AIR LAND SEA BULLETIN

Issue No. 2018-2 **Air Land Sea Application (ALSA) Center** *Summer 2018*

Approved for public release; unlimited distribution.

ALSA Staff

Director
Col Brian Gross, USAF

Deputy Director
COL Matthew Ketchum, USA

Bulletin Editor
Maj Ryan Batchelor, USAF

Editor
Ms. Patricia Radcliffe, Civilian, USAF

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

Publications Officer
Lt Col Darin Lupini, USAF

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

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

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

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

CONTENTS

FEATURE ARTICLES

IN HOUSE

AIR LAND SEA BULLETIN
Issue No. 2018-2
Air Land Sea Application (ALSA) Center
Summer 2018
Approved for public release; unlimited distribution.

Cover Photo Information

Multinational special operations forces provide security after exiting a US Army CH-47 Chinook helicopter March 12, 2018, during the Close Quarters Battle (CQB) training course held at the International Special Training Centre in Pfullendorf, Germany. The four-week course consisted of introductory and advanced CQB procedures, as well as mechanical and shotgun breaching. The course was designed to teach special operations forces and enablers standard techniques when working with different nations. Soldiers from four countries including the Italy, the Netherlands, Norway, and the United States, attended the course. (Photo by Staff Sgt. Matt Britton, USA)

DIRECTOR'S COMMENTS

The Air Land Sea Application (ALSA) Center team's goal is to meet the needs of the joint warfighter by providing timely, relevant, and compelling doctrine. This summer, ALSA will welcome several new, talented officers to help achieve this goal. Unfortunately, we must also say goodbye to some of our most capable people as they move on to new endeavors.

We welcome Lt Col Brent Blandino, United States Air Force (USAF); Maj Craig Pachlhofer, USAF; MAJ Ethan Loeffert, United States Army (USA); Maj James Quigley USAF; MAJ John Robertson, USA; Melissa Villanueva, civilian Budget Analyst to the ALSA team.

We extend a special farewell and thank you to the following team members: COL Michael Wiser, USA, who moved on to the Office of the Program Manager, Saudi Arabian National Guard Modernization Program; Lt Col Ian Boyd, USAF, retired after 22 years of faithful military service; and Lt Col Lawrence Evert, USAF, assigned to USAF Fighter Weapons School as Deputy Commandant, Nellis Air Force Base Nevada. Maj Ryan Batchelor, USAF, is assigned to Air Force Institute of Technology Cyber 200 and Cyber 300 courses as an instructor at Wright-Patterson Air Force Base, Ohio; MAJ Mark Peckham, United States Marine Corps, is assigned to Marine Air-Ground Task Force Training Command, 29 Palms California; and Budget Analyst Sonya Robinson, is assigned to the US Army Aviation and Missile Command, Fort Eustis, Virginia.

This Air Land Sea Bulletin (ALSB) is an open forum offering a wide mix of lessons learned, current statuses, and future considerations for joint warfighters. It contains a variety of articles that provide thought-provoking viewpoints and showcase the ingenuity and flexibility of United States (US) Service men and women and our international partners.

The first article is "Why the 'Intelligence-centric' Approach to Cyberspace Management Hampers Dynamic Multidomain Warfare", by Master Sargent Donald D. Gansberger, USAF. This article advocates a fundamental change in how offensive cyber operations are planned, coordinated, and organized as they connect with joint tactical operations. It discusses integrating cyberspace effects into the mulitdomain attack mission planning model to reduce mission planning time and enable a more effective target development model for time-sensitive targets scenarios.

The second article, "Artificial Judgement: A Case for Rethinking the Future Vector of Military Technological Innovation", is by Col Brian J. Gross, USAF; Col Douglas D. DeMaio, USAF; and COL Matthew F. Ketchum, USA. This article examines the US military's development and acquisition of artificial intelligence and machine learning technologies. It advocates for artificial intelligence and automation in augmenting human capabilities to ensure future technological superiority against global peer adversaries at the tactical level, while warning against the dangers of embracing "artificial judgement."

The third article, "A Conversation about Creating a Mission-Critical Team Learning Event Review Process (R4 Model)", is by Preston B. Cline, EdD. This article discusses ways to resolve the Tactical Knowledge Transfer Problem using the Mission-Critical Team Learning Event Review Process. This article proposes capitalizing on integrated groups of indigenously trained and educated experts to leverage tools and technology to resolve complex adaptive problems in an immersive, but constrained, temporal environment where the consequence of failure can be catastrophic loss.

The fourth article, "Successful Tactical Joint Fires Integration Training in a Resource-Constrained Environment at Fort Sill", is by Lt Col Nick Sargent, United Kingdom, Royal Airforce. This article discusses how to synchronize US Army live artillery training and US Special Operations Command close air support training sortie generation to ensure readily available joint, integrated training. This would achieve proficiency and meet the minimum standards articulated in the Joint Fires Support Executive Steering Committee for joint terminal attack controllers, tactical air control parties, and forward air controllers (Airborne).

We invite you to seize opportunities to represent your Service and share your ideas, not only by being published in future ALSBs, but by participating in joint working groups, also. As we tackle the challenges ahead, your ideas matter now more than ever. Your unique perspective can spark innovation on current and future tactics, techniques, and procedures.

To help shape the discussion and be part of the solution, go to www.alsa.mil and provide your ideas and contact information through the "Contact Us" link. Thank you for reading.

Brian J. Gross, Colonel, USAF
Director

WHY THE 'INTELLIGENCE-CENTRIC' APPROACH TO CYBERSPACE MANAGEMENT HAMPERS DYNAMIC MULTIDOMAIN WARFARE

TSgt Kyle Hanslovan (center), a cyber-warfare specialist serving with unidentified members of the 175th Cyberspace Operations Group of the Maryland Air National Guard, works in the Hunter's Den at Warfield Air National Guard Base, Middle River, Mayland, Dec. 2, 2017. Photo by J.M. Eddins Jr.

By MSgt Donald D. Gansberger, USAF

JOINT MANEUVER WARFARE AND TACTICAL CYBER OPERATIONS

The current joint fire support (FS) to the cyberspace effects integration process is convoluted, difficult, and only functional with a lot of planning. Coordinating the cyber effects request takes an unreasonable amount of time[1] and is not tactically effective for a time-sensitive target scenario such as a "pop-up" threat found in support of maneuver warfare. Within combat operations, using cyber effects as part of a multidomain attack would not, merely, be appropriate, but optimum. However, the cyber-to-tactical integration process is so inefficient it makes cyber integration clumsy. In the following tactical scenario, current cyber domain tactics, techniques, and procedures (TTP), combined with restrictive policies, make using cyberattack impossible.

> ... the cyber-to-tactical integration process is so inefficient it makes cyber integration clumsy.

THE TACTICAL PROBLEM

In the opening stages of a conflict, with a credible enemy, a likely scenario would involve a United States (US) Army Operational Detachment Alpha (ODA)[2], with a small team of foreign fighters attached to them and an aligned US Air Force joint terminal attack controller (JTAC) staring at an enemy formation from a concealed position. In this scenario, the ODA commander's marching orders are simple:

gather information concerning enemy forces and create a situation favorable for air dominance.

Immediately preceding this situation, air assets and over-the-horizon (OTH) FS systems, such as cruise missiles, will attempt to cut off the enemy's command and control (C2) and signals capabilities and degrade the integrated air defense system (IADS)[3]. This represents a typical plan during the initial phases of combat, when opening a new theater of operations.

While the enemy C2 and strategic IADS are destroyed from OTH FS, the joint force commander (JFC) will position special operations forces on the ground to degrade the enemy surface-to-air threat and support intelligence preparation of the operational environment (IPOE) efforts. These actions set conditions for the ODA to begin operations.[4] Prior to the joint forces land component commander (JFLCC) sending forces on the ground to seize objectives, there is a requirement for the air component, special operations elements, and strategic elements to neutralize the enemy's close air support (CAS) capability. This is done through achieving air superiority or dominance. A prerequisite for air dominance is neutralizing surface-to-air threats that can pose an unacceptable risk to tactical CAS platforms.

While the ODA and attached JTACs push into enemy territory with their foreign fighter escorts, they find enemy threats that prevent air superiority.

In the past, the next step would be for the ODA and JTAC to coordinate using an OTH asset (i.e., a Tomahawk cruise missile, high-mobility artillery rocket system, or conventional air-launched cruise missile). In an anti-access/area denial fight the near-peer enemy's systems have evolved to a point where single-point weapons are no longer effective enough to neutralize threats.

An example of the latest generation of surface-to-air missile (SAM) systems is the SA-22, a rapidly deploying, Russian-made system used in several countries.[5] It poses a high risk[6] to OTH cruise missiles and low-observable (LO) CAS assets, like the F-35. It forces manned platforms to increase their standoff range. Engagements require using new tactics, including swarming precision weapons. Further complicating issues is the proliferation of electronic intelligence assets in proximity to advanced tactical SAMs which put the JTAC's and ODA's communications systems at risk of being targeted. The traditional ultrahigh frequency, line of sight, and satellite communications are now easily defeated through jamming, or used to target friendly forces with effective indirect fire (IDF). To prevent mission failure in this scenario, the ODA and JTAC employed alternative communications waveforms and spectrums (such as beamforming high frequency or using data obfuscation on indigenous networks). They are part of a changed dynamic of the requirements to defeat an advanced tactical SAM system.

The SA-22 is one of several systems across the enemy C2 and IADS inventory that benefits greatly in combat efficacy from network integration with the ability to share a common operating picture with friendly and enemy force data. The SA-22, effectively, shares radar capabilities between disparate systems, making these networked weapons a massive force multiplier. However, this network integration is exploitable, potentially by tactical cyber warriors who could use the integrated nature of the IADS as an attack surface area to diminish, greatly, the efficacy of the surface-to-air threat.

... this network integration is potentially exploitable by tactical cyber warriors who could use the integrated nature of the IADS as an attack surface area to diminish, greatly, the efficacy of the surface-to-air threat.

