FORENSICS
An Essential Battlefield Capability

DSCA - Reframing Homeland Defense

LEVERAGING NEW TECHNOLOGY - A Holistic Overhaul

KNOWLEDGE MANAGEMENT - People, Processes, and Tools

审批公开；不限制分发。
CONTENTS

Director’s Comments..........................................................3

FEATURE ARTICLES

Forensics in Support of Military Operations..........................4
Reframing Homeland Defense through a Defense Support of Civil Authorities Lens..............................................9
Leveraging New Technology and Creative Development will Enhance Air Defense..............................................15
Achieving Knowledge Management Interoperability across the Joint Force: The Case for KM Multi-Service Tactics, Techniques, and Procedures........................................22

IN HOUSE

Current ALSA MTTP Publications........................................26
Future Air Land Sea Bulletins...............................................29
ALSA Organization and Joint Working Groups.........................30
ALSA Mission and Voting JASC Members..............................31
Online Access to ALSA Products..........................................31

DIRECTOR’S COMMENTS

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

Several new action officers joined the ALSA organization, while others departed for new assignments.

We welcome LTC John Newman, United States Army (USA); MAJ Erik Jorgensen, USA; Lt Col Nathan Owen United States Air Force (USAF); and Lt Col William McTernan (USAF) to the multi-service team.

We say farewell to LTC Steve Padilla, and LTC Kate Oglethorpe, USA. LTC Padilla is assigned as the Field Artillery Officer on the Joint Deployable Analytics Team at Joint Staff (JS) J6 and is stationed at Eglin Air Force Base, Florida. LTC Oglethorpe is assigned to JS 26, Collection Management, and is stationed at the Defense Intelligence Agency Headquarters at Joint Base Anacostia-Bolling, Washington, DC. We wish these officers the best of luck as they face challenges in their new assignments.

The Air Land Sea Bulletin (ALSB) is one of the tools ALSA staff members use to convey innovative thoughts and ideas collected from the Services. The following articles capturing that innovation, ranging from developing a new multi-service publication to leveraging new technologies.

The first article is “Forensics in Support of Military Operations,” by Mr. Bob Cosgrove, LTC, USA, Retired. This article showcases how battlefield forensics can be a force multiplier for Service components by identifying threat networks and denying the threat’s anonymity. It is an enduring capability commanders may continue employing in multi-domain operations.

The second article is “Reframing Homeland Defense through a Defense Support of Civil Authorities Lens”, by LTC Matthew Giblin, USA. This article discusses an evolving threat to the United States along with rapidly changing technology. The author encourages Service professionals to continue adapting their thinking and finding efficient and effective ways to defeat the nation’s adversaries while operating in the gap between peace and war.

The third article, “Leveraging New Technology and Creative Development to Enhance Air Defense”, is by Maj Peter Hickman and Captain Greg Elliott, USAF, and reminds the joint force of the need to embrace new technologies to defeat the nation’s adversaries. To deliver the rapid change needed for success in the 21st century, today’s warfighters need to become more creative than potential enemies. For air defense missions, this means embracing new equipment and moving beyond institutional comfort zones.

The fourth article, “Achieving Knowledge Management (KM) Interoperability across the Joint Force: The Case for KM Multi-Service Tactics, Techniques, and Procedures (MTTP)”, is by Elaine LaMaster, Chief Master Sergeant, USAF, Retired; with contributions from the Department of Defense and Joint KM Working Group members. It describes KM as more than information technology, information management, and knowledge sharing. In simple terms, KM is focused on finding and fixing gaps or disconnects between people, processes, and tools.

We invite you to seize opportunities to represent your Service and the joint community by sharing articles to be published in future ALSBs and, also, participating in MTTP joint working groups. As we tackle the challenges ahead, your ideas matter now more than ever. Your unique perspective can spark innovation for current and future joint tactics, techniques, and procedures. To help shape the discussion and be part of the solution, go to www.alsa.mil and provide inputs through the “Contact Us” link.
The campaigns in Iraq and Afghanistan brought forensics to the forefront as an essential battlefield capability in countering irregular threat networks. The nature of how irregular threat networks organized and operated drew logical comparisons to criminal networks. Many innovative leaders recognized the similarities between irregular threats and criminal networks and began employing capabilities often used by law enforcement (such as forensics and criminal intelligence) to investigate gangs and organized crime and target irregular threat networks. Battlefield successes followed almost immediately.

US conventional and special operations units have relied upon forensics to enhance their effectiveness in identifying, understanding, characterizing, and targeting terrorist, insurgent, and transnational criminal networks. Latent fingerprint and deoxyribonucleic acid (DNA) collection and analysis enabled forces to positively identify, target, and prosecute threat actors and networks responsible for attacks against friendly forces and civilian populations. The forensic disciplines of firearms and tool marks, engineering, and chemistry enabled US personnel to have an understanding of how irregular threat networks constructed and employed improvised explosive devices (IEDs). Building forensics databases provided friendly forces and mission partners a wealth of intelligence to enable tracking equipment and materials used in constructing IEDs and other threat systems back to their countries of origin.

The outcomes enabled by forensics, in recent campaigns, have been significant. Forensic threat technologies informed the development of effective countermeasures and contributed to the development of new equipment with enhanced protection qualities. These enhanced protection qualities have reduced the effectiveness of threats attacks and reduced causalities among joint force service members. Forensic identification of threat actors has enabled improved force protection, preventing these individuals from accessing US and coalition partner forward operating bases and mitigating hostile acts. Equally important has been the joint forces’ ability to use forensic results to deny threat actors their anonymity and immunity from their crimes; critical factors irregular threats require to move in proximity to friendly forces and achieve their desired effects and outcomes.

**MILITARY PROBLEM**

While forensics directly contributed to joint forces’ successes against irregular threat networks, problems arose, nonetheless, that hindered joint forces’ from achieving forensics’ true potential on the battlefield. Though commonality in capabilities and tactics, techniques, and procedures (TTP) existed, in some instances, between Services within specific theaters of operation, the joint force lacked an overall common operational framework and TTP standardization for conducting the six forensics functions: recognize, preserve, collect, analyze, store, and share across the force.

The lack of a common framework and standardization in TTP became apparent when theater commands required one Service to provide forensic laboratory support on an area support basis for multiple Services operating within the same area of operation.

Unlike criminal investigators and other law enforcement personnel, tactical-level operators rarely received formal, institutional training on how to properly recognize, preserve, and collect materials with potential forensic value. Items of interest were sometimes overlooked by operators and, therefore, not collected for forensic analysis. Forensic technicians received collected samples that, often, were contaminated or damaged. Some
samples were destroyed, albeit inadvertently, during collection or transfer to the forensic labs. The chain-of-custody was neither properly documented (if done at all) nor maintained from the time the operators collected the items of interest to the time the forensic lab received them. Planning considerations varied from unit to unit depending on the unit’s experience, training, and available equipment needed to support forensics operations. Differences in laboratory procedures, reporting formats, and storage and sharing procedures resulted in additional challenges for forces. The absence of standardized TTP contributed to a lack of interoperability, lost opportunities, and excessive and unnecessary time delays that inhibited commanders from exploiting time-sensitive opportunities and maintaining the initiative against the threats. In extreme cases, host-nation judicial authorities freed threat actors due to discrepancies in forensics evidence presented at their criminal trials.

