and their requirements is critical for the development of ACMREQs designed to maximize employment of airspace-using assets, to include aviation, field artillery, and air defense.

Ideally, any brigade staff element with a stake in airspace, or representing an airspace user, would be an ACWG attendee. The ACWG is chaired by the brigade aviation officer and a non-comprehensive list of ACWG attendees would include the brigade fire support officer (representing the fires warfighting function), the brigade air defense officer (representing the supporting air defense unit), and the air liaison officer (representing the joint air element). Other attendees should include the military intelligence company (representing the brigade RQ-7 Shadow capability) and the aviation or air defense unit liaison officer (if the brigade is provided direct or general support by an aviation or air defense unit).

Outputs of the ACWG include developed ACMREQs for airspace users supporting the brigade, developed airspace usage priorities and risk acceptance guidance, the air-ground operations communications plan, and the completed brigade unit airspace plan. Developing airspace usage priorities during planning are especially important, in that they will guide timely decision-making during current operations as to what airspace user takes precedence over others in the event of an airspace conflict. Risk acceptance guidance will determine where the commander is willing to take risk when there is an inevitable airspace conflict while conducting operations. Receiving the commander's risk acceptance guidance ahead of time will decentralize decision-making and allow for timely responses during current operations. The air-ground operations communications plan will identify frequencies, call signs and check-in procedures for rotary and fixed-wing aircraft, highlighting how aircraft will check in to the ADAM/BAE or supported unit

while traveling through airspace above the brigade area of operations.

The product of brigade airspace planning efforts is the unit airspace plan. The unit airspace plan incorporates guidance from higher headquarters operations orders, the theater airspace control plan, and area air defense plan, as well as the brigade's own ACMREQs and fire support coordination measure requests built to support the brigade commander's scheme of maneuver. Utilizing the brigade TAIS, the unit airspace plan and its associated ACMREQs are then transmitted digitally to the division and onward, for incorporation in higher organization's unit airspace plan and ultimately for inclusion into the airspace control order for execution. Building a flexible, simple, and well-understood unit airspace plan is critical for success while conducting air-ground operations, as both organic and external airspace users operating in support of the brigade will be required to know and understand their task and purpose to support brigade operations.

LSCO AIRSPACE MANAGEMENT

ADAM/BAE airspace managers not only plan airspace for future operations, but also manage airspace users during current operations. Airspace management during LSCO is reliant upon detailed analysis and integration during the planning phase. A good unit airspace plan will facilitate better decision-making by informing commanders of where other airspace users are operating, what the airspace usage priorities are, and what risk acceptance should be implemented during operations. Conversely, a poor unit airspace plan will lead to airspace conflicts, impacting combat power by delaying response times during critical time-sensitive missions such as counterfire. This also prevents airspace utilization by critical assets such as company UAS, brigade tactical UAS, and planned fire missions. Worst-case scenarios for poor airspace planning includes the potential for fratricide and possible destruction of critical warfighting platforms (rotary-wing and fixed-wing aircraft).

Airspace management operations during LSCO must utilize the digital systems that the ADAM/BAE possesses, to include the air defense systems integrator (ADSI), the air and missile defense workstation (AMDWS), the forward area air defense (FAAD), and the tactical airspace integration system (TAIS).[16] While all possess tactical datalink capability to some degree, each provides a unique capability to the brigade command post during LSCO. The AMDWS will provide the air defense personnel the capability to plan air defense weapon and sensor employment against enemies forces, while the FAAD will provide the ability to monitor the air defense fight of supporting air defense forces against hostile aircraft. The ADSI was largely utilized during the COIN years for beyond line-of-sight tactical datalink capability in fixed static locations, such as forward operating bases. However, the ADSI will be critical in the LSCO environment for supporting Link 16 operations via the Multifunctional Information Distribution System (MIDS). The brigade command post must be mobile and displace often to avoid destruction due to enemy detection and engagement via long-range precision fires, and the MIDS Link 16 capability will support this mobility requirement.[17]

Digital sustainment training is critical to building and maintaining individual and collective skill task proficiency.

Digital sustainment training is critical to building and maintaining individual and collective skill task proficiency. The C2 systems within both the ADAM/BAE and the brigade fires cell are technically demanding and prone to skill degradation if not exercised. Operators must be proficient on their assigned C2 system. Digital sustainment ranges using organic equipment must be conducted often at home station, and incorporated onto the training schedule and annual training guidance. Every opportunity to employ the ADAM Cell shelter and its associated equipment must be taken, to include battalion live-fire exercises, artillery battalion gunnery, and aviation gunnery. Any time there is weapon systems operating or training within the brigade, the ADAM/BAE should be present to both employ the ADAM/BAE C2 systems and to conduct airspace planning and airspace management for the associated weapon system.

There is no question that the digital systems within the ADAM/BAE are a combat multiplier and must be utilized to the maximum extent possible. However, brigade airspace managers in a LSCO environment must be ready to operate in a degraded environment. The enemy possesses a wide assortment

Guardsmen conduct RQ-11 Raven training to better prepare these Soldiers and their units to conduct reconnaissance missions with the lightweight unmanned aerial vehicle at Fort Stewart, Georgia on April 16, 2014. (Photo by: MAJ. Will Cox, ARNG)

of capabilities and effects that can disrupt friendly computer networks, radio frequencies, and digital systems.[18] ADAM/BAE airspace managers must rehearse their capability to manage airspace while operating in a degraded or analog fashion. The unit airspace plan must identify provisions to account for enemy activity to disrupt the network. This should include planning to identify primary, alternate, contingency, and emergency means of conducting air-ground communications, unit airspace plan submission, and tactical datalink operations. Analog methods of tracking airspace usage, including physical maps and overlays, running estimates, and other hardcopy methods of capturing and managing information, should be considered for any period where digital system usage is impacted.