Using covert beyond line of sight communications, the US Air Force's JTAC requests an LO aircraft and a section of Navy F-35s with a full load of small diameter bomb-II's (SDB-IIs). The JTAC coordinates over a frequency-hopping network with the aircraft and gives approval for release of the weapons into the basket and attempts

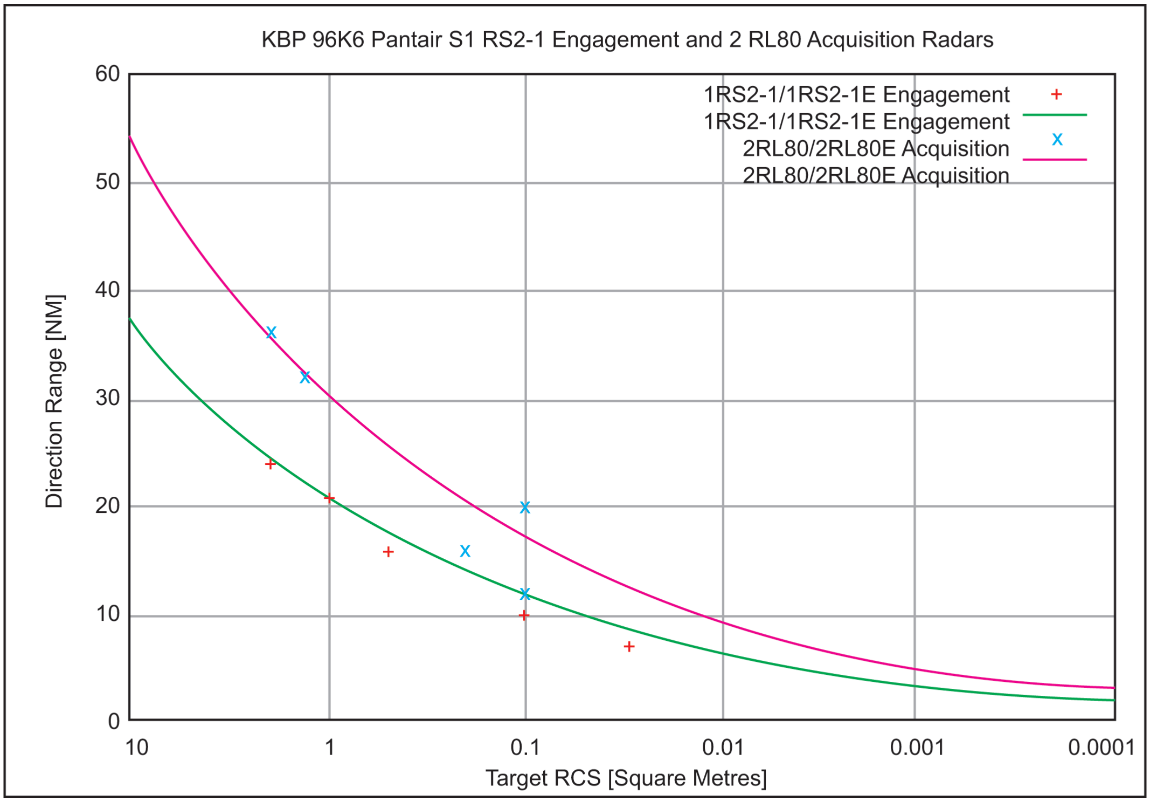


Figure 1. Estimated Detection Range Curves for the SA-22 (Dr. Carlo Kopp)

to swarm the SA-22 with a large number of the SDB-IIs homing in simultaneously.

At this point, it is a race. The F-35s are attempting to stay outside of the SA-22's engagement envelope while giving the SDB-IIs their best chance to reach the target and give the JTAC an opportunity to guide them to the target for maximum probability of kill (PK). The SDB-IIs, with their long-range glide profile, are employed to put the F-35 at the least amount of risk. The SDB-II's (and SDB-I's) biggest deficiency in CAS is that they congest airspace and make massing fires difficult for a conventional JTAC. However, this is not a factor for this scenario. The SDB-IIs give a tactical advantage in standoff for an LO platform and, most likely, the F-35 would remain safely undiscovered. If the F-35's small radar cross section is compromised by the SA-22's extremely proficient 2RL80(E) acquisition radar[7], the F-35 is at a severe temporal disadvantage; the glide weapon is much slower than the remotely-controlled 57E6 missiles. Unlike the traditional "wild weasel" missions from Vietnam where the exceptionally fast anti-radiation missiles (like the AGM-20 and AGM-88) could contend with the pace of the SAMs, the SDB-II is not going to arrive on target until long after a SAM could make it to the aircraft. Modern tactics rely on IADS systemic defeat using LO tactics to employ weapons with a great dynamic capability.

The biggest factor to exposing the overall mission to risk in a dynamic CAS-type scenario is not the engagement distance for the SDB-II ... rather, it is the JTAC's communications limitations.

The biggest factor to exposing the overall mission to risk in a dynamic CAS-type scenario is not the engagement distance for the SDB-II—the F-35 aircrews are quite competent at protecting their aircraft—rather, it is the JTAC's communications limitations. The specific frequency risks during communications between the JTAC and the aircraft is that the JTAC only has so much power to push and must avoid compromising own communications. This pulls the F-35 into a risky range for exposure to the acquisition radar.

There is no long-range, conventional artillery for the JTAC to task, in this scenario, which would allow traditional suppression methods to degrade the 1RS2-1(E) engagement or the acquisition radars. A handful of small arms for the aligned foreign fighters and the 13 rifles between the ODA and the JTAC are not going to be significant factors against enemy forces. These enemy forces may include infantry, tanks, and artillery aligned with the SA-22, and equipment like the Valeria-E electronic emissions locator system.

How could a JTAC help increase the aircraft's survivability against the SA-22? The JTAC's ability to suppress the threat is not easy with the lack of artillery or dedicated electronic warfare assets. In a multidomain conflict, the most capable attack to the IADS is a cyberattack. So, how does the JTAC request a tactical cyber effects attack against the just-found, pop-up target in timely support of the CAS asset during a time-sensitive terminal guidance operation (TGO)? The JTAC does not. Because its impossible.

The chance of success for the two F-35s to release a swarm of SDB-IIs that the JTAC "controls" all the way to terminal attack and their ability to overwhelm the SA-22 would be a coin-flip at best, with the added risk to the section of F-35s. The SA-22's ability to fire 30 millimeter antiaircraft guns and surface-to-air missiles on, approximately, one dozen targets per minute means the glide weapon of the SDB-II may not make it to the target at all.

CYBER HISTORY

Cyber operations within the US Government were pioneered by American intelligence agencies, which not only saw exploitation opportunities, but guarded American intelligence with equal tenacity.[8] The decision to segment sources, processes, and techniques, akin to the world of intelligence operations, was carried over into the cyber domain with vulnerability development, exploitations, and penetration techniques neatly compartmentalized. This organizational policy has been germane to the cyber enterprise for as long as a cyber enterprise has existed. In earlier evolutions of confrontations in the cyber domain, this methodology served US interests well. Exploitations, such as Stuxnet, operated undetected for more than a year.[9]

Stuxnet was brilliant on multiple layers; the penetration of the target network system alone was noteworthy as no external public network access existed.[10] The exploits used were not even understood by the initial civilian researchers who discovered them after they "surfaced in the wild." Even after additional penetrations and attacks with kinetic effects degraded the uranium enrichment at Natanz by a substantial amount, its complexity and sophistication was beyond the scale of most security researchers at the time.[11] Stuxnet was a strategic effort managed by the most covert cyber operators in the US Government to target a very unique vulnerability in a very specific target network. That type of operation does not easily adapt to a tactical battlefield effort. Additionally, the task of integrating cyber effects would require a more fundamental knowledge of cyber effects integration for the JTAC or the joint forward observer (JFO).

In a multidomain conflict, the most capable attack to the IADS is a cyberattack.

The JTAC is not going to do any hacking; there's no reasonable expectation that, while coordinating airspace and deconflicting FS assets from rotary- and fixed-wing CAS assets, the JTAC will attempt to cause a stack overflow to insert malicious code into the radar processing computer of a surface-to-air missile system. Cyberattacks done by computer operators, however, could be beneficial tools in the joint FS toolbox. Even the basics about opportunities, integration, and planning would be beneficial for the line-unit level combat operators to understand. The typical JTAC has a fairly complex understanding of FS capabilities and uses. It is the knowledge of how to request complex effects geometries, how to coordinate synchronous attacks with multiple assets, and how to adjust fires. JTACs can use this knowledge, passed to fire control authorities, to integrate with multiple assets giving manned and unmanned air assets the maximum freedom of maneuver while ensuring safety of flight.[12] In spite of all of this FS knowledge, the average journeyman JTAC does not know how the FS network operates or how to generate maximum ordinate values or any of a number of other FS-specific bodies of knowledge. This does not make the JTAC less effective at integrating FS into a CAS attack. It shows the marked difference in how cyber effects are coordinated, over the course of days, with compartmentalized access, and how FS is ubiquitous and responsive in support of joint warfighters. For integrated, offboard cyberattack to assist making the US' F-35 example more survivable (in the CAS/TGO operational vignette), it will take a change in how cyber, and supporting space operations, are coordinated in the realm of multidomain command and control (MDC2).

For integrated, offboard cyberattack to assist making the US' F-35 example more survivable ... it will take a change in how cyber, and supporting space operations, are coordinated in the realm of multidomain command and control (MDC2).

RUSSIAN HYBRID STRATEGY AND MULTIDOMAIN TACTICS

An informative view of this development can be seen in the evolution of near-peer operations by Russian forces over the last decade. During the 2008 invasion of the South Ossetia region of Georgia, Russia employed a disjointed mixture of integrated and unilateral cyber effects and achieved remarkable success. The initial penetration of Georgian airspace was made possible with a combination of traditional electronic attack and cyberattacks supporting kinetic operations to fully neutralize the sites.[13] This is an electronic equivalent to the operation conducted by Task Force Normandy to begin Operation DESERT STORM in 1991: the use of MH-53Js and AH-64As against Iraqi early-warning radar sites to open a "hole" for tactical fighters to pour through.[14] The Russian cyberattack was effective and done with the well-timed electronic attacks and kinetic attacks and was an effective opening salvo attack against a fixed target. The multidomain attack was a strategic effort against a fixed target that could be coordinated ahead of time and where complex timing and planning could be conducted.