TAKING A TEAM-APPROACH TO SOLVING THE MILITARY PROBLEM

In response to these recurring problems and challenges, the Joint Staff initiated a Capabilities-based Assessment (CbA) to clearly identify the joint force’s requirements for expeditionary forensics. The CbA would be used to document and describe gaps across the doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy domains contributing to the problems and find solutions to address the gaps. Subject matter experts (SMEs), from the Army, Marine Corps, Navy, Air Force, and Coast Guard and the Special Operations Command (SOCOM), united for a series of workshops (over a 12-month period) to conduct the CbA.

The SMEs documented and validated 120 capability gaps during the assessment. They concluded that the joint force’s lack of doctrine on expeditionary forensics was a contributing factor to 63 of the 120 gaps. The SMEs recommended publishing an MTTP for expeditionary forensics, among the 16 nonmateriel solutions they presented to mitigate the gaps. The Joint Staff approved all the nonmateriel solutions, in April 2015, including the requirement for a Forensic MTTP.

THE FORENSIC MTTP

SMEs from across the Services and SOCOM recently converged at the ALSA Center at Joint Base Langley-Eustis to develop the Forensics MTTP. SMEs consisted of operators, intelligence analysts, law enforcement agents, explosive ordnance disposal experts, and forensic experts. After two joint working group sessions, the team of SMEs produced a draft MTTP, which recently entered the world-wide review process.

The MTTP addresses many of the doctrine gaps identified during the CbA. It provides tactical-level commanders, staffs, and operators with TTP they can employ to support a wide range of military requirements. The TTP are designed to complement, and not conflict with, either Service- or theater-specific requirements for forensics operations. Currently, the draft MTTP’s content includes:

1. An overview of forensics and the types of operations it supports, its functions, and a brief description of the forensic disciplines.
2. TTP for units to conduct on-site activities and recognize materials of forensic interest.
3. An overview of common terms, considerations for preserving and collecting materials, and post-packaging actions.
4. An overview of the analyze function at the tactical, operational, and strategic-levels.
5. TTP and considerations for storing materials and information and for sharing information.
6. An overview of forensic capabili-
As demonstrated by the US military for well over 100 years, forensics will continue to be a mission-essential capability for joint forces well into the future. The MTTP ensures US Service members employ the capabilities to their full potential in support of their information and operational requirements.

United States Army LTC (Retired) Cosgrove works at the US Army Military Police School. His article was written in collaboration with, and on behalf of, the Defense Forensics Biometrics Agency (DFBA). The DFBA carries out the Department of Defense Executive Agent responsibilities assigned to the Secretary of the Army for Forensics and Biometrics developing enterprise policies, plans, and doctrine. It represents US interests in international programs development, information sharing agreements, and standards; and participates in key interagency relationships to detect threats as far from the homeland as possible.

Unidentified troops from the 101st Airborne Division gather clues in a mock torture chamber during the Forensic Material Collection and Exploitation Course at Fort Campbell, Kentucky March 11, 2010. (Photo by Specialist Richard Daniels, Jr. USA)

The problem DOD faces is, the threat to the homeland has changed drastically over the years and the military cannot address it alone.

By LTC Matthew Giblin, USA

It is past time for the Department of Defense (DOD) to rethink the HD mission. The military must adopt the same civilian partnership mentality that has succeeded for DSCA missions to detect and defeat the nation’s adversaries in all domains. The homeland is held at great risk by unconventional threats capable of a strategic impact. Mercenary forces, cyber warriors, space assets, and multiple advanced technologies threaten American freedoms and foundational values. The problem DOD faces is, the threat to the homeland has changed drastically over the years and the military cannot address it alone.

The United States (US) must address the current threat with all instruments of power and push the “whole of nation” response from a buzzword to an operationalized and practiced concept complete with all the authorities, plans, and budget necessary to ensure the HD mission is efficient and effective. The same approach and framework that proves effective for the military response to catastrophic disasters serves as a model to address the evolving threat to the homeland.

The most operationalized version of a whole-of-nation effort, involving DOD, is through the DSCA mission. Through the past years of waning risk of conventional conflict, DOD has proven its multifunctional capacity by supporting civil authorities in the homeland. Any local community, state, tribe, or territory in the US, that under-
The US military has gained a comfort level with the DSCA mission set and has increased key skills within the homeland that are vital to HD success. Partnering with civilians to accomplish objectives, with a sense of unity, is not an easy task. DOD has learned a lot about working with, and through, civilian organizations. That has key implications for addressing the current threat to the homeland.

The following are key lessons from DSCA that apply to HD.

1. DOD may not be in charge. When a catastrophic disaster strikes the US, there are clear authorities and established assistance request channels to direct DSCA. There is no obvious trigger to call out the military during a masked attack on the homeland, such as a cyberattack. An attack on the homeland that remains below the level of armed conflict, yet still is a risk to US sovereignty and fundamentals, is not as clear.

   Many of the advanced threats to the nation do not elicit a military response. The line between peace and war is blurred, and incursions of US sovereignty are ubiquitous. Further complicating a military response, is the fact that most of the advanced technology that makes intrusions possible are owned by private sector agencies.

   Several legal and authority restrictions, within the homeland, limit the potential of many DOD capabilities to deter attacks. In many cases, much like DSCA operations, the military will not be in charge. If the threat to the homeland is not a clear danger, DOD may need to take a backseat while providing much needed capabilities and support. It behooves DOD, civilian agencies, and the private sector to recognize they need each other to identify, track, confront, and deter shadow enemies operating in the homeland. Also, much like DSCA, they must meet and plan their responses regularly.

   If military personnel wait for a national emergency declaration to trigger DOD, it is possible to wait past the point of defeat. In a sense, the US will have lost the next war before recognizing it was a war. Conflict is a constant, with periods of calm and intensity. War does not occur at an established place and time and the actors do not operate within established rules of engagement that set aside civilians. Financial systems, water systems, transportation, electricity, satellites, networks, people, and fundamental values are all at risk. How does DOD defend the homeland when the enemy is not onshore, not firing missiles, and not threatening US physical sovereignty?

   This DOD dilemma was highlighted in a recent exchange between the late Senator John McCain, former Senate Armed Services Committee Chairman; and Mr. Kenneth Rapuano, the Assistant Secretary of Defense for Homeland Defense and Global Security. Mr. Rapuano testified to caution Congress of DOD’s role in cyber stating, “[T]he United States has a long normative and legal tradition limiting the role of the military in domestic affairs. This strict separation of the civilian and the military is one of the hallmarks of our democracy and was established to protect its institutions. Designating DOD as the lead for the domestic cyber mission risks upsetting this traditional civil-military balance.”