Key to an ADAM/BAE's performance during LSCO are rehearsals. As the brigade airspace element, the ADAM/BAE must participate in brigade combined arms rehearsals to synchronize airspace utilization within the brigade scheme of maneuver and scheme of fires. Throughout the rehearsal, the ADAM/BAE must identify key decision points, ensure that the commander's airspace usage priorities are known and understood, and ensure that planned airspace usage during all phases is consistent with the commander's intent.

Other required rehearsals for successful airspace management during LSCO includes battle drill rehearsals. The ADAM/BAE must identify and delineate battle drills and TTPs to support common LSCO activities requiring airspace management, such as medical evacuation (MEDEVAC) operations, counterfire missions, immediate fire support, immediate close air support, and deliberate rotary-wing attack operations. These battle drill rehearsals should include all affected sections within the brigade command post and should be rehearsed often to build proficiency, develop technical proficiency (if utilizing C2 systems), and to maximize responsiveness while conducting the LSCO fight.

CONCLUSION

The ADAM/BAE was conceived from a need to manage Army airspace users in the COIN environment. While the ADAM/BAE grew and developed during the COIN years of Iraq and Afghanistan, the need for airspace management grows even greater during operations against a peer competitor in LSCO. As technology develops, the number of airspace users and their capabilities will continue to grow, and our enemies capabilities grows as well. The brigade ADAM/BAEs must be trained and equipped to integrate and synchronize air defense, aviation, and

airspace management to support brigade operations. The ADAM/BAE remains the Army's solution to managing airspace users at the brigade echelon, providing for the safe, efficient, and flexible use of airspace while maximizing combat power and preventing fratricide.

Chief Warrant Officer 3 Christopher Cronen is the ADAM/BAE Air-Ground Operations lead instructor and is assigned to Headquarters and Alpha Battery, 2nd Battalion, 6th Air Defense Artillery at Fort Sill, Oklahoma. He has served in a variety of positions at the battalion, brigade, and division, both in garrison and deployed.

Chief Warrant Officer 3 Michael Rich is the ADAM/BAE Air-Ground Operations course manager and is assigned to Headquarters and Alpha Battery, 2nd Battalion, 6th Air Defense Artillery at Fort Sill, Oklahoma. He has served in a variety of operational positions, from ADAM Cells to Patriot and THAAD.

END NOTES

[1] CSA, 2004 Army Transformation Roadmap, July 2004. https://apps.dtic.mil/dtic/tr/fulltext/u2/a440478.pdf

[2] Defense Industry Daily Staff, https://www.defenseindustrydaily.com/raven-uav-draws-raves-from-the-field-067/.

[3] Army Field Manual FM 3-04 Army Aviation, 6 April 2020, page 2-13.

[4] US Army, "ADAM Cell Combines ADA, Aviation in Iraq." http://www.defense-aerospace.com/articles-view/release/3/43939/us-army-tests-new-doctrine-in-iraq-(aug.-12).html.

[5] Army Tactical Publication ATP 3-01.50 *Air Defense and Airspace Management Cell Operations*, 5 April 2013, page 2-4.

[6] There are only two battle system operators to operate four C2 systems during continuous current operations. Cross-training of personnel is a must to ensure digital systems are fully employed.

[7] Army Field Manual FM 3-04 *Army Aviation*, 6 April 2020, page 3-1.

[8] Army Field Manual FM 3-52 *Airspace Control*, November 2016, page 1-4.

[9] Army Training Publication ATP 3-91.1 *The Joint Air-Ground Integration Center*, 17 April 2019, page 1-2.

[10] Army Field Manual FM 3-52 *Airspace Control*, November 2016, page E-2.

[11] Gary Sheftick, "Army Rebuilding Short-Range Air Defense." https://www.army.mil/article/224074/army_rebuilding_short_range_air_defense.

[12] Mark VanGerpen, "Low-altitude drops cut costs, keep Soldiers safe." https://www.army.mil/article/109180/low_altitude_drops_cut_costs_keep_soldiers_safe.

[13] Todd South, "This Army fires experiment covers detection, jamming, drone kill chains and new ways to shoot artillery." https://www.armytimes.com/news/your-army/2018/11/14/this-army-fires-experiment-covers-detection-jamming-drone-kill-chains-and-new-ways-to-shoot-artillery/.

[14] Theresa Hitchens, "DARPA Builds AI To Avoid Army, AF Fratricide." https://breakingdefense.com/2021/02/darpa-builds-ai-to-avoid-army-af-fratricide/.

[15] Army Field Manual FM 3-52 *Airspace Control*, November 2016, page 2-4.

[16] Army Tactical Publication ATP 3-01.50 *Air Defense and Airspace Management Cell Operations*, 5 April 2013, page 1-12.

[17] Sydney J. Freedberg Jr, "A Perfect Harmony Of Intense Violence': Army Chief Milley On Future War." https://breakingdefense.com/2018/10/a-perfect-harmony-of-intense-violence-army-chief-milley-on-future-war/.

[18] Sebastien Roblin, "Electronic warfare: The U.S. is losing the invisible fight to Russia's dominant capabilities." https://www.nbcnews.com/think/opinion/russia-winning-electronic-warfare-fight-against-ukraine-united-states-ncna1091101.