... but the Department of Defense (DOD) does not have effective TTP for cyber support of maneuver warfare.

The Russian invasion of Georgia in 2008 did not, merely, have strategic commonality with the US military in the theory of Operation NORMANDY busting open a hole in an IADS network that non-LO tactical aircraft could exploit, it also employed a very similar style of cyber effect to kinetic maneuver warfare integration the US DOD does now. These are complex and coordinated time-based operations against fixed targets.

In the current MDC2 planning conferences, the integration of cyber effects is almost exclusively limited to these types of operations, which are of vital importance; particularly, against fixed strategic threats like an S-400 or similar systems, but the Department of Defense (DOD) does not have effective TTP for cyber support of maneuver warfare.

In other words, the Russian attack on Georgia was one the US could also facilitate and operate right now with the organizational limitations of the cyber domain and the slow turnaround of the air tasking order cycle. The Russian multidomain attacks facilitated an environment where dynamic tactical targeting could occur. Subsequent Russian cyber efforts were less integrated and more unilateral in nature, and succeeded in defacing Georgian propaganda and conducting widespread denial of service attacks to make Georgian C2 difficult.[15]

During operations in Eastern Ukraine, less than a decade later, the Crimean, Syrian, and Russian cyber effects were often done at a tactical level, with much faster integration between cyber operators and ground forces. In the "Hybrid Warfare Model", small scale tactical attacks are conducted to elongate protracted and expensive operations for the enemy while shrinking individual combat engagements to benefit the survivability of a small footprint of deployed assets. The Russian forces' primary mission was to support nonmilitary objectives, such as diplomatic overtures based upon misinformation or political aims. Many of the deployed ground combat forces were either mercenaries, giving the Russian state great plausible, deniability,[16] or were Russian special operators embedded with friendly guerilla forces who would benefit the Russian aims within the state. (This is much like the ODA relationship to the friendly foreign fighters in the opening vignette.)

This relatively effective doctrine was simple. It included a complex structure of FS assets, electronic intelligence assets, unmanned aerial vehicle controllers, and cyber operations teams. All were uniformed Russian forces protected by Russian heavy armor. They gave multidomain intelligence, surveillance and reconnaissance capabilities to the special operations and mercenary forces that make contact with the enemy. The integrated efforts of Russian cyber operations, with support for maneuver warfare, was more effective than the disjointed efforts in Georgia after the initial invasion.

CYBER EVOLUTION AT AN INDUSTRIAL SCALE

The notion of a more advanced usage of TTP by an enemy (compared to American operations) is, at first, rebuked by the idea that Russian cyber operators are using more "juvenile" cyberattacks against an even more vulnerable enemy, and that overuse of tactical cyberattack is a vulnerability to itself. The overarching theory, supported by a trilateral policy for process approval, is that by employing tactical cyberattack TTP against tactical threats, the strategic value of the exploit and the attack infrastructure are put at unreasonable risk. This is true with regard to exploits of strategic value; but if it becomes the only methodology for using cyber effects, it negates all forms of maneuver warfare.

From a multidomain combat perspective, in support of modern maneuver warfare, this Russian force is far more dynamic and integrated than current American cyber doctrine would allow. Cyberattack exploits, often, are only operationally valid for hours or days and a massive infrastructure of industry exists to neutralize and defeat cyber threats that occur at a very rapid pace. In the meantime, the "intelligence-style" policy for strategic cyber infrastructure means tactical exploitations are not timely to use against a strategic infrastructure due to policies.

In February 2018, there were 1,339 common vulnerabilities and exposures reported to the national vulnerability database,[17] many of which were critical vulnerabilities exposing systems to complete takeover by an effective attacker. This rapid growth in vulnerabilities is countered with an even more dramatic growth in the cybersecurity industry. From 2004 to 2017, investment in the cybersecurity industry grew by approximately 3,480% with industry predictions of more than $1 trillion in spending between 2017 and 2021.[18] Cybersecurity costs are increasing faster than the DOD could afford to spend. Every time a hack compromises thousands of customers' personal information, the commercial sector increases its focus on cybersecurity and drives the industry further forward. Even for vulnerabilities obfuscated from public release due to inherent intelligence value, there is an industry which will seek to either exploit them or, commercially, patch them anyway.

Cyberattack exploits, often, are only operationally valid for hours or days and a massive infrastructure of industry exists to neutralize and defeat cyber threats that occur at a very rapid pace.

This commercial growth is exploited into US forces' potential near-peer adversaries' tactical combat capabilities better than by the existing DOD acquisition system. From 2010 to 2016, an estimated 10% of venture capital deals in the Silicon Valley were funded by China,[19] with cybersecurity advancements among the technologies sent overseas with robotics, artificial intelligence (AI) and augmented reality. Combining the inefficient Joint Capabilities Integration Development

System (JCIDS), that has proven time and again to be an abject failure for software and cyber projects[20], with the general bureaucratic issues regarding cyber integration into joint tactical combat, allows near-peer enemies to use American-developed technological advances on the battlefield faster than the US. A simpler example of this is: the US Air Force took over two and a half years to implement Windows 10 on its internal networks.[21,22] The idea that the JCIDS process will be able to deal with threats where 1,339 new exploits are found in a month is only half of the problem. The true issue impacting US cyber operations is that the enemy is much better than the US military at leveraging the $1 trillion cybersecurity investment into tactical advantages.

CHANGING VIEW

Since the commercial world is advancing cybersecurity as an industry faster than militaries can keep up, there come exploitative opportunities. As new vulnerabilities are found, existing deployed systems are at more and more risk, and the difficulty for militaries (the US DOD worse than most) to implement upgrades and patches is problematic. In modern network-enabled warfare, the threat surface area is massive. Forty years ago, the idea of neutralizing a tactically significant IADS node without kinetic effects might have required getting an intelligence agent to compromise the air defense battery commander or sabotage it by an elite agent. Now, potential avenues for attack may involve guessing the passwords used by a maintenance technician and making educated guesses by attacking the technician's favorite blog site with a SQL (or other language) injection attack. As wider surface areas appear, the opportunities for a competent cyberattacking organization to exploit them grows. Given the US DOD acquisitions system's flaws, a near peer may be able to out-pace the DOD's ability to attack and defend in the cyber domain. Only by embracing innovative development efforts will the cybersecurity industry bridge that gap for the operators in the cyber domain. The massive cyber threat surface area[23] is rife for exploitation in any number of ways, and an enemy using a large swath of new commercial knowledge to develop threats is going to be ahead of American cyber-defenders. However, even fixing the acquisition problems will not benefit the US' ODA, JTAC, and F-35. To give them a better chance at defeating a cyber-vulnerable IADS will take a paradigm shift in how cyber operators interact with the tactical warfighter.

Cyberattack exploits, often, are only operationally valid for hours or days and a massive infrastructure of industry exists to neutralize and defeat cyber threats that occur at a very rapid pace.

WHAT MAKES A DOMAIN UNIQUE?

With the establishment of the JTAC Weapons Instructor Course (WIC), the JTACs became the first ground combat operators to operate an Air Force weapons course,[24] and it is modeled on the Air Force Fighter Weapons School model used for all WICs. The JTAC cadre has learned, while the principles of instruction, the value of debriefs, and the value of understanding integration and equipment are the same as with their fighter pilot peers, there are fundamental differences in TTP evolution in the land domain. As an example, the principles of dogfighting have evolved remarkably over the last 60 years than small-unit tactics for gunfights on the ground. The JTAC WIC graduates are able to teach the advantages of certain datalinks or mobile ad-hoc networks for enhanced situational awareness, but they are using the same basic small arms rifle (i.e., M4 carbine, a derivative of the M-16) as their fathers or grandfathers did in Vietnam while using the same techniques[25] for breaking contact against a larger infantry force. This parallels the real world, as infantry units facing one another date back more than a millennium, with advancements corresponding to the slow evolution of equipment. Conversely, the aircraft itself is barely more than a century in age, with rapid innovation over the decades enabling beyond visual range engagements and split-formation tactics with coordination conducted using covert communications technologies. This drives a rapid TTP evolution model, one that is the basis for many of the advances taught by the JTAC WIC instructors. Communications, awareness, and data integration are the technical advancements driving new ground tactics for the JTAC.

In the cyber domain, TTP development does not conform to an annual, or even semi-annual, weapons and tactics development cycle. Vulnerabilities with commercial applicability used as attack vectors may have effective shelf-lives of hours, if not minutes, and it takes a fundamental shift in organization to exploit these cycles. For strategic attacks, such as Stuxnet, no real change to the TTP process is necessary. All that would benefit a strategic cyberattack organization is a change in the acquisition nightmare to enable a greater exploitation of the enemy at a faster rate. For the tactical cyber operator, the acquisition reform would be the lifeblood of tactical exploits, but it will only be the integration with the tactical warfighter that allows cyber effects to reach their potential.

THE STRATEGIC VS. TACTICAL SHIFT

Fundamentally, the effective solution is to alter the way organizations split their strategic and tactical warfighting approaches to fight in the cyber domain. The intelligence-driven cyber organizations must be maintained as they exist now, complete with their overwhelming compartmentalization. This is to keep a library of effective "strategic" cyberattacks available for the cyber equivalent of Operation NORMANDY in another shooting war's opening stages, or for a hybrid attack like Stuxnet. Their library of exploits needs either to weaponize emerging "zero day" vulnerabilities, immediately, to create persistent access in support of expeditionary strategic attacks; or maintain the types of vulnerabilities not likely to be the focus of the growing cybersecurity industry. Flaws with commercial applicability may be powerful and grant the attacker complete access, but as a vector, are short-lived. The existing cyberattack infrastructure needs to maintain an eye on the obscure, system-based exploits that are not going to be found by an AI-driven, exploit discovery and patching system. The difficulties of this job are myriad. They include building a "burnable" infrastructure to activate and apply the exploits, maintaining weaponized exploits in light of a growing cybersecurity industry, crafting exploits against obscure systems that do not have an analogue in the commercial world, and providing persistent access when expeditionary cyber access projects turn into strategic kinetic attacks.