   The late Senator McCain responded, “For you to sit there and say, ‘Well, but it’s not [the] Department of Defense’s responsibility’—it is; to defend the nation … if you can change the outcome of an election, that has consequences far more serious than a physical attack. I am in fundamental disagreement with you about requirements of the Department of Defense to defend the fundamentals of this nation, which is to defend a free and fair election, [of] which we all know the Russians tried to affect the outcome. … it’s the Department of Defense’s job to defend this nation; that’s why it’s called the Department of Defense.”

   This conversation highlights the changing nature of the threat to the homeland and DOD dilemma. It highlights the historic, limited authority of the military in the homeland. The obvious remedy is to leave civilians in charge while employing critical DOD capabilities.

2. A dual mission for the military, homeland and DOD dilemma. This conversation highlights the changing nature of the threat to the homeland and DOD dilemma. It highlights the historic, limited authority of the military in the homeland. The obvious remedy is to leave civilians in charge while employing critical DOD capabilities.

   The same efficiencies could be made in the HD missions addressing advanced threats. If DOD builds readiness against the clear and present, evolving threat, it does not matter if it is within US boundaries or on foreign soil. Readiness for the threat is readiness for the threat regardless of where it appears. Mercenary forces, terrorist plots, cyber hacks, unmanned-platform form attacks, biological attacks, and all other forms of advanced threat will occur in the homeland and in the overseas war fight.

   If there is anything America’s enemies can take away from the last three decades of conflict, it is this:... separation of the civilian and the military is one of the hallmarks of our democracy and was established to protect its institutions.
challenging the US through an American war of way is not a good option. Challenging the US through drawn-out insurgency, proxy forces, information warfare, and shadowy domains is a much easier path to defeating the US. DOD’s number one priority is readiness. The question the US must ponder is: ready for what?

The US has a perfect record of being wrong when guessing what warfare will look like in the next war. While building advanced, conventional threats to meet what might be the next war, the homeland is at risk. There is a good probability that the threats that hold the homeland at risk today are the same threats that hold our military at risk in the next war. Additionally, working through partnering and networking skills to address the future threat were skills needed in the last war, and will most certainly be needed in the next war. While the US spends exorbitant amounts of money in building traditional military readiness, the rest of the world is taking the easier, and less risky, path short of armed conflict. The defense budget continues to soar while the record of military lasciviousness continues to rise. America’s overseas conflicts and homeland threats must be addressed with a DSCA-like framework that works toward increased security, not increased instability. The same is necessary for the traditional war.

General Anthony Zinni (United States Marine Corps, Ret), a DOD senior leader who led through the transition from the clear-cut Cold War threat to the current age of globalization, said: “What do we do in Government? Well, we have another level of bloated bureaucracy.” The threat to the homeland changed, so we added a new department; the DHS. The threat overseas changed, so we added the State Department’s Office of the Coordinator for Reconstruction and Stabilization, interagency coordination groups, civil-military operations centers, and interagency staff sections (J9s). These organizations are attempts to address the problem but they all have no bill payer and, therefore, are grossly underfunded.

For DSCA operations, civilian agencies identified gaps and looked to an existing organization to fill them, while gaining a training benefit. Congress approved a Fiscal Year 2019 defense budget of 716 billion dollars, and the primary mission of the DOD is defense of the homeland. Despite, the US having the DHS to combat risks to the homeland, the homeland is still at risk. How is that possible? Within the homeland, the separation of the DOD and DHS missions leads to potential misunderstandings, capability gaps, and unsynchronized execution; especially, since the two are responsible for the same space and the threat operates in the space between the two organizations’ responsibilities. It appears to be much like the security situation in Iraq that begged the questions: Is that nefarious actor a criminal or a combatant? Is homeland security responsible for that threat to the homeland or is DOD?

DOD doctrine for HD has changed along with the changing security environment; however, there is room for growth. DOD no longer considers HD something that occurs only within the nation’s borders. The doctrine of “active, layered defense” means DOD will deter and defeat aggression toward the US overseas as well as within the homeland. DOD is moving in the right direction with homeland defense doctrine but there is one more important step to deal with: that is the current risk to the homeland. DOD must develop agreements and a framework, much like those that exist with DSCA, to ensure civilian partners are armed with the tools, intelligence, and plans to keep the homeland safe.

A DSCA concept has the dual-status commander and federal coordinating officer serving as facilitators between federal and state authorities. A similar concept may be in order for threats to the homeland. The military Services, and each of their components, continue to grow force structure and capabilities to meet the technological threats to the homeland (such as a space force, cyber teams, and artificial intelligence research). Now the US Government must ensure these capabilities have the partnerships, authorities, plans, and supporting exercises to make certain the capabilities are able to react to threats within the homeland. Defense of the homeland is no longer about just a physical boundary that will trigger a military HD response. The current threat does not have to cross a border or overcome a barrier. The threat may be a nation state, a proxy of a nation, or independent actors. The threat is here in the homeland, among the population, and within networks; and it sometimes has anonymity. This is the new point of entry for the enemies of this nation and they do not cross the threshold of armed conflict. In a September 2018 speech, the Secretary of Homeland Security Kirstjen Nielsen, stated, “the pace of innovation, our hyperconnected-ness, and our digital dependence have opened cracks in our defenses, creating new opportunities and new vectors through which these nefarious actors can strike us.” These actors are not conventional military forces and the threat is here in the homeland, among the population, and within networks; and it sometimes has anonymity.
cracks that exist within private sector, state, territory, and local government-owned infrastructure.

In today’s security environment, leaders (from the President to the most senior DOD leadership) are refocusing the Armed Forces on the priority of HD. However, the current threat cannot be addressed with military forces alone, solely focused on HD. DOD defines HD as “the protection of US sovereignty, territorial, domestic population, and critical infrastructure against external threats and aggression or other threats, as directed by the President of the United States”. There is a lot of room, in this definition, to broaden the DOD horizon. However, additional military technology, additional organizational layers, and inflated military budgets will not address all that is involved in HD, given the widespread threat. The HD definition must include civilian agencies and the private sector as foundational elements, much like DSCA. For DSCA, the US has developed the National Response Framework as a strategy to coordinate a holistic response. During DSCA operations, civilian leaders at the local, state, and tribal levels leverage unique DOD capabilities, the civilian workforce, and the private sector to minimize loss of life and prevent suffering after a disaster. This synchronization is exercised and executed in real-world disasters regularly. The nation must have a similar strategy for the homeland, which should include a smart mixture of military and civilian authorities and capabilities.