KILL BOX UPDATE 2022

An MQ-9 Reaper flies a kill box training mission over the Nevada Test and Training Range, July 15, 2019. (Photo by: A1C William Rio Rosado, USAF)

Maj Evan "WAYST" Fillman, USAF and Lt Col Greg "Skidder" DeFore, USAF (RET)

INTRODUCTION

In the fall of 2008, members of the inaugural and second MTTP Kill Box joint working groups published an article called, "Kill Box Update," in the Air Land Sea Bulletin. Large changes in MTTP Kill Box and the need to consolidate information and decisions generated from a joint staff joint fires area test motivated the authors to publish an update to the field. History repeats itself, and again, 13 years later, another kill box update is necessary to educate the joint force on the results of a joint test affecting the development of MTTP *Kill Box*.

In the fall of 2020, the Air Force and Army doctrine centers requested an in-depth review of MTTP *Kill Box* to ensure the MTTP was executable in fielded command and control (C2) systems. The resulting research revealed the 2014 and 2018 versions of MTTP *Kill Box* contained doctrinally correct, but tactically incorrect, instructions to execute a kill box in a standardized way across the joint force. Ultimately, another joint test was needed to ensure the next published version of MTTP *Kill Box* contained standardized and executable TTP for kill box. This kill box update is intertwined with the history of MTTP *Kill Box* leading to the 2021 joint kill box test.

KILL BOX AND C2 AUTOMATION HISTORY

The historical instances of large-scale combat operations requiring joint fires interdiction against fielded forces are intermittent. As such, MTTP *Kill Box* has changed with peacetime tests, exercises, doctrine, and technology. MTTP *Kill Box*, as an operationally planned and jointly integrated tactic, technique, and procedure relies heavily on fielded C2 capabilities. Therefore, the limitations and applicable details of C2 automation systems are provided as well.

During the late 1970s in South Korea and in West Germany, planners created a grid system to enable quick C2 of airspace and identified them as kill boxes (two words). These kill boxes were used to coordinate bomber, fighter, attack helicopter, and artillery attacks.

From 2001 to 2003, killboxes (one word) were used extensively in Operation ENDURING FREEDOM and Operation IRAQI FREEDOM as a grid system for navigation, force deconfliction, and control during a variety of missions including air interdiction, strike coordination and reconnaissance, airborne alert interdiction, and airborne surveillance and reconnaissance. The killboxes did not imply or require support relationships or prior coordination. Killboxes were synonymous with the theater's common geographic reference system (CGRS) used in Operation ENDURING FREEDOM and Operation IRAQI FREEDOM. The Global Area Reference System (GARS) had not been developed yet, and killboxes were also not integrated onto the airspace control order (ACO).

TBMCS and USMTF became the backbone for CAOC operational wartime planning and is still the backbone in 2022.

In 2001, the Theater Battle Management Core System (TBMCS) replaced the Contingency Theater Air Planning System (CTAPS) in the USCENTAF Coalition Air Operations Center (CAOC). TBMCS was an enormous leap forward for air tasking order (ATO) and ACO capabilities. TBMCS generated the ATO and ACO into a data format called United States Message Text Format (USMTF) 2000 that enabled periodic digitally integrated updates across the joint force. TBMCS and USMTF became the backbone for CAOC operational wartime planning and is still the backbone in 2022.

In 2004 (published 2005), the inaugural MTTP *Kill Box* was penned to codify the lessons learned of killbox use in Operation IRAQI FREEDOM while refining and expanding the concept for worldwide use. This refinement re-adopted the historical term kill box (two words), moved the concept towards a fire support coordination measure and introduced the idea of color coding the kill box as blue or purple. An assumption was made that as an official MTTP, the refined and expanded kill box concepts would be integrated to fielded C2 digital systems. This assumption did not happen and this erroneous assumption would not be recognized until 2020.

In 2005, the Defense Information Systems Agency (DISA) USMTF Change Control Board captured the MTTP *Kill Box* updates for inclusion into the USMTF 2006 baseline. To enact the change, DISA used a recently outdated code, KILLB, and modified it to KILLBX. Six characters was also the safe digital limit preventing the full use of the two words. As is common practice with data standards, the authors of the standard, DISA, could not control which entities implemented the standard and USMTF 2006 was never adopted into TBMCS and therefore the ACO.

In 2006, the Secretary of Defense directed the development of the standardized GARS defined in Joint Publication (JP) 2-03, *Geospatial Intelligence in Joint Operations*. The GARS is a common reference system across the surface of the world. The GARS standard allowed the navigation and deconfliction aspects of the killboxes used in Operation IRAQI FREEDOM to have standardized naming and apply across the globe.

In 2007, the USAF decided that TBMCS would be replaced; however, in 2022, that TBMCS replacement has yet to be fielded. The TBMCS replacement decision resulted in TMBCS entering sustainment funding. This decision meant TBMCS would not be adequately funded to upgrade beyond USMTF 2004. The USMTF 2004 data format was penned based off standing doctrine in 2003. Effectively, this meant that the ATO and ACO content was frozen with the code options and terminology provided in USMTF 2004. Ultimately, as a result of having the ATO and ACO trapped in a singular digital format for more than 17 years there arose two major consequences.

As a negative consequence, adding any modified tactic, developed after 2003, to the ACO, such as kill box, became impossible until a TBMCS replacement could be fielded. Warfighters developed local workarounds to meld new ideas into the old format.

As a positive consequence, the usage of

USMTF 2004 remained the only option for ATO and ACO dissemination and became an anchor point. This inadvertent anchor point ensured digital interoperability as the general pace of software development increased from 2004 to 2022.