In the cyber domain, TTP development does not conform to an annual, or even semi-annual, weapons and tactics development cycle.

While strategic cyberattacks are treated like nuclear weapons, retaining their close relationship with United States Strategic Command, tactical cyber organizations within each Service need to change their focus from being part of the strategic cyber effort to one of broad cyber defense and tactical warfighter support. Current defensive efforts of maintaining and patching cyber threats based on a, woefully, inadequate set of bureaucratic policies needs to be abandoned and shifted to embrace the cybersecurity industry. This will advance the US cyber defenses from borderline obsolescence to state of the art.

Tactical cyberattack will use commercial, open source, and nefarious sources to build a rapidly-growing (and decaying) library of tactically-beneficial attacks, a dynamic infrastructure for access (even when it is not persistent), and a C2 structure to interact with the tactical warfighter to bring them to bear. Library maintenance would be difficult for the following reasons:

1. The dynamic number of threats and exploits and which ones are still effective against what targets in a combat environment is broad.
2. The commercial cybersecurity in-

dustry is playing a role in the rapid evolution of offensive and defensive measures.

3. Predicting efficacy would involve complex models.

Overcoming these difficulties would be central to maintaining a continuously effective, tactically offensive cyber operator. Furthermore, many exploits developed to support the tactical cyber operator may have greater "firepower" than their strategic counterparts, but will only be viable for short time periods. While a strategically valuable enemy system could be attacked by DOD strategic cyber operators as soon as an exploit is discovered (if for no other reason than to insert another persistent access exploit), it may have minimal value against a system with minimal network access. Ironically, many systems on protected networks can be exposed to incredibly old, well-known, and often-patched exploits[26] due to the nature of compartmentalized network systems.

There is no standard among the Services regarding the maturity of cyber operations integration at the tactical level.

Fundamentally, the US needs to change how cyberattacks are planned, coordinated, and organized; especially, as the shelf-life of attacks may last for minutes or even fail during their execution. The tactical cyberattack operators must be cognizant of attack efficacy and ever-dynamic library with an understanding of how attacks will interact with the tactical operators.

There is no standard among the Services regarding the maturity of cyber operations integration at the tactical level. However, there is a lack of overall integration, particularly across the joint effects coordination and MDC2 enterprise. This makes true tactical target exploitation in a timely, adhoc manner nearly impossible for any Service.

MULTIDOMAIN TACTICAL VIGNETTE

Given a tactical cyber operator capable of providing support in the original vignette, the organizational model would most likely employ an Air Force cyberattack, even if the JTAC was from another branch of Service or an allied country. Exploiting an SA-22 system will be an intense focus area for the Air Force, especially during a theater operation. In the SA-22 example, the JTAC passed the request for CAS, and that the target was an SA-22, over the chosen medium. The threat of the SA-22 should be rapidly disseminated across multiple networks. Efforts should be made to begin "enhancing" target resolution on the platform and should be coordinated across several domains. This means, even prior to the JTAC requesting a cyberattack, the tactical operators in the cyber domain will be able to begin IPOE of the SA-22 and assess a myriad of options from how they will gain digital access to what exploits are likely and available.

The JTAC in the field, with the ODA, receiving a digital common operating picture (such as tools delivered on top of Android Tactical Assault Kit) would give the JTAC notification that a cyber effect was available for this factor threat and an operator was available for the mission. The JTAC would craft an attack plan using the section of F-35s to deliver kinetic effects from the SDB-IIs, but use the cyberattack similar to an indirect fire attack, timing the coordinated attack between the two domains, and drastically reducing the efficacy of the SA-22. This would increase the PK for the SDB-IIs because the SA-22 would either not fire or fire errantly, and reduce the number of weapons needed to prosecute the attack and reduce the overall factor threat to the section of F-35s.

After prosecuting the attack, the SA-22 is neutralized and the factor threat to the F-35 is significantly reduced. Then, the JTAC is able to neutralize the Valeria-E system and a few of the artillery and armor pieces in a follow-up attack prior to the aircraft returning to base.

Subsequently, the JTAC and the ODA are notified that national assets have confirmed there is no longer a factor threat or an effective electronics intelligence threat in the area, and a flight of two A-10Cs is sent for support.

The A-10Cs would be the most effective tools against the heavy armor and artillery pieces remaining, but would have stood little-to-no chance against the SA-22, and the JTAC would have had no effective way to communicate with the A-10C if the Valeria-E remained viable. Instead, using a tactical cyberattack in a timely and effective manner, coordinated with kinetic operations from fifth- and third-generation tactical aircraft, the JTAC is able to annihilate the entire enemy formation with only two flights of aircraft and hardware already in existence, in the air and on the ground.

This vignette is a microcosm of a potential integration among the ground combatant, strike platform, and cyber warrior against a potential enemy system. The ability to degrade the enemy's defenses and force combative terms to those benefitting American maneuver doctrine warfare will require a migration to a multidomain combat capability. The ability for joint warfighters, especially those integrating multi-Service TTP and coalition firepower (like the JTAC and the JFO) will require greater tactical cyber integration. Also, the need for those combat operators to understand cyber capabilities and integration requirements must be expanded. Facilitating integration will require the cyber enterprise embrace more dynamic TTP and interface with a burgeoning commercial cybersecurity sector to enable greater offensive and defensive capabilities than those currently in use.

END NOTES

[1] Air Land Sea Application Center (2016), "JFIRE, Multi-Service Tactics, Techniques and Procedures for Joint Application of Firepower".

[2] Air Land Sea Application Center (2015), "J-SEAD, Multi-Service Tactics, Techniques and Procedures for Joint Suppression of Enemy Air Defenses".

[3] Bucki, Elliot (2016) "Flexible, Smart and Lethal: Adapting US SEAD Doctrine to Changing Threats".

[4] Joint Staff (2017) Joint Publication 3-01, "Countering Air and Missile Threats," 21 Apr 2017.

[5] Egozi, Aryeh & Alex Fishman (2007) "IDF: Syria's antiaircraft system most advanced in [the] world" yNet News.

[6] Kopp, Carlo, PhD. (2012) "Technical Report APA-TR-2009-0703." Air Power Australia.

[7] Kopp.

[8] Jackson, William (2009) "DOD Creates Cyber Command as US Strategic Command subunit." Federal Computer Week.

[9] Camacho, Jennifer. (2013) "The Stuxnet Virus and the Damages it Caused." The Machiavellian Eye.

[10] Langner, Ralph. (2013) "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve." The Langner Group.

[11] Oleg, Kupreev, and Ulasen Sergey. (2010) "Trojan-Spy.0485 and Malware-Cryptor.Win32.Inject.gen.2 Review." VirusBlokAda.

[12] Department of the Air Force (2016) "Tactical Air Control Party Career Field Education and Training Plan."

[13] Hollis, David (2011) "Cyberwar Case Study: Georgia 2008." Small Wars Journal.

[14] Dorr, Robert (2009) "Task Force Normandy Fired the Opening Shots of Desert Storm." Defense Media Network.

[15] Hollis.

[16] Taylor, Adam (2018) "What We Know about the Shadowy Russian Mercenary Firm behind an Attack on US Troops in Syria." The Washington Post.

[17] National Institute of Standards and Technology (2018) "National Vulnerability Database".

[18] Morgan, Steve (2017) "Cybersecurity Ventures Predicts Global Cybersecurity Spending will Exceed $1 trillion from 2017 to 2021"

[19] Brown, Michael, and Pavneet Singh (2017) "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of US Innovation." Defense Innovation Unit—Experimental.

[20] Insinna, Valerie (2017) "Air Force Cancels Air Operations Center 10.2 Contract, Starts New Pathfinder Effort." Defense News.

[21] Microsoft (2018) "Windows 10 release information."

[22] Naskar, Rahul (2018) "The US Air Force is Upgrading all the PCs to Windows 10." Windows Latest.

[23] Walker, Zach (2017) "Project Voltron: Defense Innovation Unit Experimental Briefing".

[24] Ika, Siuta (2015) "Air Force Weapons School JTAC Graduates to Receive Hallowed Patches," Military.com.

[25] Department of the Army (2016) "Army Techniques Publication 3-21.8—Infantry Platoon and Squad".

[26] Gerritz, Chris (2016) "Breach Detection by the Numbers: Days, Weeks or Years?" Infocyte.