The three DSCA lessons identified herein are a start to building an HD strategy that addresses the entirety of the evolving threat. Prioritizing HD appears to be a binary choice over DSCA. However, in today’s security environment, this is not a choice, but a blend of the two missions. The lessons DOD has learned from DSCA apply to the homeland, address the threat gaps, and concurrently train for the overseas threat. The alternative is to continue to build organizations to address all the new threats, while the DOD holds on, dearly and aimlessly, to the next major force-on-force war within the confines of the American way of warfare. The DSCA framework offers the efficiency and effectiveness that embodies a whole-of-nation effort and provides the capacity to confront America’s enemies in all domains.

**END NOTES**


4. “Written Testimony of DHS Secretary Kirstjen Nielsen for a Senate Committee on Homeland Security and Governmental Affairs Hearing Titled ‘Threats to the Homeland,’” 2018. (Photo by Capt Kimberly Burke, USAF)


6. LTC Matt Giblin is a National Guard officer serving as a joint planner at the North American Aerospace Defense Command and United States Northern Command. His primary responsibilities are DSCA strategy, doctrine, and policy.

**LEVERAGING NEW TECHNOLOGY AND CREATIVE DEVELOPMENT WILL ENHANCE AIR DEFENSE**

By Maj Peter Hickman (USAF) and Capt Greg Elliott (USAF)

“Our ability to command and control air and space forces will be affected by three major, interrelated trends: emerging threats, new technologies, and the velocity of information.”

Air Force Lt Gen (ret) David Deptula.

To provide a credible deterrent against potential adversaries, the United States (US) needs “simultaneous offensive and defensive capabilities.”

Emerging unmanned aircraft systems (UASs), advanced cruise missiles, and hypersonic weapons threaten the United States Air Force’s (USAF’s) approaches to air defense. This shift presents a challenge that requires a transformation in the way the USAF warfighters execute air defense and, as threat systems increasingly leverage technological innovations to become faster, smaller, and harder to detect, USAF warfighters also must embrace technological innovations to assist in the ability to find, fix, track, target, engage, and assess (F2T2EA) threats. In addition, the challenges the US faces take place in the context of needing to do more with less where sudden attacks (that can quickly overwhelm steady-state and alert force postures or attacks in overseas operating environments, on adversaries’ doorsteps) can create force generation and sustainment issues.

US warfighters should not be content to rely on retaliation as the best defense and continuously tempt an adversary’s first strike. To provide a credible defense, the USAF needs to undertake a holistic overhaul of the way it thinks about air defense. Advanced sensor fusion, artificial intelligence (AI), and cooperative tracking...
form the main pillars of rethinking. There are no longer decades to bring about change and, therefore, the US requires the kind of creative capability development that is available, should USAF warfighters have the courage and motivation to use it.

Threat trends challenge the relevance of existing approaches to air defense in North America and overseas. Small UASs, advanced cruise missiles, and hypersonic weapons are being proliferated, fielded, or tested by potential adversaries. In the case of UASs, potential adversaries include nonstate actors. Physically small targets with small radar cross sections (RCSs) challenge sensors and fast targets challenge existing response postures and weapon systems. These are some developments which have outpaced defensive capabilities and, currently, retaliation is the best deterrent against many of these threats. This reactive posture results in vulnerability to first strikes from these weapons, the consequences of which the US may not be postured to absorb or able to accept, regardless of the retaliatory damage US warfighters may inflict on the adversary. The consequence for air defense is that the US is facing a rapidly changing battlespace and rapid change will be required from existing air defense approaches to maintain relevance in the near future, and form part of a reliable military deterrent to prevent attacks.

Throughout the years immediately after 9/11, air defense of North America has remained focused on manned threats. Existing radar networks and alert aircraft were sufficient to provide a credible defense against manned aircraft. Today, threats from manned aviation are being surpassed by unmanned systems and weapons that render existing defenses insufficient.

Commercial UAS proliferation has resulted in a wide array of available systems that can be used to attack US interests at home and abroad. The potential implications of UASs for attacks have been illustrated by an operator landing a small system near utility German Chancellor Angela Merkel in 2013 and attacks disrupted by US intelligence agencies in 2011 and 2015. Also, an operator landed a UAS on the roof of the Prime Minister of Japan, Shinzo Abe, that was “marked with radioactive symbols, carried a plastic bottle with unidentifiable contents, and registered trace levels of radiation.” The current North American Aerospace Defense Command Commander, General (Gen) Terrence J. O’Shaughnessy, recently updated guidance to prioritize this problem set. His assessment is that it is “likely only a matter of time before UASs will be used for nefarious purposes in the homeland.”

Another concern is that Russia has fielded advances in air-launched cruise missiles with considerably more standoff range and are, reportedly, more accurate and difficult for radars to detect than their past weapons. Capable of carrying conventional and nuclear payloads, these new cruise missiles have ranges over 1,000 miles, and are capable of low-altitude flight profiles, making them difficult for ground-based radar networks to detect and track. Starting in 2015, Russia employed dozens of conventional versions of these advanced cruise missiles in Syria (from standoff distances greater than 1,000 miles).10

Hypersonic weapons are being tested by Russia and China11 with the possibility both countries may field weapons that can achieve speeds of Mach 5 (about 4,000 miles per hour) prior to comparable US development. At hypersonic speeds, aircraft could fly from Beijing to New York in two hours. Chinese researchers have already completed wind tunnel tests of vehicles up to Mach 7 (5,600 miles per hour).

The significance of these threats has not escaped the attention of those tasked with air defense, yet, the threats have been considered isolated from each other. A holistic way ahead for air defense against fast, small, attributable unmanned systems is not central to the short-term problem. The implication of the communications shortcoming must change to catch up to threats already available to adversaries. The USAF is exploring the future of battle management through the Advanced Battle Management System Analysis of Alternatives (AoA), however, a holistic vision is needed for the future of air defense. Thus far, work remains stove-piped to independent efforts to address specific threat categories.

Cooperative Engagement Capability (CEC) is a real-time sensor netting system that enables high quality situational awareness and integrated fire control capability, for a superior air picture and may hold the key to the future of enhanced air defense. One reason the USAF has not embraced approaches like CEC are based in a historical inability of battle management platforms to produce weapons-quality data. Innovations, however, have resulted in emerging sensors that can support weapons-quality track updates feeding battle management platforms. Though airborne platforms have update rate challenges, the Advanced Battle Management System (ABMS) AoA suggests next-generation platforms will present improved sensors and update rates over those of today. Nonetheless, the air defense mission cannot wait for long-term solutions to address current and emerging threats.