In fact, CJCSI 6241.04D directs the services to utilize the most current version of USMTF, USMTF(B), for digital interoperability. Although, CJCSI 6241.04D has been ignored in extant practice for over 17 years as a low priority for the allocation of service acquisitions funds.[2] DISA still produces new versions of USMTF based on doctrine even though updated versions are not widely implemented regarding ATO and ACO messages and formats.[3]

In 2007, the joint staff concluded a joint test titled, Joint Fires Coordination Measures, which introduced the concept of a Joint Fires Area for integrating and coordinating joint fires. The services reviewed the test and concepts but ultimately consolidated many of the results into MTTP *Kill Box* in 2009. The major update was basing kill boxes around GARS and adding the kill box coordinator (KBC). The joint test results were not incorporated fully as fielded systems could not keep pace with conceptual updates.

Unfortunately, post 2007 MTTP *Kill Box* volumes continued to be published without conducting fielded systems tests to ensure their tactical validity. Unbeknownst to the authors, the extant practice in the field was limited to using USMTF 2004 language and workarounds, meaning that many of the instructions in MTTP *Kill Box* version 2014 and 2018 were not executable within digital systems.

In 2020, the Army and Air Force doctrine centers initiated an in-depth review to ensure doctrine alignment for MTTP *Kill Box* with JP 3-52 Joint Airspace Control. The centers requested an update to MTTP *Kill Box* to specify which type of restricted operations zone (ROZ) should be used for the ACM portion of the kill box in the ACO. The review noted the type of ROZ selected for the ACM portion of the kill box would have implications in critical digital fires systems. More importantly, the review revealed that the FSCM term KILLBX was not available for use in an ACO produced from TBMCS.

In 2021, in order to ensure a valid and executable MTTP, and consistent with joint all domain command and control (JADC2) efforts, the ALSA center conducted a multiservice test to evaluate the extent of digital interoperability of kill boxes. The test focused specifically on ACO dissemination and processing. An executable standard was developed to ensure kill boxes are transmittable across the joint force on a USMTF 2004 ACO and incorporated into this manual. The doctrine test also confirmed that kill box execution still requires manual C2 status battle tracking regarding fires and airspace status of kill boxes throughout all theater air ground system (TAGS) echelons.

CONCLUSION

The results of the 2021 joint kill box test and history of kill box led the joint working group to make two major update recommendations to MTTP *Kill Box*.

The first recommendation was that in order to ensure joint force synchronization, a kill box should appear on an ACO or ACO update. The entire purpose of kill box is to represent pre-coordinated intra-component communication to the warfighter to allow for expedient target execution. The best way to represent this coordination as complete and as an official order, while minimizing the chances for friendly fire, is to leverage the existing infrastructure and procedures that allow for an ACO update. Historical large-scale combat operations show ACO updates may have happened up to 12 times a day during initial actions. The MTTP also provides options for evolving or unexpected targets that do not provide time to conduct an ACO update. If a kill box does not appear on the ACO, it will be very difficult to ensure all players are aware of the kill box's existence and thus able to conduct coordinated operations.

The second major update was to specify the manner in which a kill box should be schematically constructed on the ACO. The specific ACO construction is considered controlled unclassified information data so it does not appear in this article and will be available in the MTTP. The kill box ACO construction represents the best set of tradeoffs to ensure that MTTP *Kill Box* is executable in digital C2 systems across the joint force. Apart from ensuring basic transmission and processing, the tested kill box standard also ensured that AFATDS responds to the portions of a kill box correctly and further enhanced usability for C2 operators. The approach was live-

tested on the joint C2 systems listed in the table below in December of 2021.

On a macro level the kill box test illustrates that digital joint interoperability remains a difficult task, even with older systems. There are many levels of nuance involved with joint interoperability that involves not only the technology, interfaces, and data formats required but also the manner in which warfighters interact with systems. As new systems are fielded and doctrine advances to support joint all domain command and control, the kill box experience shows that operational tests and joint exercises remain an essential step along the development path. Any assumed, and not tested, digital linkage represents risk to the joint force.

The 2022 version of MTTP *Kill Box* containing the recommended updates is currently out for worldwide review and has an expected publication date of July 2022.[4] Warfighters can download a copy of MTTP Kill Box at https://www.alsa.mil/mttps/killbox

END NOTES

[1] Col (Ret) David Neuenswander, USAF, Mr Bo Bielinski, Col (Ret) Russ Smith, USAF. Kill Box Update. Originally published September 2008. https://www.alsa.mil/News/Article/2656499/kill-box-update/.

[2] CJCSI 6241.04D, 12 January 2021, Policy And Procedures For Management And Use Of United States Message Text Formatting, https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%206241.04D.pdf

[3] United States Message Text Format (USMTF) Website. https://disa.deps.mil/ext/cop/jintaccs/USMTF/default.aspx

[4] MTTP Kill Box. https://www.alsa.mil/mttps/killbox/

Joint C2 Systems Tested in 2021 Kill Box Test

US Air Force	US Army	US Marine Corps	US Navy	All/Joint
TBMCS	TAIS	TBMCS	TBMCS	JADOCS
-WEBAD	AFATDS	AFATDS	AFATDS	GCCS
-WARP	AMDWS	CAC2S	CAC2S	FV
-MCAMP			JMPS	
-MAAPTK			E-2C	
-ESTAT				
ASAMA-FB				