ARTIFICIAL JUDGEMENT: A CASE FOR RETHINKING THE FUTURE VECTOR OF MILITARY TECHNOLOGICAL INNOVATION

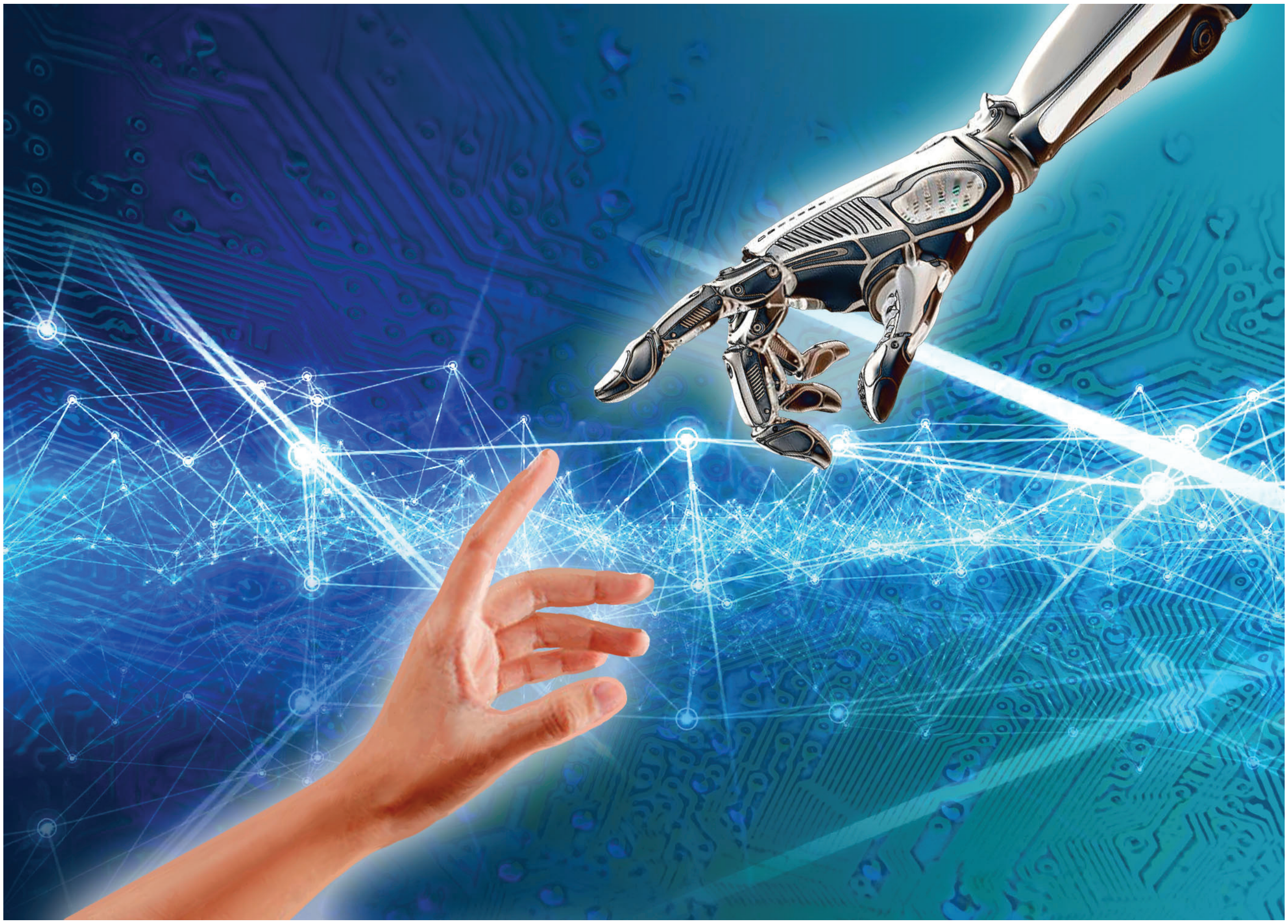


Illustration by Daniel Armstrong, LeMay Center, USAF

By Col Brian J. Gross, USAF; Col Douglas D. DeMaio, USAF; and COL Matthew F. Ketchum, USA

INTRODUCTION

The United States (US) military is falling behind in the global race for military technological superiority. This lag is due to a number of factors, which include: a cumbersome acquisition system, budget constraints and uncertainty, a focus on the counterinsurgency fight, a culture that is adverse to failure, and a pervasive lack of focus on innovation and invention. The Service secretaries and chiefs, among others in the Department of Defense (DOD) and defense industrial base, have made a marked push to reverse course. Now that the counterinsurgency fight has subsided, the DOD budget forecast is more robust, and a concentrated effort to devise a rapid acquisition process has begun, the Services have signaled full speed ahead for innovation and risk tolerance. In a future faced with contested domains across the spectrum of warfare (particularly air, space, and cyber), the US must not only catch up with technology, but leap ahead to regain a competitive advantage.

Many of the latest Service initiatives center on two ideas: gaining better networks and exploiting machine learning.

Many of the latest Service initiatives center on two ideas: gaining better networks and exploiting machine learning. There are incentives to improve the US military's command and control (C2) networks and reap the benefits of big data synthesis and artificial intelligence (AI). However, when it comes to pulling the trigger on the front lines in battle, networks cannot be guaranteed and AI will continue to fall short of human capabilities. Neither the unaided human nor unmanned machine will win a future conflict. Exploring the benefits of AI at the tactical level requires a new strategy for innovation and invention.

A NEED FOR INNOVATION

"…our technological overmatch is decreasing as near-peer adversaries increase their capability and capacity," said General Joseph F. Dunford Jr. during his nomination for reconfirmation as Chairman of the Joint Chiefs of Staff in September 2017. He later added, "While we have identified areas in which we have limited capacity, the larger issues are that our technological overmatch is eroding and our adversaries' speed in narrowing capability gaps is accelerating; increasing capacity alone will not reverse these issues."[1] Adversaries who were once labeled as near-peer have leveled the battlefield by possessing technological capabilities that are on par with, and in some instances have exceeded the capabilities of, the armed forces of the US. It is clear from his comments, and those of other Service leaders, the US is lagging behind in a global race for military technological superiority. For the last 16 years, the Services have focused their attention on battling the counterinsurgency fight while failing to recapitalize or modernize legacy weapons systems and C2 capabilities.

The Service chiefs are endeavoring to reverse course and enter a new era of technological advancement with an increased or renewed focus on innovation. They are seeking advanced, integrated communications technologies to support the future operations in multiple domains. American military leadership acknowledges the benefits of coordinated air, land, sea, space, electromagnetic spectrum, and cyber operations but lack the compatible technology, acquisition strategy, and doctrine to guide it.[2]

Though it is not a new concept, when one considers future conflict with a sophisticated adversary or competitor, advancing the multidomain battle concept is almost certain. Adversaries, potential adversaries, and competitors have learned to exploit US military vulnerabilities and contest US superiority in warfighting domains, particularly in the cyber domain. In the last 50 years, the US was contested in the air, ground, and maritime domains. Now, US capabilities and access are contested in space, cyberspace, the electromagnetic spectrum, and across C2 networks.[3]

Exploring the benefits of AI at the tactical level requires a new strategy for innovation and invention.

The Service chiefs, among others in the DOD and defense industry, have advocated for a technological revolution to unite warfighting domains and functions, and the Services to counter advancing adversary capabilities. During the 2017 Air, Space, and Cyber Symposium in Washington DC, General David L. Goldfein, Air Force Chief of Staff, emphasized an imperative for Air Force advancement of technology, and what he called the future "wars of cognition." General Goldfein posed the question, "what does the Air Force need to be in the year 2030?" He went on to consider that question, partially answering it with two additional questions and answers: "Can it connect? Good. Can it share? Even better."[4]

Soon after, General Mark A. Milley, who spoke at the AUSA Eisenhower Luncheon in 2016, relayed much of the same sentiment, but went a bit further in depth discussing the role of AI and potential, profound changes in the future character of war.[5]

General Goldfein posed the question, "what does the Air Force need to be in the year 2030?" He went on to consider that question, partially answering it with two additional questions and answers: "Can it connect? Good. Can it share? Even better."[4]

General Goldfein's point on a connectivity and data sharing imperative highlights the military's current lack of innovation and a dynamic acquisition strategy. The problem with the connectivity and data sharing argument with a 2030 target, however, is that the timeframe is off by about

30 years. Technology in 2030 will, or should, surpass the proposed benchmark. The world is already connected and can share. US weapons systems cannot; and potential adversaries know it. If leaders want to shape an acquisition strategy which targets the year 2030, they must ask different questions and try to understand what is beyond connectivity.

The world is already connected and can share. US weapons systems cannot; and potential adversaries know it.

During the February 2018 Air Force Association Symposium, General Goldfein updated his position by pushing out the timeframe to the year 2045 and adding an important question to his earlier ones. In addition to the ability to connect and share, he asked and answered, "Can it learn?" "Perfect." This addition is important because he took the Air Force effort from current technology to emerging technology. While this was an important step forward, it continues to miss the mark in some regard. If the Air Force is to "push the boundaries of Moore's Law" and "kick-start the technological edge," it should not equate machine-learning technology with perfection.[6] Machine learning and AI represent immense opportunities, not necessarily the pinnacle. While defining future technology, perfection is difficult. It is reasonable to suggest including the human nexus as well.

FUTURE LANDSCAPE

Big data, machine learning, and other forms of AI will inform the future joint warfighter, with access to, and rapid synthesis of, information being key asymmetric factors to winning the next fight. Leveraging information to build perfect situational awareness has been the dream of warfighters since the dawn of warfare; a quest that can never be fully achieved. However, coordinated, multidomain operations are achievable but will require instantly and reliably integrating all domains and warfighting functions, with a common understanding of the battlespace.[7] Integration begins with common, reliable communications. Commanders at the strategic and operational levels who already have access to enormous amounts of information will soon have access to much, much more. They will have so much data that computers will have to learn to do the heavy lifting. This represents an area in which the military is falling behind; it is, effectively, throwing away enormous amounts of usable data due to a lack of capacity for machine learning and other forms of AI[8] to help lighten and, exponentially, speed up the traditionally human burden of information synthesis.

… coordinated, multidomain operations are achievable but will require instantly and reliably integrating all domains and warfighting functions, with a common understanding of the battlespace.[7]

Current efforts for redundancy and hardening networks are needed but do not, necessarily, equate to ensured network reliability. At all levels of warfare (particularly, the tactical level), redundant, multi-node, layered networks will not be enough to ensure US weapons systems remain connected. The legacy networks, like the Army's Warfighter Information Network-Tactical, are insufficient to counter emerging threats, therefore, new systems are needed. As the US military builds new capabilities (where every tactical vehicle, aircraft, and ship are nodes in the network) the US becomes more dependent on a system which can never be guaranteed. This is an era where America's adversaries have a proven ability to deny network access, target and exploit electromagnetic signatures, and shoot down communications satellites. The US' competitors have modernized their forces and have learned to exploit America's vulnerabilities.[9] Therefore, tomorrow's warfighter cannot expect unlimited network access.

TACTICAL-LEVEL APPROACH AND ARTIFICIAL JUDGEMENT

With a future of contested domains and increased effort toward simultaneously enabling operations on multiple domains, the joint community must not focus on a catch-up strategy but step up efforts in developing innovative strategies designed to leap forward. Current efforts to bolster C2 systems and jump-start innovation initiatives take a top-down approach, tackling the enterprise perspective first. A bottom-up approach is warranted also.