To get ahead of these threats, shortcomings must be addressed in three components of air defense systems. First, sensors must continue to be incorporated that can detect and track emerging threats. Second, innovations in algorithmic approaches to data analysis should be incorporated to assist operators in processing vast amounts of information and help find the proverbial “needle in a haystack.” Third, cooperative tracking should be embraced by digital sharing weapons-quality information developed by off-board platforms. All of these in

Marines with 2nd Low Altitude Air Defense Battalion Counter-Unmanned Aerial Systems Detachment test the Marine Air Defense Integrated System (MADIS). The MADIS is the first vehicle to use kinetic and nonkinetic measures to disable counter-unmanned aircraft systems. (Photo by Lance Cpl Jack C. Howell, USMC)
In North America thousands of aircraft fly daily, any of them could be a threat, but almost none of actually are. While surveillance techni-
cians spend the majority of their time evaluating routine traffic, they have less bandwidth for the difficult work of detecting and assessing true threat profiles, if existing sensors provide limit-
it conditions. Low RCS threats fol-
lowing terrain at low altitudes are dif-
ficult to detect and require focus and 
time. These kinds of detections have 
little likelihood of occurring because 
the routine workload of the surveil-
lance technicians is devoted to sorting 
through hundreds of routine tracks.

To address the needle in a hay-
stack problem, new software tools 
should be leveraged to enable more ef-
fective detection and tracking.

Where large amounts of data 
constitute a problem for human ana-
lysts, big data provides an opportunity 
for machines. One of the keys to AI 
access to significant amounts of data to 
enable learning.16 A variety of systems 
provide an enormous amount of data 
from the airspace over North America. 
These data sources include the feeds 
from civilian and military radars and 
other sensors, aircraft self-reporting 
systems and interrogation response 
codes. Additional airspace monitoring 
facilities (such as the Air Marine Op-
erations Center and Customs and Bor-
der Patrol) provide data feeds, and a 
host of other agencies, flight services, 
weather feeds, and flight data track-
ers provide additional data. Potential-
ally overwhelming to human operators, 
this data enables machines to create 
an understanding of normal patterns of 
life (POL) and detect and report signif-
ificant deviations from POL. The POL 
capability compiles weeks, months, 
and years of data to determine common 
flight paths, flight profiles, work pat-
terns and timing, and departures and 
arrivals to build and maintain a POL.

The days of relying, solely, on 
steadily spinning, ground-based radar 
dishes are being rendered obsolete by 
small, low, fast targets.

Instead of relying on spinning 
radars, the USAF should follow the 
lead of the US Navy and pursue fused 
data from a network of sensors capable 
of providing detection and tracking 
gaps. A simple detection ability (by 
one or more sensors) in a coverage 
volume, does not close the detection 
and tracking gaps. With big data (gen-
erated by small, low, and slow targets) 
comes big analysis challenges. Conse-
quently, though the needle remains 
the same size, the haystack grows.

The 7th Space Warning Squadron has an enhanced, upgraded early warning radar system with a great capability to detect and track missile 
attacks against the United States and its allies, at Beale Air Force Base, California. This improved system is expected to be fully operational by 
the end of 2019. (Photo by Cameron Hunt, USAF)
This enables coordinated engagement, avoids duplicative engagements, and offers the possibility of a digitally optimized response to attacks.

Though there are several important reasons the USAF remains some time away from integrating with Navy CEC, there are near-term opportunities to remove existing data storepipes to share available weapons-quality information among ground- and air-based platforms that can produce and use it. Several fielded or fielding sensor systems can produce weapons-quality data, and the ability to share it digitally requires little more than minor software and existing data link modifications.

Finally, the US cannot rely, solely, on the glacially-paced acquisition approaches of the past or hope to afford many of the price tags attached to procurements. However, this is a time senior leaders are encouraging the Services to find ways to move fast, innovate, and take responsible risks.

Some of the innovations of CEC are an “intelligent averaging” of radar data—weighting each data point according to the accuracy of the radar, which effectively creates a shared tactical picture that is greater than the sum of its parts. This allows other platforms to provide precise cueing to enable radar acquisition, at the limits of its radar range, and enable engagement against targets a shooter does not hold with organic radar. This provides distinct advantages against low RCS targets, especially those that present varying RCSs, depending on the angle of illumination. While being painted by different radars at different angles, a cooperative track can be produced at higher fidelities than any is capable by any radar given target location relative to transmitter. The result is “a dramatic improvement in the ability of US Navy ships and aircraft to defend the battlefield against difficult air threats by maximizing the effectiveness of existing sensors and weapons, i.e., sensor networking with integrated fire control.” CEC provides additional decision space to commanders due to increased engagement options. Sensor networking builds to an integrated fire-control capability that pairs the usability of various platforms to contribute to a cooperative fire-control air picture, then shares engagement information among the various participants.

This enables coordinated engagement, avoids duplicative engagements, and offers the possibility of a digitally optimized response to attacks.

Maj Peter Hickman is a National Guard officer serving as the Chief, Homeland Defense Branch, Command and Control Requirements Division, at Air Combat Command Headquarters. He leads modernization and sustainment efforts for Homeland Defense programs.

Capt Greg Elliott is Chief, Weapons and Tactics, 224th Air Defense Squadron, serving as the principle advisor to the Commanders, Eastern Air Defense Sector and 224th Air Defense Group on tactics, integration, and mission planning for the air defense of the homeland.

END NOTES

1 As cited in Sizikov, Ian, and Hazen, Ben, Global Command and Control for the Future Operating Concept, Air & Space Power Journal, (Winter 2017), 73.
9 Grant, Conrad J., CEC Sensor Netting with Integrated Fire Control, Johns Hopkins APL, Technical Digest, Volume 23, Numbers 2 and 3 (2002), 149
10 Grant, Conrad J., CEC Sensor Netting with Integrated Fire Control, Johns Hopkins APL, Technical Digest, Volume 23, Numbers 2 and 3 (2002), 152
9 Grant, Conrad J., CEC Sensor Netting with Integrated Fire Control, Johns Hopkins APL, Technical Digest, Volume 23, Numbers 2 and 3 (2002), 149
10 Grant, Conrad J., CEC Sensor Netting with Integrated Fire Control, Johns Hopkins APL, Technical Digest, Volume 23, Numbers 2 and 3 (2002), 152
ACHIEVING KNOWLEDGE MANAGEMENT (KM) INTEROPERABILITY ACROSS THE JOINT FORCE: THE CASE FOR KM MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES (MTTP)

By Elaine Lamaster (Chief Master Sergeant, USAF, Retired)

Chances are, those who have been in the military for more than a few years have heard of KM. KM resides at all levels of command, though it is usually more prevalent at the operational level. At a combatant command (CCMD), the KM office usually reports directly to the chief of staff, because the chief of staff owns the battle rhythm. However, in the last few years, KM has started to inundate tactical operations. This is because KM is focused on finding and fixing the gaps or disconnects between three entities: people, processes, and tools. Once the disconnects are addressed, the information and knowledge flow seamlessly in an organization, thus enabling mission success.