Legend:
AFATDS—Advanced Field Artillery Tactical Data System
AMDWS—Air and Missile Defense Workstation
ASMA-FP—Air Space Management Application Fieldable Prototype
CAC2S—Common Aviation Command and Control System
E-2C—Hawkeye
ESTAT—Execution Status and Monitoring
FV—Falcon View
GCCS—Global Command and Control System
JADOCS—Joint Automated Deep Operations Coordination System
JMPS—Joint Mission Planning System
MAAPTK—Master Air Attack Plan Toolkit
MCAMP—Marine Corps Air Mission Planner
TAIS—Tactical Airspace Integration System
TBMCS—Theater Battle Management Core Systems
WARP—Web-Based Airspace Request Processor
WEBAD—Web-Based Airspace Deconfliction

OVER THE HORIZON

INTRODUCTION

The summer is the season of transition and we had a significant turnover. In addition to welcoming the newly assigned action officers as well as the Director and Deputy Director, ALSA had the privilege of welcoming two new civilians filling the editor and administrative support assistant roles. Please, introduce yourself to the new ALSA members as they become familiar with the organization's processes to support joint warfighters. ALSA invites you to follow day to day operations on our website and social media accounts and hopes to see you at future joint working groups.

AIR AND SEA BRANCH

The Air and Sea branch is wrapping up the printing, revision and updates of *Personnel Recovery, Air and Missile Defense, Kill Box, Fighter Integration, Survival,* and *JFIRE* this summer. Over the next six months Air and Sea branch begins revision of *MTTP Air Operations in Maritime Surface Warfare (AOMSW)*. The Request for Feedback (RFF) *AOMSW* is expected this fall with a projected publication in early 2024. If you are interested in participating in the Joint Working Group (JWG) for *AOMSW* please contact Maj Jared Towles at jared.towles@us.af.mil.

LAND BRANCH

ALSA is finalizing and publishing revisions of two MTTPs: *Military Diving* and *Advising*. At the same time, the team has begun the revision of MTTP *Airfield Opening*.

C2, CYBER, AND SPACE BRANCH

Four MTTPs are currently under revision: *Airspace Control; Brevity; Intelligence, Surveillance, and Reconnaissance Optimization;* and, *Air-to-Surface Radar Employment*. With the recent update to JP 3-52 *Joint Airspace Control* we are reviewing it for changes that may impact our revision of *Airspace Control* MTTP. A fifth MTTP, *Theater Air-Ground System*, should begin the review cycle in fall 2022.

As the joint force moves away from conflicts in Iraq and Afghanistan, ALSA will work with Services to ensure TTPs and valuable solutions that were developed over the last two decades are retained until fully integrated into current Service doctrine. As solutions to interoperability gaps are established in current Service doctrine, ALSA will focus attention on new tactical problems through the lens of today's operating environment and change in warfare direction.

We rely on the users of our publications to keep our MTTPs current through article submission, joint working group participation, and feedback on our publications. To that end, we ask that you please stay in touch with ALSA through social media, our website, or the organizational email accounts listed in the back of this journal. We are always interested in receiving feedback and look forward to the Service member participation as we update MTTP doctrine in the coming year.

Thank You!

MAJOR EVENTS OF INTEREST

Date	Unit/Event	Description	Location	POC
20 May - 22 Jun	VALIANT SHIELD 22	Multi-Service exercise with Navy, AF participation.	INDOPACOM	C2, Cyber, and Space Branch
29 May - 3 Jun	ADRIATIC STRIKE	JTAC exercise with 22 NATO nations	Slovenia	Air/Sea Branch
06-10 Jun	RESCUE Joint Test/ TWG	Develop and validate a TTP that enables PR and IRC	JB San Antonio, TX	Air/Sea Branch
29 Jun - 04 Aug	RIMPAC 2022	Rim of the Pacific multi-national exercise	Pearl Harbor, HI	All
25-28 Jul 22	Joint Airspace Conference (JAC)	Annual multi-national and Joint airspace conference	JB Andrews, MD	All
16-18 Aug	US Army Space Training Forum	US Army space related training and initiatives brief	Peterson SFB, CO	All

ALSA JOINT WORKING GROUPS

Date	Publication	Location	Point of Contact
Sep 22	TAGS	Nellis AFB/MS Teams	C2, Cyber, and Space Branch
Nov 22	ACC	Langley AFB	Air/Sea Branch
Jan 23	AOMSW	Langley AFB	Air/Sea Branch
Jan 23	Explosive Ordnance	Langley AFB	Land Branch
Jan 23	Biometrics	Langley AFB	Land Branch
Jan 23	ACC	Langley AFB	Air/Sea Branch
Feb 23	AOMSW	Langley AFB	Air/Sea Branch

All Dates are Subject to Change
See the ALSA website for the most current Joint Working Group schedule.
https://www.alsa.mil/jwgs/