Looking from the tactical warfighter's perspective, the ability for all warfighters (from Air Force fighter pilots to infantry Marines) to win will be determined by their ability to fight in a denied or degraded operational environment against a peer competitor. The challenge is not to figure out how to capture big data and advance machine learning (both of which US forces must do) but how the trigger pullers can leverage information when access is intermittent or denied. This, of course, presumes trigger pullers are human, which is not necessarily what some developers are working toward.

As technology evolves and traditional human tasks become more automated, a compulsion emerges where autonomous tactical weapons systems are almost a foregone conclusion. The defense industry appears intent to write humans out of the equation, replacing them with the superior speed and accuracy promised from AI. However, important questions remain. What about the paradox which exists where data and algorithms are continually informed by a network which cannot be guaranteed due to outage or exploitation? What is the failure rate of a computer versus the failure rate of a human? While it is difficult to determine the consequences of connectivity that is not guaranteed or is exploited upon implementation of AI on live targets, it is reasonable to assert, at a minimum, mistakes will occur and innocent lives could be lost. Left to themselves, brilliantly-fast machines likely will decide counter to what military leadership and politicians want, and they will fail.

The benefits of automation to the warfighter, on the other hand, are great. Automated systems designed for threat detection and response (for physical and cyber threats) offer superior response times and accuracy over those requiring human input[10]. For example, when it comes to physical threats, such as inbound surface-to-air missiles, the success of automated detection and countermeasure systems is immediate. Likely, future systems will be even better, such as closed-loop infrared countermeasures, which promise to identify specific missiles and jam threats before they are launched and without human input. For cyberattacks, detection is becoming increasingly difficult as adversaries capabilities grow in sophistication and using advanced automation. Future threat detection and countermeasure employment will rely on cyber teams with their own automated, adaptive AI tools.[11]

Automation has bested human capacity and capability in many areas, yet, it is more difficult to determine which traditional human activities are better suited for AI and machine learning. While automation follows predefined and predictable actions based on human authorization, an autonomous system would identify its own course of action without human interaction.[12] What is required for a machine to continue a mission with imperfect, compromised, or missing information? It is impossible to program a machine with every possible scenario it could encounter in combat, because a machine would have to analyze all information, discount erroneous or otherwise useless information, extract relevant information, and learn from it.[13] It is easy to envision the risks involved. The ability of a machine to learn to drive a car from San Francisco to Los Angeles, California; determine which movie a person from Des Moines, Iowa may enjoy on a Saturday; or to pick potential terrorists from a live video feed can be accomplished with relatively little risk. As the US debates who is accountable when AI fails, the stakes increase immensely when considering inserting machine learning into the kill chain.

The challenge is not to figure out how to capture big data and advance machine learning (both of which US forces must do) but how the trigger pullers can leverage information when access is intermittent or denied.

Can AI replace having a human in the loop? Even if we accept that the world is open to a future where AI takes over part, or all of, large data synthesis functions, the risks associated with AI-driven kill or live decisions are unacceptable. At a time when the US is risk adverse, considering collateral damage, civilian casualties, fratricide, or a laser-guided bomb drop without a combined force component commander's approval, it is unlikely the US will allow a machine to make life or death decisions.

America's next generation weapons systems require near-continuous connectivity for everything from navigation and identifying friendly systems to data sharing and voice communications for weapons release clearance.

To abide by the principles of international law, autonomous systems would be required to distinguish between civilians and combatants, and adhere to the principles of proportionality and precaution.[14] Autonomous systems would have to make informed, considered decisions and come to a sensible conclusion—in other words, they must use their own judgement.[15] Furthermore, should a mistake occur where a machine directed or caused the death of a noncombatant, officials involved would want to know how the machine made its judgement. With machine learning, there is no guarantee the decision points can be explained clearly and lessons learned.

... a similar effort should be placed on ways to leverage large amounts of synthesized information without fully relying on it.

As the world becomes more comfortable with the prospects and potential benefits of AI, the idea of becoming comfortable relying on "artificial judgement" seems unpalatable. If intelligence is the ability to acquire and apply knowledge, and judgement is the ability to make considered decisions and arrive at sensible conclusions, it is clear which role is more suited to machine learning. When it comes to life or death decisions, the world is not ready for artificial judgement.

When it comes to life or death decisions, the world is not ready for artificial judgement.

It is reasonable to predict that a future foe, whether a state or non-state actor, will opt to wage war with rules of engagement lacking moral value by international standards. The adversary will trade what the US considers moral conduct for the speed and accuracy of AI and the promise of a quick and complete victory. It can be argued that the US and allies will not have the same calculus, and will have to figure out a way to retain its morals while defeating a moral-less enemy. That avenue to victory will need man-machine teaming.

A VECTOR FOR INNOVATION

Getting the warfighting trigger pullers to their targets in a contested environment, armed with the best AI-informed data to make sensible decisions is a challenge. America's next generation weapons systems require near-continuous connectivity for everything from navigating and identifying friendly systems to data sharing and voice communications for weapons release clearance. To remain ahead of competitors and continue enjoying freedom to maneuver and relative freedom from attack, the US must innovate.

The great effort afforded to hardening networks and adding redundancy are important, but the US should not rely on that which cannot be guaranteed. Thus, a similar effort should be placed on ways to leverage large amounts of synthesized information without fully relying on it. While America's best and brightest throughout the defense industrial base advance AI and bolster C2 systems, the military should consider focusing some of that intellect on dumbing down weapons and weapons systems. This involves refraining from the current momentum in distributing capability and capacity across large communications environments to concentrating it in time and space, while eliminating much of the connectivity requirement.

Consider this: humans are the smartest, "dumb" weapons system available. No computer can replicate the ability to assess a situation with limited information like a human. Also, consider computers with AI and machine learning can synthesize, exponentially, more information at a much faster rate than humans. Military leaders must marry human cognition with machine learning and automation; i.e., team man with machine. This imperative becomes clear when looking from the tactical perspective as opposed to the theater-wide/operational perspective.

"Dumbing down" US weapons systems is a bit of a misnomer, but is meant to paint a picture that intelligence does not require constant connectivity. To survive in a future contested electronic environment, weapons and weapons systems must be AI informed, and human and machine applied. Humans for cognition, situational awareness, and judgement; machines for synthesis and automation. These systems should be nearly autonomous, informed before deployment, self-navigating, able to run without (or with little) outgoing electronic emission, and able to receive updates via data burst or a similar direct means. They should leverage information, never fully relying on it, while being capable of distilling limited, available information to make the weapons systems or man-machine team smarter.

For the Services, "dumbing down" appears to go against a tradition of continual cutting edge invention. It does not. The next revolution (or offset) in American military capability may be the ability to merge AI and human cognition to stop envisioning the two capabilities as independent, and begin building complementary systems from the ground up. The next generation bomber, submarine, or combat vehicle should be able to transit theaters and travel to their targets without electronic transmission of any kind. For example, the US Army's Next Generation Combat Vehicle is being envisioned with some remarkable technology, including an unmanned turret and autonomous driving capability with a flexible architecture designed to allow for future innovation.[16] That technology could be built with the flexibility to travel and employ weapons without being connected to a network.

The same applies to all future capabilities the US must continue to fund and research, including hypersonic weapons.[17] Having the capability to disconnect and work autonomously eliminates an adversary's opportunities for electronic spectrum denial, spoofing, or using emissions to find and target a friendly weapons system. Integrating a human with AI at the tip of the spear helps ensure future leaders make the right judgment call.

The next revolution (or offset) in American military capability may be the ability to merge AI and human cognition to stop envisioning the two capabilities as independent, and begin building complementary systems from the ground up.

END NOTES

[1] General Joseph F. Dunford, Jr., For reappointment to the grade of general and reappointment to be Chairman of the Joint Chiefs of Staff, United States Committee on Armed Services, September 26, 2017. https://www.armed-services.senate.gov/hearings/17-09-26-nomination_--dunford

[2] David G. Perkins and James M. Holmes, Multidomain Battle: Converging Concepts Toward a Joint Solution, JFQ 88, 1st Quarter 2018. http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-88/jfq-88_54-57_Perkins-Holmes.pdf?ver=2018-01-09-102340-943

[3] See Multidomain Battle: Combined Arms for the 21st Century, 24 February 2017 http://www.tradoc.army.mil/MultiDomainBattle/docs/MDB_WhitePaper.pdf

[4] See 2017 Air, Space & Cyber Symposium Remarks by General David L. Goldfein, US Air Force Chief of Staff, 19 September 2017. http://www.af.mil/Portals/1/documents/csaf/CSAF_AFA_2017%20Air_Space_and_Cyber_Symposium.pdf

[5] General Mark A. Milley, AUSA Eisenhower Luncheon, October 4, 2016. http://wpswps.org/wp-content/uploads/2016/11/20161004_CSA_AUSA_Eisenhower_Transcripts.pdf

[6] https://www.dvidshub.net/video/586175/2018-air-warfare-symposium-gen-david-goldfein-csaf

[7] Multi-Domain Battle: Evolution of Combined Arms for the 21st Century (December 2017). http://www.tradoc.army.mil/MultiDomainBattle/docs/MDB_Evolutionfor21st.pdf

[8] Gideon Grudo (February 22, 2018). Alphabet Executive: USAF Wasting Opportunities for Future Innovation. http://www.airforcemag.com/Features/Pages/2018/February%202018/Alphabet-Executive-USAF-Wasting-Opportunities-for-Future-Innovation.aspx

[9] Corey Dickstein (2017). Army Rolls Out Field Manual Focused on Fighting Near-peer Adversaries, Stars and Stripes. https://www.military.com/daily-news/2017/10/11/army-rolls-field-manual-focused-fighting-near-peer-adversaries.html

[10] Knowles, J. (2003). Infrared Countermeasures. PC Magazine, 22(12), 87.

[11] Gale, S. F. (2017). AI vs. Hackers. PM Network, 31(4), 14-15.

[12] Future Unmanned System Technology: Legal and Ethical Implications of Increasing Automation, Joint Air Power Competence Centre (November 2016), 12. www.japcc.org

[13] Reema Bhatia (August 7, 2017). What is Machine Learning? Forbes.com. https://www.forbes.com/sites/forbestechcouncil/2017/08/07/what-is-machine-learning/#7e3e2f4979a7

[14] Future Unmanned System Technology, 20-27.