PEOPLE
KM is mission focused and commander centric. It is a resource to assist the chief of staff in establishing and maintaining effective, repeatable staff processes to improve knowledge flow within the unit and execute the mission. When joint staffs use collaboration computer tools, such as SharePoint, the goal is to facilitate collective understanding. The critical tasks are centered on how to elicit ideas from all members, even those on the sides at all levels of command, though it is usually more prevalent at the operational level. At a combatant command (CCMD), the KM office usually reports directly to the chief of staff, because the chief of staff owns the battle rhythm. However, in the last few years, KM has started to inundate tactical operations. This is because KM is focused on finding and fixing the gaps or disconnects between three entities: people, processes, and tools. Once the disconnects are addressed, the information and knowledge flow seamlessly in an organization, thus enabling mission success.

In simple terms, KM is about getting the right knowledge to the right person at the right time for the right effect (or decision). When KM was instituted in CCMDs and provided effective processes, it improved the decision-cycle and, ultimately, enhanced mission and organization performance at units. Personnel were using clearly documented processes that could be measured and enforced to enable efficient and effective work accomplishment. Battle rhythm mapping and decision support systems proved invaluable as they provided critical information to leadership. Moreover, implementation of business modeling reflected leadership guidance and management techniques.

An organization’s leaders who wish to cope dynamically with the changing operational environment need to create information and knowledge while meeting operational challenges, not merely process information and knowledge. The KM cell enables this creation by improving knowledge flow for organizational learning and effective decision making, but this does not mean the KM cell owns or manages all the KM processes. For example, the chief of staff owns the battle rhythm. KM assists the process owners in achieving and maintaining effective information and knowledge exchange processes by helping the chief of staff find and fix the gaps and disconnects among people, processes, and technology. This keeps the knowledge flowing in the organization and enables cross-functional integration for achieving a shared understanding, the commander’s decision-cycle support, organizational learning, and performance.

TOOLS
The final aspect of KM is incorporating automated and collaborative tools. An example of this can be a stop-light chart which, through visualization, quickly and efficiently displays the status of a certain project posted on SharePoint. The goal is an integrated and evolved set of user friendly, multi-purpose, collaborative tools that leverage authoritative, filterable data.

JOINT TERMINOLOGY AND EXISTING DOCTRINE
Often, KM is confused with information technology (IT) and information management (IM) because they are codified and known, but KM is broader than discrete technology and data. KM integrates concepts from a variety of research areas (i.e., information science and epistemology, communication science, computer science and technology, social science, behavioral science, management science). According to joint publication (JP) 3-0, Joint Operations, interoperability is “the ability to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives”. It is achieved through human, procedural, and technical means based upon the mission partner’s level of interoperability. Consequently, there is no single, agreed-upon definition of KM. It also integrates with several management disciplines, such as IM, data management, process management, performance management, learning management, and business intelligence. In many cases, the definition depends upon the strategic objectives of the organization employing it. Most agree, KM centers on selecting and applying knowledge from functional integration for achieving a shared understanding, the commander’s decision-cycle support, organizational learning, and performance.

Figure 1. KM core services empower the workforce to use collaborative tools and methods to efficiently and effectively execute processes that enable decision making. This figure shows the core services associated with each of the three components of KM.
If US military forces are to train as they fight, they need to train to one standard within an established joint task force (JTF) KM capability.

After-action reviews from the Air Force’s Fight and Recover the Base, Adaptive Basing Initiatives, and the Operational Data (OD) Quick Turn Capabilities Based Assessment (QTCBA) Report detail failures in KM doctrine among the joint force and mission partners. The recommendations specify a need for doctrine to codify a holistic approach to data, knowledge, records, and IT management. The prevailing recommendation of the Department of Defense (DOD) and the joint KM community is that knowledge is the output of all these efforts, but sustained performance and integration come from KM. These are achieved through human, procedural, and technical means based upon the mission partner’s level of interoperability. KM, as a command and control capability, seeks to integrate strategic-to-tactical-level knowledge gaps and solutions ensuring effective decision support to the commander and enabling globally-integrated operations that deliver competitive advantages in “the great power competition.”

Over the course of two DOD-wide KM events in November 2017 and May 2018, it was clear Service and CCMD KM efforts have been hindered, in their support of global integration, by a lack of uniformity and varying degrees of command support and staffing to implement critical KM efforts. KM, as a discipline, is applied, defined, and structured differently throughout all levels and components of the DOD. Each branch of Service has applied KM, data, records, and IT management in a manner that suits the individual Service’s needs. If US military forces are to train as they fight, they need to train to one standard within an established joint task force (JTF) KM capability. This begins in phases zero and one with planning, training, forming, and organizing.

Current joint doctrine and policy are insufficient to address KM tactics, techniques, and procedures (TTP) in standing up and operating a combined JTF and its Service component headquarters down to the tactical level. Developing and implementing a KM MTTP will enable improved performance so planning, force management, and decision making are made “at the speed of relevance” in an uncertain, complex, global environment. Annex I (Knowledge and Information Management) to the Chairman of the Joint Chiefs of Staff manual 3130.03A, Planning and Execution Planning Formats and Guidance; the Mission Partner Environment Joining Membership and Existing Instruction; and the Joint Staff (J7) Insights and Best Practices Focus Paper for KM and IM do not provide a sufficient level of detail for standardizing KM TTP across the Services and JTF. For example, the TTP are not detailed enough for establishing effective, repeatable battle rhythms, IM, and a commander’s decision cycle processes. Also, they do not provide methodology, tools, and procedures for measuring KM capability maturity, designing/implementing solutions, or facilitating change management/culture changes. They do not identify KM principles, competencies, training, and knowledge services for standardizing and optimizing decision support to the commander. As a result, after-action reports, lessons learned, and operational assessments continue to cite longstanding KM deficiencies which mean the Services need to change to stay competitive in the global operations environment. A KM MTTP will help do this by providing the Services a common lexicon and set of processes/techniques to improve joint interoperability down through the tactical level.

Ms. LaMaster is a retired Air Force Chief Master Sergeant with thirty-nine years of combined military and civil service. She serves as a program analyst at Air Combat Command, Joint Base Langley-Eustis, Virginia. Her focus is on Air Operations Center Weapon Systems, Air Force forces, and Unit Command and Control KM requirements, capability development, and delivery.