ACCESS TO ALSA PRODUCTS

ALSA Public Website

https://www.alsa.mil

ALSA SIPR Website

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

Facebook

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

Twitter

https://twitter.com/ALSA_Center

DOCTRINE CENTER LINKS

Army - https://usacac.army.mil/organizations/mccoe/cadd

Marine Corps - https://www.mccdc.marines.mil/

Navy - https://nwdc.navy.mil/

Air Force - https://www.airuniversity.af.edu/LeMay/

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**	02 SEP 21	ATP 3-52.4 MCRP 3-20F.10 NTTP 6-02.9 AFTTP 3-2.8	Description: This publication establishes communications TTP for TAC C2 to manage air operations and control airspace and aircraft. It establishes TTP for force packaging and direct air support coordination, air-to-air communication, intercept, threat warning, threat surface-to-air warning, and air-to-surface communication. **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 includes considerations for planning, coordinating, integrating, and employing joint air and missile defense systems. The publication also includes planning considerations for BMD, counter-UAS system missions, and combat-ID of air assets or threats. **Status: Revision**
AOMSW *Multi-Service Tactics, Techniques, and Procedures for Air Operations in Maritime Surface Warfare* **Distribution Restricted**	18 DEC 20	ATP 3-04.18 MCRP 3-20.4 NTTP 3-20.8 AFTTP 3-2.74	Description: This publication consolidates the Services' best TTP for missions involving air assets conducting maritime surface warfare (SUW). The objective is to enable seamless integration of joint air assets conducting maritime SUW. This publication lays the foundation for integrating forces in either preplanned or dynamic scenarios. **Status: Current**
AVIATION URBAN OPERATIONS *Multi-Service Tactics, Techniques, and for Aviation Urban Operations* **Distribution Restricted**	01 FEB 22	ATP 3-06.1 MCRP 3-20.4 NTTP 3-01.04 AFTTP 3-2.29	Description: This publication complements established doctrine and provides a single-source reference to assist aviation and ground personnel in planning and executing tactical aviation support to urban operations. It promotes an understanding of the complexities of urban terrain, incorporating lessons learned. **Status: Current**
DYNAMIC TARGETING *Multi-Service Tactics, Techniques, and Procedures for Dynamic Targeting* **Distribution Restricted**	05 JAN 22	ATP 3-60.1 MCRP 3-31.5 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: Current**
FIGHTER INTEGRATION *Multi-Service Tactics, Techniques, and Procedures for Fighter Integration* **Classified SECRET**	15 JUN 20	MCRP 3-20.7 NTTP 3-22.6 AFTTP 3-2.89	Description: This publication is a single-source set of integration standards intended to enhance air operations involving legacy aircraft and fifth generation fighters. **Status: Revision**
JFIRE *Multi-Service Tactics, Techniques, and Procedures for the Joint Application of Firepower* **Distribution Restricted**	18 OCT19	ATP 3-09.32 MCRP 3-31.6 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: Revision**
JSEAD *Multi-Service Tactics, Techniques, and Procedures for the Suppression of Enemy Air Defenses in a Joint Environment* **Distribution Restricted**	15 DEC 15	ATP 3-01.4 MCRP 3-22.2A NTTP 3-01.42 AFTTP 3-2.28	Description: This publication contributes to Service interoperability by providing the JTF and subordinate commanders, their staffs, and SEAD operators a single reference. **Status: Revision**
KILL BOX *Multi-Service Tactics, Techniques, and Procedures for Kill Box Employment* **Distribution Restricted**	18 JUN 18	ATP 3-09.34 MCRP 3-31.4 NTTP 3-09.2.1 AFTTP 3-2.59	Description: This MTTP publication outlines multi-Service kill box planning procedures, coordination requirements, employment methods, and C2 responsibilities. **Status: Revision**
PR *Multi-Service Tactics, Techniques, and Procedures for Personnel Recovery* **Distribution Restricted**	4 JUN 18	ATP 3-50.10 MCRP 3-05.3 NTTP 3-57.6 AFTTP 3-2.90	Description: This MTTP publication for personnel recovery is a single source, descriptive, reference guide for staffs and planners executing the military option of personnel recovery using joint capabilities. **Status: Revision**
SCAR *Multi-Service Tactics, Techniques, and Procedures for Strike Coordination and Reconnaissance* **Distribution Restricted**	31 JAN 18	ATP 3-60.2 MCRP 3-20D.1 NTTP 3-03.4.3 AFTTP 3-2.72	Description: This publication provides strike coordination and reconnaissance MTTP to the military Services for conducting air interdiction against targets of opportunity. **Status: Current**

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

TITLE	DATE	PUB #	DESCRIPTION/STATUS
SURVIVAL, EVASION, AND RECOVERY *Multi-Service actics, Techniques, and Procedures for Survival, Evasion, and Recovery* **Distribution Restricted**	21 AUG 19	ATP 3-50.3 MCRP 3-05.1 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: Revision**
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 provides units and personnel working with or advising foreign security forces with viable TTP to plan, train for, and carry out advising missions at any level and in any region or theater. This MTTP provides guidance that will help to enhance the activities of some advisor functions and improve multi-Service coordination. **Status: Revision**
AIRFIELD OPENING *Multi-Service Tactics, Techniques, and Procedures for Airfield Opening* **Approved for Public Release**	27 OCT 18	ATP 3-17.2 MCRP 3-20B.1 NTTP 3-02.18 AFTTP 3-2.68	Description: This publication supports operational commanders and staffs by establishing TTP for airfield opening. 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 surveys, opening the airfield, and transitioning the airfield in all operational environments. **Status: Revision**
BIOMETRICS *Multi-Service Tactics, techniques, and Procedures for Tactical Employment of Biometrics in Support of Operations* **Distribution Restricted**	30 APR 20	ATP 2-22.85 MCRP 10-10F.1 NTTP 3-07.16 AFTTP 3-2.85	Description: This publication provides fundamental TTP for planning, integrating, and employing biometrics capabilities at the tactical level in support of operations. It also provides TTP on the integration and employment of this data in operations at the tactical level for targeting, force protection, and supporting operations throughout the intelligence cycle. **Status: Current**
CF-SOF *Multi-Service Tactics, Techniques, and Procedures for Conventional Forces and Special Operations Forces Integration, and Interoperability, and Interdependence* **Distribution Restricted**	25 JAN 22	FM 6-05 MCRP 3-30.4 NTTP 3-05.19 AFTTP 3-2.73 USSOCOM Pub 3-33	Description: This publication provides joint force operational and tactical commanders and staffs with planning guidance concerning missions, requirements, and capabilities of CF and SOF and TTP to effectively integrate operations across the competition continuum. **Status: Current**
DEFENSE SUPPORT OF CIVIL AUTHORITIES (DSCA) *Multi-Service Tactics, Techniques, and Procedures for Defense Suport of Civil Authorities* **Approved for Public Release**	11 FEB 21	ATP 3-28.1 MCRP 3-30.6 NTTP 3-57.2 AFTTP 3-2.67 CGTTP 3-57.1	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**	12 MAR 20	ATP 4-32.2 MCRP 10-10D.1 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**
FORENSICS *Multi-Service Service Tactics, Techniques, and Procedures for Expeditionary Forensics* **Distribution Restricted**	30 Oct 20	ATP 3-39.21 MCRP 10-10F.5 NTTP 3-07.8 AFTTP 3-2.7 CGTTP 3-93.10	Description: This publication ensures successful planning, integration, and employment of expeditionary forensic capabilities at the tactical level. The TTP details the six forensic functions that occur during, or in support of, tactical operations. It is designed for tactical level commanders, staffs, small unit leaders, and collectors. **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 3-35.9A NTTP 3-07.7 AFTTP 3-2.75 CGTTP 3-95.17	Description: This publication is a single-source guide to ensure effective planning and integration of multi-Service diving operations. It provides combatant command, joint force, and operational staffs a comprehensive resource for planning military diving operations, including considerations for each Service's capabilities, limitations, and employment. **Status: Revision**