[15] Definition adapted from https://en.oxforddictionaries.com/definition/judgement

[16] Sean Kimmons (January 29, 2018). Army Secretary Directs New Team to Speed Up Next-Gen Combat Vehicle Program, Aerotechnews. http://www.aerotechnews.com/blog/2018/01/29/army-secretary-directs-new-team-to-speed-up-next-gen-combat-vehicle-program/

[17] Sharon Weinburger (March 1, 2018). The Pentagon Official Says US Hypersonic Weapons research Underfunded, Foreign policy. http://foreignpolicy.com/2018/03/01/pentagon-official-says-u-s-hypersonic-weapons-research-underfunded/

A CONVERSATION ABOUT CREATING A MISSION CRITICAL TEAM LEARNING EVENT REVIEW PROCESS (R4 MODEL)

Unidentified members of the 379th Expeditionary Security Forces Squadron demonstrate room clearing procedures during National Police Week at Al Udeid Air Base, Qatar, May 16, 2018. Throughout the week, security forces members held numerous events to highlight capabilities and competencies of the squadron. Photo by SSgt Enjoli Saunders, USAF

By Preston B. Cline, EdD

At some point in many people's careers, a coach, trainer or mentor will offer the "you suck, suck less" feedback. The feedback is accurate, but unhelpful. Most people who are underperforming know it, do not like it, and would already have improved if they knew how. Equally, most experienced instructors know what "right" looks like (tacit knowledge), but often lack the language to describe it. For example, former professional bike riders would obviously know how to ride a bike. That does not mean, however, they automatically have the skills or language to explain how to ride a bike to someone else. This is called the "Tacit Knowledge Transfer Problem."

Equally, most experienced instructors know what "right" looks like (tacit knowledge), but often lack the language to describe it.

The following paper emerged from long hours of watching the instructor cadres in Special Operations, Tactical Law Enforcement, Fire Fighting, and Emergency Medicine teams attempt to resolve the Tactical Knowledge Transfer Problem through storytelling (Bishop, 1999 and Connelly & Clandinin, 1990). These stories were told as an instructional tool and also to communicate the team's history and lessons learned. In addition, all of those teams meet the definition as Mission Critical Teams (MCTs). These are defined as small (4–12 agents), integrated groups of indigenously trained and educated experts who leverage tools and technology to resolve complex adaptive problems in an immersive, but constrained (5 minutes or less) temporal environment where the consequence of failure can be catastrophic loss (Cline, 2017). These teams operate at the edge of things; and, over the last decade, are increasingly responding to rapidly emerging, complex, adaptive problem sets (RECAPS) (Cline, 2017).

The nature of these new problem sets means many of the teams have had to transition from a contingency planning mindset to a capacity building mindset. For predictable problem sets, it is appropriate to build contingency plans. But for unpredictable problems, the team needs to have the adaptive capacity ready, within the team, to respond to whatever shows up. Building adaptive capacity requires learners and instructors to accelerate our ability to learn in real time, which means we must move beyond the "you suck, suck less" conversation.

Building adaptive capacity requires both learner, and instructors, to accelerate our ability to learn in real time ...

To this end, the following (Recognize, React, Respond and Recover) (R4) model was designed to leverage the instructor cadre's existing story telling expertise through breaking the model into a sequential story (in the gray boxes) by describing each phase of an operational or training evolution, and the theory that describes that evolution.

MCT MISSION EVENT LIFECYCLE THEORY AND NARRATIVE

Equilibrium

"Any living system ...is in a state of continual fluctuation, even when there is no disturbance. Such a state is known as homeostasis. It is a state of dynamic, transactional balance in which there is great flexibility." —Fritjof Capra (Capra, 2005)

Narrative: From 1994 to 1998, the author worked as a civilian safety officer at a Marine Research Institute in the Florida Keys. A primary responsibility was responding to terrestrial or marine incidents among the resident scientists, staff, and students. Part of this role was to take a rotational shift as the one in charge of property (ICOP). This position was the acting authority in any radical change of events.

Theory: Equilibrium is a state in which the system we inhabit is able to balance all the competing influences. At any given time, this is considered "normal". What we have to remember is: normal is socially constructed. It is a product of our culture and place in time. What was normal during a civil war, or in another country as you read this, may not be normal to you today (Skinner, 1969).

Rarely are incidents and opportunities a result of catastrophic failure, they are more often the small accumulation of connected variables that condense into a radical change event ...

Period of Condensation

"Seventy-three seconds after lift-off, one of the shuttle's fuel tanks failed, generating a rapid cascade of events that culminated with a fireball in the sky, eventually killing all the passengers on board." —Jessica Orwig (Ebeling, 2016)

Narrative: One day, my boss informed me that Sam, her nephew (and junior staffer), would take a rotation as ICOP during the upcoming holiday. Considering his inexperience, I thought this was a bad idea. But, because of the holiday, only a skeleton staff would be on the property. As I was not going anywhere, I could act as his back up. One of the few staffers who stayed was Tom, one of the harbor masters. Tom lived a pretty simple life and had an old 10-speed bike he would ride into town to restock his minimal supplies. Tom's bike was equipped with old, metal, serrated pedals. The bike had no kickstand. So, for several years, each time he laid it down on the ground, rocks would scrape the outside of the pedal, slowly shaping the metal into a sharp edge. Normally, this would not be a huge deal, but a truckload of gravel had just been spilled on the road that Tom was about to ride down.

Theory: Rarely are incidents and opportunities the result of catastrophic failure. They are, more often, the small accumulation of connected variables that condense into a radical change event, like water droplets condensing on a glass that suddenly emerge into a stream of water. It is during this period that teams need to be engaged in evidence accumulation. In the last few decades, many teams have had to transition from making achieving the 70% solution, where decisions need to be made with only 70% of the information, to facing the 700% problem where teams have 700% of the information they require and now need to determine which of that information is relevant. These are very different skill sets. Being intuitive is very different from tracking weak, but important, signals in noisy environments (Taleb, 2007).

Emergence

"The phenomenon of emergence takes place at critical points of instability that arise from fluctuations in the environment, amplified by feedback loops. Emergence results in the creation of novelty, and this novelty is often qualitatively different from the phenomenon out of which it emerged." —Fritjof Capra (Capra, 2005)

Theory: Emergence is a term used in complexity science to describe a process where a radical change event emerges from the interaction of other nonrelated entities, like discovering a new invention or the start of a pandemic (Goldstein, 1999). Every day there are variables in life that, under the right conditions, can undergo a cascade of events or failures that coalesce into a radical change event. It represents threshold, or phase transition, between the old reality and new reality in the sense that people may not yet recognize that the garbage can behind them has caught fire or that they just purchased tomorrow's winning lottery ticket.

Narrative: About mid-morning, I checked in with Sam to let him know that I was going into town to grab some supplies and would be gone for 15 minutes. As I left the property I saw Tom heading for his bike. As Tom began riding into town, in his flip flops, his tire caught a piece of gravel dropped the previous day. As soon as his tire hit the rock, it forced his front wheel sideways pitching him forward. In the process, his foot slipped off the pedal and his leg shot down onto the sharpened edge of one his pedals, lacerating his pedal artery (dorsalis pedis), the artery just on the inside of his ankle. I was in my truck about a mile away when Tom cut his ankle, but in that moment, my life along with Tom's and Sam's changed significantly. Whatever Tom, or I, intended to do that day, a radical change event caused an emergence which altered our paths. At this point, Tom could either find a way to stop the bleeding or die of blood loss.

Moment of Recognition

"The difficulty of accurate recognition constitutes one of the most serious sources of friction in war... War has a way of masking the stage with scenery crudely daubed with fearsome apparitions."
—Karl von Clausewitz (Clausewitz, 2004)

Theory: Anagnorisis (or moment of recognition) is a transformative moment within an ancient Greek theater performance when an agent makes a critical discovery that allows him or her to transition from ignorance to knowledge. These moments of recognition can happen on precognitive threat detection (Öhman, 2005) and cognitive levels through a process of pattern dissonance (Ploran et al., 2007).

Precognitive recognition is built around the automatic threat detection process in which the brain is continu-

Narrative: As I reached the institute and got out of my truck, I looked down to the white rocky marl and saw a pool of blood and bloody footprints heading in the direction of my infirmary. At this point, I didn't know that Tom was in trouble, but I had certainly detected a shift in the pattern. I started running toward the infirmary.

ously engaged (Ochsner & Gross, 2005). Unconsciously, a pattern of sensory cues (bad smell, loud sound, etc.) can exceed a threat detection threshold and trigger what is called a “startle response” (Koch, 1999), which can trigger a limbic system response. The limbic system response can be broken into trained (Saunders, Driskell, Johnston, & Salas, 1996) or untrained (fight, flight, freeze) responses (Ward, 2015). Cognitive recognition is built around the concept of “thin slicing” (Gladwell, 2007) where there exists dissonance in established patterns. It is the feeling that something is not quite right.

What the instructor cadre needs to focus on is whether learners are not recognizing the threat, or opportunity, because they are too inexperienced and do not know what they are looking at (no existing patterns), or over experienced and cannot see through the noise (too many patterns). Novices and experts require the instructor cadres to employ different strategies for learning (Wlodkowski, 2011).

The Immersion Event Horizon

“So it is that we must weather that dark time, the period of transformation when what is familiar has been taken away and the new richness is not yet ours.”
—Ram Dass (Dass & Goleman, 1990)

Theory: The event horizon represents a threshold between equilibrium and chaos. For MCTs, once the event horizon is crossed, there is no pause button; there is only performance or catastrophic failure. This is the entrance to the immersion event, or what anthropologists refer to as a “liminal” space (Van Gennep, 2011), a place “betwixt and between” time and space (Turner, 1995, p. 107) and equilibrium and chaos (Arrow, Poole, Henry, Wheelan, & Moreland, 2004). Most of the recognized decision models, which can be incredibly useful if to clarify a path forward under periods of great uncertainty, require time to think. The nature of an immersion event is such that we do not think, within those events, in the way that is commonly understood. On good days, we experience more of what Mihály Csíkszentmihályi would call a “flow experience”(Csikszentmihalyi, 1990) a period of effortless calm and focus where solutions seem to emerge as fast as the problem sets. But flow is not accidental, or spontaneous, it comes after long practice and preparation.