END NOTES

1 Army KM Interoperability Information Paper, 11 January 2019
CURRENT ALSA MTTP PUBLICATIONS

<table>
<thead>
<tr>
<th>TITLE</th>
<th>DATE</th>
<th>PUB #</th>
<th>DESCRIPTION/STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFTTP 3-2.15</td>
<td>14 MAR 19</td>
<td>ATP 03-11.15 MCRP 10-10B NTP 3-01.08 AFTTP 3-2.31</td>
<td>Description: This publication provides joint planners with a single-source set of multi-service tactics, techniques, and procedures to include integration procedures. Status: Current</td>
</tr>
<tr>
<td>AFTTP 3-2.3</td>
<td>15 FEB 16</td>
<td>MCRP 3-2.05 NTP 3-30.08 AFTTP 3-2.37</td>
<td>Description: This publication consolidates Service doctrine, tactics, and procedures to include current operations and exercises to maximize the effectiveness of air attacks on enemy surface vessel. Status: Revision</td>
</tr>
<tr>
<td>AFTTP 3-2.06</td>
<td>27 APR 16</td>
<td>MCRP 3-30.3A NTP 3-01.04 AFTTP 3-2.32</td>
<td>Description: This publication provides MTTP for tactical-level planning and execution of fixed- and rotary-wing aviation employment. Status: Revision</td>
</tr>
<tr>
<td>AFTTP 3-2.60</td>
<td>10 SEP 15</td>
<td>MCRP 3-18.6A NTP 3-39.01 AFTTP 3-2.26</td>
<td>Description: This publication provides the JFC, operational staff, and components MTTP to coordinate, de-conflict, synchronize, and prosecute direct fires in any AOR. It includes lessons learned, and multinational and other government agency considerations. Status: Revision</td>
</tr>
<tr>
<td>AFTTP 3-2.61</td>
<td>16 JAN 17</td>
<td>MCRP 3-27.0 NTP 3-39.01 AFTTP 3-2.89</td>
<td>Description: This publication provides JFC, operational staff, and components MTTP to coordinate, de-conflict, synchronize, and prosecute direct fires in any AOR. It includes lessons learned, and multinational and other government agency considerations. Status: Revision</td>
</tr>
<tr>
<td>AFTTP 3-2.62</td>
<td>15 DEC 15</td>
<td>MCRP 3-22.2A NTP 3-39.02 AFTTP 3-2.26</td>
<td>Description: This publication contributes to Service interoperability by providing the JTF and subordinate commanders, the Service departments and SEAD operators a single reference. Status: Revision</td>
</tr>
<tr>
<td>AFTTP 3-2.63</td>
<td>18 JUN 18</td>
<td>MCRP 3-31.01 NTP 3-39.02 AFTTP 3-2.26</td>
<td>Description: This MTTP publication outlines multi-service kill box planning procedures, coordination requirements, employing tactics, and CO responsibility. Status: Current</td>
</tr>
<tr>
<td>AFTTP 3-2.64</td>
<td>4 JUN 18</td>
<td>MCRP 3-30.3 NTP 3-37.06 AFTTP 3-2.26</td>
<td>Description: This MTTP publication provides joint planners with a single-source set of multi-service tactics, techniques, and procedures to include integration procedures. Status: Current</td>
</tr>
<tr>
<td>AFTTP 3-2.65</td>
<td>31 JAN 18</td>
<td>MCRP 3-26.0 NTP 3-33.43 AFTTP 3-2.27</td>
<td>Description: This publication provides joint planners with a single-source set of multi-service tactics, techniques, and procedures to include integration procedures. Status: Current</td>
</tr>
<tr>
<td>AFTTP 3-2.66</td>
<td>11 SEP 12</td>
<td>MCRP 3-30.03 NTP 3-33.43 AFTTP 3-2.26</td>
<td>Description: This is a weather-proof, pocket-sized, quick reference handbook to include information needed to assist multi-service coummand and staff with information needed to assist Service members in a survival situation regardless of geographic location. Status: Revision</td>
</tr>
<tr>
<td>AFTTP 3-2.67</td>
<td>22 JAN 15</td>
<td>MCRP 3-42.1A NTP 3-35.14 AFTTP 3-2.64</td>
<td>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</td>
</tr>
</tbody>
</table>