LAND BRANCH–POC alsaB@us.af.mil

TITLE	DATE	PUB #	DESCRIPTION/STATUS
NONLETHAL WEAPONS (NLW) *Multi-Service Service Tactics, Techniques, and Procedures for the Tactical Employment of Nonlethal Weapons* **Distribution Restricted**	29 MAY 20	ATP 3-22.40 MCTP 10-10A NTTP 3-07.3.2 AFTTP 3-2.45 CGTTP 3-93.2	Description: This publication discusses the policy and parameters governing nonlethal weapons (NLW). This publication increases commander and subordinate awareness for nonlethal weapons planning, capabilities, and employment. **Status: Current**
OP ASSESSMENT *Multi-Service Tactics, Techniques, and Procedures for Operation Assesment* **Approved for Public Release**	07 FEB 20	ATP 5-0.3 MCRP 5-10.1 NTTP 5-01.3 AFTTP 3-2.87	Description: This publication serves as a commander and staff guide for integrating assessments into the planning and operations processes for operations conducted at any point along the range of military operations. It provides operation assessment how-to techniques and procedures which complement current joint and Service doctrine. **Status: Project Assessment**
PEACE OPS *Multi-Service Tactics, Techniques, and Procedures for Conducting Peace Operations* **Approved for Public Release**	2 MAY 19	ATP 3-07.31 MCTP 3-03B AFTTP 3-2.40	Description: This publication offers a basic understanding of joint and multinational PO, an overview of the nature and fundamentals of PO, and detailed discussion of selected military tasks associated with PO. **Status: Current** **Ownership of this MTTP and responsibility for future revisions has been transferred to the Peacekeeping and Stability Operations Institute**
TACTICAL CONVOY OPERATIONS *Multi-Service Tactics, Techniques, and Procedures for Tactical Convoy Operations* **Distribution Restricted**	26 MAR 21	ATP 4-01.45 MCRP 4-11.3H NTTP 4-01.6 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: Current**

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: Revision**
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: Revision**
BREVITY (Change 1) *Multi-Service Brevity Codes* **Approved for Public Release**	28 MAY 20	ATP 1-02.1 MCRP 3-30B.1 NTTP 6-02.1 AFTTP 3-2.5	Description: This publication defines and standardizes multi-Service brevity codes agreed upon by each U.S. Service branch. A brevity code provides no additional communications security. Brevity codes only serve to shorten transmissions. This publication does not include service-specific brevity codes nor is it synonymous with NATO APP-7. Updates to this publication have been shared with the NATO Standardization Office for inclusion or modification into Allied Communications Publications. **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 2-10A.8 NTTP 2-01.3 AFTTP 3-2.88	Description: This publications highlights key information to optimize ISR during the planning, execution, assessment phases and the PED process. This publication is useful to commanders, staff members, and new users desiring to know more about the ISR process. **Status: Revision**
TACTICAL RADIOS *Multi-Service Tactics, Techniques, and Procedures for Tactical Radios* **Distribution Restricted**	14 JUL 21	ATP 6-02.72 MCRP 3-30B.3 NTTP 6-02.2 AFTTP 3-2.18	Description: This publication is a single source, descriptive reference guide to ensure tactical level operators and planners have a comprehensive resource for planning, employing, creating, and operating radio networks (nets) in a joint Service environment. Highlighted in this MTTP are tactical radios operating in the HF, VHF, and UHF spectrums. **Status: Current**
TAGS *Multi-Service Tactics, Techniques, and Procedures for the Theater Air-Ground System* **Approved for Public Release**	21 MAY 20	ATP 3-52.2 MCRP 3-20.1 NTTP 3-56.2 AFTTP 3-2.17	Description: This publication describes how each of the Service component's systems operate within the Theater Air Ground System (TAGS) which is a conglomeration of systems. For this publication, TAGS refers to the organizations, personnel, equipment, and procedures that participate in planning and executing air-ground operations. **Status: Project Assessment**

VOTING JOINT ACTION STEERING COMMITTEE MEMBERS

BG Charles Masaracchia

Director, Mission Command Center of Excellence

Col Eric R, Quehl

Director, Policy and Standards Division, Training and Education Command

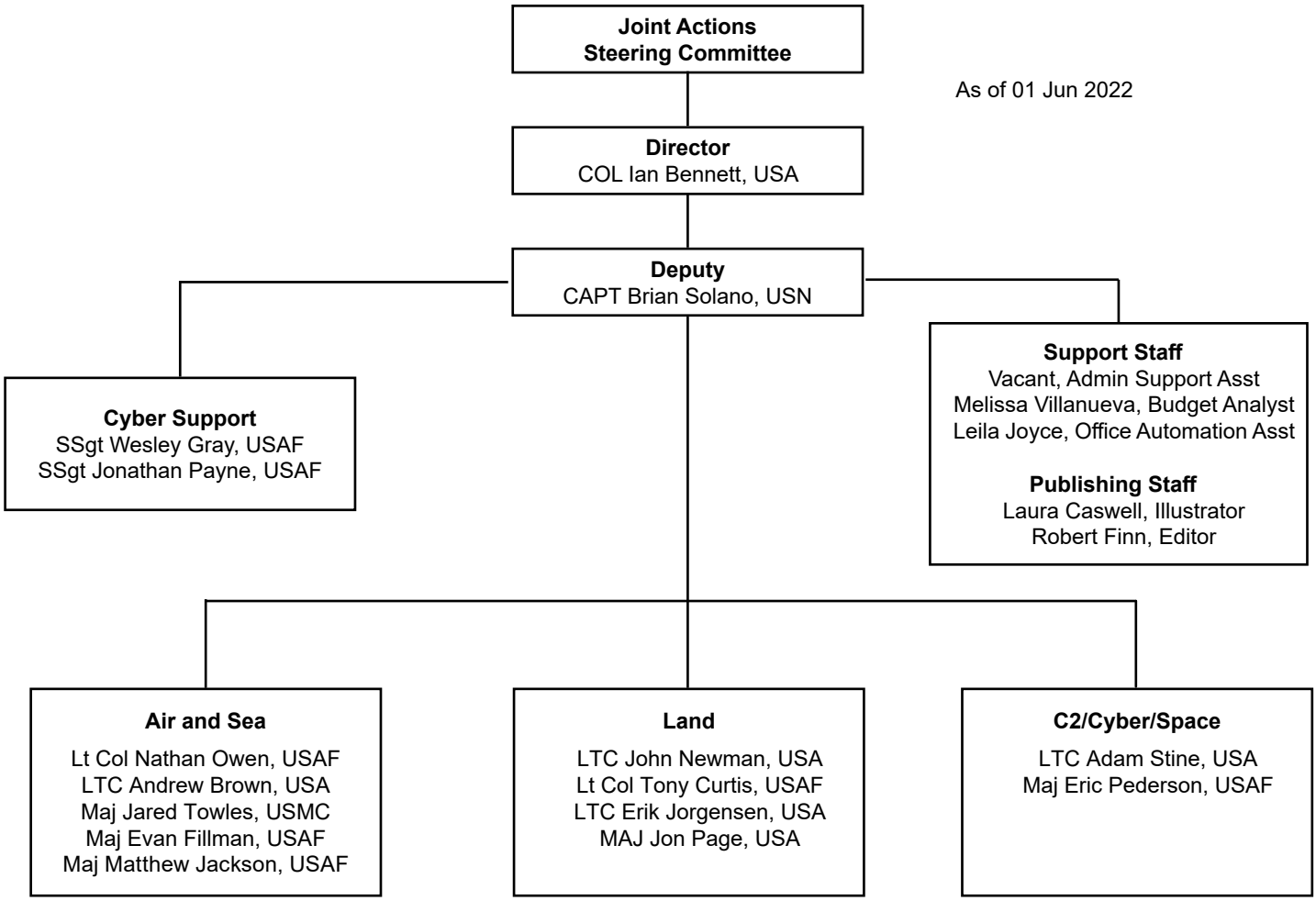
Mr. Michael R. Durkin

Executive Director, Navy Warfare Development Command

Maj Gen William Holt

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

ALSA ORGANIZATION



ALSA MISSION AND INTENT

MISSION:

ALSA synchronizes joint tactical warfighting capabilities and processes through digital/print media and professional networking to improve near-term, multi-Service interoperability.

INTENT:

ALSA is the principal DOD organization charged with synchronizing multi-Service warfighting capabilities at the tactical level. We will accomplish this through professional networking, collaborative tools, digital media and any method that allows us to engage and inform the warfighter. Adaptability, credibility, and speed are the pillars of ALSA's organizational culture. These pillars ensure we provide timely, relevant, and accessible multi-Service solutions in ways that bolster the interoperability and lethality of the Joint Force.

UPCOMING BATTLESPACE JOURNAL

Upcoming Articles (Subject to Change)

1. Tactical Interoperability Gaps in Defense Support of Civil Authorities
2. Army Aviation: No Man's Land and Peanut Butter
3. Ensuring Stability in North America and the Euro-Atlantic Region Through NATO's Warfare Development Agenda
4. Army FA Radars for C-UAS
5. Fortior Simul – Stronger Together
6. Time versus Tempo
7. The Use of the Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian War

BATTLESPACE JOURNAL SUBMISSIONS

Get published—ALSA solicits articles and readers' comments. Contributions of 3,000 -5,000 words 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. Authors are responsible for ensuring that their unclassified submissions are cleared for public release through their publication or security office. Send email submissions to alsacenter@us.af.mil. The ALSA Center reserves the right to edit content to meet space limitations and conform to the BSJ style and format.

ALSA CENTER

ATTN: BATTLESPACE JOUNRAL

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