LAND BRANCH – POC alsA@us.af.mil

<table>
<thead>
<tr>
<th>TITLE</th>
<th>DATE</th>
<th>PUB #</th>
<th>DESCRIPTION/STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADVISING Multi-Service Tactics, Techniques, and Procedures for Advising Foreign Forces Distribution Restricted</td>
<td>13 NOV 17</td>
<td>ATP 03-10.10 MCRP 3-33.8A NTP 3-07.05 AFTTP 3-2.76</td>
<td>Description: This publication discusses how advising fits into security assistance/security cooperation and provides definitions for specific terms as well as listing examples to facilitate the advising process. Status: Current</td>
</tr>
<tr>
<td>AIRFIELD OPENING Multi-Service Tactics, Techniques, and Procedures for Airfield Opening Approved for Public Release</td>
<td>27 OCT 18</td>
<td>ATP 03-17.2 MCRP 3-20.01 NTP 3-02.18 AFTTP 3-2.68</td>
<td>Description: This publication provides guidance for operational commanders and staffs on opening and transitioning an airfield. It contains information on service capabilities, planning considerations, airfield assessment, and establishing operations in all operational environments. Status: Current</td>
</tr>
<tr>
<td>BIOMETRICS Multi-Service Tactics, Techniques, and Procedures for Tactical Employment of Biometrics in Support of Operations Approved for Public Release</td>
<td>6 MAY 16</td>
<td>MCRP 3-37.16 NTP 3-05.16 AFTTP 3-2.65 CGTTP 3-06.36</td>
<td>Description: This is a comprehensive reference for commanders and staffs at the operational and tactical levels for employing biometrics in support of operations. Status: Revision</td>
</tr>
<tr>
<td>CF-SOF Multi-Service Tactics, Techniques, and Procedures for Conventional Forces and Special Operations Forces Integration and Interoperability Distribution Restricted</td>
<td>4 APR 18</td>
<td>FM 6-05 MCRP 3-36.1 NTP 3-05.19 AFTTP 3-2.73 USSOCOM Pub 3-33</td>
<td>Description: This publication provides joint planners with a single-source set of multi-service tactics, techniques, and procedures to include integration procedures. Status: Revision</td>
</tr>
<tr>
<td>DEFENSE SUPPORT OF CIVIL AUTHORITIES (DSCA) Multi-Service Tactics, Techniques, and Procedures for Defense Support of Civil Authorities Approved for Public Release</td>
<td>25 SEP 15</td>
<td>MCRP 3-35.2 NTP 3-06.1 AFTTP 3-2.65</td>
<td>Description: This publication provides joint planners with a single-source set of multi-service tactics, techniques, and procedures to include integration procedures. Status: Revision</td>
</tr>
<tr>
<td>EO Multi-Service Tactics, Techniques, and Procedures for Unleashed Explosive Ordnance Operations Distribution Restricted</td>
<td>15 JUL 15</td>
<td>MCRP 3-37.27 NTP 3-01.04 AFTTP 3-2.65</td>
<td>Description: This publication provides joint planners with a single-source set of multi-service tactics, techniques, and procedures to include integration procedures. Status: Revision</td>
</tr>
<tr>
<td>MILITARY DIVING OPERATIONS Multi-Service Tactics, Techniques, and Procedures for Military Diving Operations Approved for Public Release</td>
<td>2 JAN 19</td>
<td>MCRP 3-34.84 MCRP 3-10.2 NTP 3-02.41 AFTTP 3-2.75 CGTTP 3-06.17</td>
<td>Description: This publication provides joint planners with a single-source set of multi-service tactics, techniques, and procedures to include integration procedures. Status: Revision</td>
</tr>
<tr>
<td>NONLETHAL WEAPONS (NLW) Multi-Service Tactics, Techniques, and Procedures for Nonlethal Weapons Distribution Restricted</td>
<td>13 FEB 15</td>
<td>MCRP 3-36.8 NTP 3-07.32 AFTTP 3-2.45 CGTTP 3-06.12</td>
<td>Description: This publication provides joint planners with a single-source set of multi-service tactics, techniques, and procedures to include integration procedures. Status: Revision</td>
</tr>
<tr>
<td>OP ASSESSMENT Multi-Service Tactics, Techniques, and Procedures for Conducting Phase Operations Approved for Public Release</td>
<td>18 AUG 15</td>
<td>MCRP 5-0.3 MCRP 5-10 NTP 3-01.03 AFTTP 3-2.87</td>
<td>Description: This publication provides joint planners with a single-source set of multi-service tactics, techniques, and procedures to include integration procedures. Status: Revision</td>
</tr>
<tr>
<td>PEACE OPS Multi-Service Tactics, Techniques, and Procedures for Conducting Phase Operations Approved for Public Release</td>
<td>1 NOV 14</td>
<td>MCRP 3-33.8 NTP 3-07.32 AFTTP 3-2.40</td>
<td>Description: This publication provides joint planners with a single-source set of multi-service tactics, techniques, and procedures to include integration procedures. Status: Revision</td>
</tr>
<tr>
<td>TACTICAL CONVOY OPERATIONS Multi-Service Tactics, Techniques, and Procedures for Tactical Convoy Operations Distribution Restricted</td>
<td>22 FEB 17</td>
<td>MCRP 3-34.07 AFTTP 3-2.58</td>
<td>Description: This is a single-source, consolidated reference guide for convoys and convoy commanders to include operational considerations, planning, operations, and execution of convoys and convoy operations. Status: Revision</td>
</tr>
<tr>
<td>TITLE</td>
<td>DATE</td>
<td>PUB #</td>
<td>DESCRIPTION/STATUS</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AIRSPACE CONTROL</td>
<td>14 FEB 19</td>
<td>ATP 3-52.1</td>
<td>Multi-Service Tactics, Techniques, and Procedures for Airspace Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MCRP 3-20F.4</td>
<td>Distribution Restricted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NTTP 3-58.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFTTP 3-2.78</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Description: This publication covers theater-level, air-to-surface radar systems and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>discusses system capabilities and limitations performing airspace command and control;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>wide area surveillance for near-real-time targeting and target development;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>and processing, exploiting, and disseminating collected target data</td>
</tr>
<tr>
<td></td>
<td>10 NOV 15</td>
<td>ATP 3-65.6</td>
<td>Multi-Service Tactics, Techniques, and Procedures for Air-to-Surface Radar System</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MCRP 2-24A</td>
<td>Employment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NTTP 3-55.13</td>
<td>Distribution Restricted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFTTP 3-2.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Description: This publication covers theater-level, air-to-surface radar systems and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>discusses system capabilities and limitations performing airspace command and control;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>wide area surveillance for near-real-time targeting and target development;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>and processing, exploiting, and disseminating collected target data</td>
</tr>
<tr>
<td>BREVITY</td>
<td>20 JUN 18</td>
<td>ATP 1-02.1</td>
<td>Multi-Service Brevity Codes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MCRP 3-30B.1</td>
<td>Distribution Restricted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NTTP 6-02.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFTTP 3-2.5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Description: This publication defines multi-Service brevity which standardizes air-to-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>air, air-to-surface, surface-to-air, and surface-to-surface brevity code words in</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>multi-Service operations.</td>
</tr>
<tr>
<td>ISR OPTIMIZATION</td>
<td>14 APR 15</td>
<td>ATP 3-65.3</td>
<td>Multi-Service Tactics, Techniques, and Procedures for Intelligence, Surveillance,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MCRP 2-23A</td>
<td>and Reconnaissance Optimization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NTTP 2-01.3</td>
<td>Distribution Restricted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFTTP 3-2.88</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Description: This publication provides a comprehensive resource for planning,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>executing, and assessing surveillance, reconnaissance, and processing,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exploitation, and dissemination operations.</td>
</tr>
<tr>
<td>TACTICAL CHAT</td>
<td>24 JAN 14</td>
<td>ATP 6-02.73</td>
<td>Multi-Service Tactics, Techniques, and Procedures for Internet Tactical Chat in</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MCRP 3-40.2B</td>
<td>Support of Operations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NTTP 6-02.8</td>
<td>Distribution Restricted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFTTP 3-2.77</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Description: This publication provides commanders and their units guidelines to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>facilitate coordinating and integrating tactical chat when conducting multi-Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>and joint force operations.</td>
</tr>
<tr>
<td>TACTICAL RADIOS</td>
<td>19 MAY 17</td>
<td>ATP 6-02.72</td>
<td>Multi-Service Communications Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MCRP 3-30B.3</td>
<td>for Tactical Radios in a Joint Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NTTP 6-02.2</td>
<td>Approved for Public Release</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFTTP 3-2.18</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Description: This is a consolidated reference for TTP in employing, configuring, and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>creating radio nets for voice and data tactical radios.</td>
</tr>
<tr>
<td>TAGS</td>
<td>30 JUN 14</td>
<td>ATP 3-52.2</td>
<td>Multi-Service Tactics, Techniques, and Procedures for the Theater Air-Ground System</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MCRP 3-25F</td>
<td>Distribution Restricted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NTTP 3-58.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFTTP 3-2.17</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Description: This publication promotes Service awareness regarding the role of</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>airpower in support of the JFC’s campaign plan, increases understanding of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>air-ground system, and provides planning considerations for conducting air-ground</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ops.</td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

---

**Air Land Sea Bulletin Article Requirements and Deadlines**

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

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

<table>
<thead>
<tr>
<th>Issue</th>
<th>Deadline</th>
<th>Point of Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Winter</td>
<td>1 October 2019</td>
<td><a href="mailto:alsC@us.af.mil">alsC@us.af.mil</a></td>
</tr>
<tr>
<td>Summer</td>
<td>1 March 2020</td>
<td><a href="mailto:alsA@us.af.mil">alsA@us.af.mil</a></td>
</tr>
<tr>
<td>Winter</td>
<td>1 October 2021</td>
<td><a href="mailto:alsB@us.af.mil">alsB@us.af.mil</a></td>
</tr>
</tbody>
</table>
ALA’s mission is to rapidly and responsively develop multi-Service tactics, techniques and procedures, studies, and other like solutions across the entire military spectrum to meet the immediate needs of the warfighter.

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