Narrative: As I opened the door to the infirmary, I immediately saw Tom seated in a treatment chair, with a very pale face, and looking embarrassed. Blood covered his right foot and much of the tile floor. Sam, who had little to no emergency training was experiencing an Amygdala Hijacking and was desperately trying to remember how to use the phone to call for help. At that moment I had crossed a threshold into a different reality. Time and space constricted and everything became clearer while my world suddenly narrowed to just that room. All other hopes, anxieties and plans disappeared as I dropped away and my training took cortical authority.

For MCTs, once the event horizon is crossed, there is no pause button; there is only performance or catastrophic failure.

Moment of Reaction

“Man’s last freedom is his freedom to choose how he will react in any given situation.”—Viktor Frankl (Frankl, 1985)

Theory: The moment our brain recognizes a radical change event, we cross the immersion event horizon and begin to react. In an untrained person, these responses can emerge from the limbic system as metabolically taxing defensive behaviors, such as attack, immobility, or escape (fight, flight, freeze) and may act independent of higher cognitive processes (Bracha, 2004; Öhman, 2005). The way in which we override our limbic response is to rewire it through iterative training, education, and experience that allow us to rewire or limbic system

(Barwood, 2006). A common example of this is military boot camp. Through iterative behavioral modification and stress inoculation, most people can be trained to move toward threats while carrying out tasks. Specifically, this kind of training experience builds the neural networks that allow us to construct mental models, heuristics, and patterns of normal behavior within chaotic events. Even experts, however, will occasionally encounter events in which they are untrained and may default to their primary limbic response. What the instructor cadre needs to focus on is whether learners are inexperienced and need more repetition (Bezzola, Mérillat, & Jäncke, 2012) or whether they are too experienced and need to engage in "reversal learning" (Kalyuga, Rikers, & Paas, 2012). (Reversal learning is the process of overwriting old habits, or what is sometimes called "training scars".)

Narrative: The time it takes the body to move from recognition to reaction is approximately 30 milliseconds (Koch, 1999). As soon as my brain recognizes and categorized what was happening, my medical training began to call out the checklist of the primary survey: airway (check), breathing (check), circulation (STOP THE BLEEDING!). Sam, had no such training to fall back on. So, I grabbed a handful of gauze and spun toward Tom to put pressure on the wound.

Cortical Authority Established

"Consciousness has developed the ability to override its genetic instructions and to set its own independent course of action."
—Mihaly Csikszentmihalyi (Csikszentmihalyi, 1990)

Theory: Cortical Authority is the point where the prefrontal cortex is able to assert authority (Monat & Lazarus, 1991) over the limbic system enabling people to transition from reaction to response. The limbic system cannot think abstractly and can only do one thing at a time. In complex adaptive environments, new problem sets are emerging while a person is reacting and as a result of that person's reaction. Therefore, learners need to have the experience and tactical maturity to be able to step back from reaction, organize their thoughts, respond to the larger event, and then transition back to reaction. The ability to have cortical authority is determined by how rapidly and consistently people are able to transition between reaction and response. Instructors know effective training can inoculate individuals against the type of stress they will encounter within an immersion event (Saunders et al., 1996). Instructors also know certain levels of stress increase a student's learning, but that too much stress will prevent an individual from learning (LePine, LePine, & Jackson, 2004).

Narrative: As I spun toward Tom, gauze and bandages in hand, a small voice in my head is screaming THINK! Because, this is not my first bloody patient and I am a little older than Sam, I have greater throttle control over my reaction so I can actually hear the small voice which is yelling,THINK! To help Tom and Sam, I needed my prefrontal cortex (the part of the brain capable of multitasking and abstract thinking), to regain control, or more precisely, establish cortical authority.

Moment of Response

"Between stimulus and response there is a space. In that space is our power to choose our response. In our response lies our growth and our freedom." —Viktor Frankl (Frankl, 1985)

Theory: This is the moment of choice. Where agents inject their will upon their unfolding events. The ability to respond well depends upon how well one understands the complex system within which one is nested. Since training is for certainty, and education is for uncertainty (Army, 2012), this remains an educational problem. If there are no preexisting mental models or heuristics that have been gained through training and education, operational momentum can stall. One of the predictors of how well we will respond is based on how well we diagnose the problem or opportunity being faced.

What the instructor cadre needs to focus on for inexperienced learners is expanding their joint cognitive systems (JCSs) (Potter, Woods, Roth, Fowlkes, & Hoffman, 2006) or collective intelligence (Woolley, Chabris, Pentland, Hashmi, & Malone, 2010), so the system and the rest of the team are helping learners move from reaction to response as they gain the requisite experience. For the experienced learner, in addition to refining JCSs, further developing situational awareness (Endsley, 2000) and mindfulness (Darwin & Melling, 2011; Weick, Sutcliffe, & Obstfeld, 2008) will help them avoid getting stuck in reaction mode.

Narrative: So, I paused for a brief moment as my training screamed for me to put pressure on the bleeding, and realized that if I was the person to apply pressure to the wound, I would tie myself to the patient. I also knew I needed to call for support. I was not sure if Sam could even hear what I was saying due to panic. So I spun back to Sam, shoved the bandages in his hand, pulled him over to Tom and pressed his gauze-filled hand against the wound. I looked him directly in the eyes and yelled, "Keep pressure here no matter what". I, then, elevated Tom's leg, ensured the patient could still talk to me and called 911. Once that was done, I went back and started providing direct care to Tom.

Surface Event Horizon

"But the all-clear sounds—then its okay. You take a deep breath, the stress has passed by. But real fear is a stone deep down in your chest."

—Ilya Selvinskiy (Clancy, 2002)

Theory: Individuals that cross out of an immersion event often talk about being able to take a deep breath. It is where the immediate danger has passed and the context has stabilized. It is the moment the individual, and the team, take control of the temporal environment or come to "own the clock", which is to say, they are moving from a reactive status to a proactive status.

Moment of Recovery

"And once the storm is over you won't remember how you made it through, how you managed to survive. You won't even be sure, in fact, whether the storm is really over. But one thing is certain. When you come out of the storm you won't be the same person who walked in."

—Haruki Murakami (Murakami & Gabriel, 2006)

Narrative: As soon as the paramedic arrived and started working on the Tom, I took a deep breath, like I had come up from a deep dive. Suddenly, I become aware that we made it. That we now own the clock again.

Theory: Shaun Huls, the Director of Sports Science and Reconditioning for the Philadelphia Eagles, spent 7 years as the head Strength and Conditioning Coach for Naval Special Warfare. When asked about recovery he answered:

> *"During the first decade of after 9/11, a lot of operators were damaged. It's hard for a community, like special operations, who prioritize hardship and adversity during their selection and training to see beyond those traditions as they transitioned to long-term sustained combat. The cultural disregard for wellbeing carried a heavy price tag, physically, mentally, emotionally, and intellectually when they began engaging in so many back-to-back missions. Everyone just figured the solution was to work harder and longer. What we have actually learned is that we have to put the same*

thought and intention in our recovery as we do in our training, or guys will never reach their potential as warfighter[s] or their longevity as operator[s]" (Huls, 2016).

While this may seem obvious, the challenge with this solution is that it is often counter intuitive to highly-motivated individuals who maintain very high personal standards. It requires a, fundamentally, new way of thinking about things like fatigue, error, and loss. It also proposes that all individuals have inherent blind spots to their own performance, which require someone else to identify and help resolve them (Luft & Ingham, 1961). With many operators, fatigue is a sign of weakness and the solution is to work harder, which in the long term can be really damaging. To make it even more complicated, it takes a certain amount of maturity and experience to understand the difference between lethargy, which requires motivation, and fatigue which requires recovery.

It requires a, fundamentally, new way of thinking about things like fatigue, error, and loss.

Narrative: As soon as the paramedics began packaging Tom to transport him to a hospital, fatigue washed over me as a look around at the aftermath of the trauma, sounds, smells and sights all returned. It will take a while before the adrenaline, cortisol, norepinephrine begin to burn off, but I started to see the crowd of staff that were gathered around the infirmary. I found Sam and made sure he was ok, my boss was there and needed to understand what happened. As we began to piece together the events, I found out that only about 20 minutes had passed from when I entered the infirmary.

Closure

"The trick is what one emphasizes. We either make ourselves miserable or we make ourselves strong. The amount of work is the same." Carlos Castaneda (Carlos, 1968)

Theory: MCTs are unique in that they are constantly recovering from one immersion event while preparing for the next emergence. In some cases, the immersion event can leave a lasting impact and, as a result, can take time for the operators [team] to put the event behind them. Having the team formally, or ritually (Bell, 1997), close an event provides permission for the operators to put it behind them and, at the same time, acts to highlight the operators who continue to try to make meaning of the event or trauma. The point of a formal closure is to help identify people who lack the skills to cope with the aftermath of the event and get them the resources to strengthen their coping mechanisms.

Narrative: The next few days are filled with meetings as we pieced together all the events that lead to the incident. My boss considered firing me for leaving the property when I was the back up, but decided against it. Sam removed himself from the response roster but enrolled in an emergency medical technician course. Tom was on crutches for a while and became a bit more cautious. I had dreams, for a while, about what would have happened if I had come along 10 minutes later. At the end of the week, our boss pulled us together to share the findings and declared the incident was officially over.

Period of Reconstitution: The New Normal

"Through learning we grow, becoming more than we were before, and in that sense learning is unselfish, because it results in the transformation of what we were before, a setting aside of the old self in favor of a more complex one." Mihaly Csikszentmihalyi (Csikszentmihalyi, 1990)

Theory: Teams that fail to stay on the same bearing, or recognize the changes that have occurred to each other over time, risk losing their cohesion (MacCoun, 1993). It is only after the team has experienced closure that they can truly enter a period of reconstitution. This is when the team is restored to effectiveness, commensurate with new knowledge, personnel, technology, threats, and opportunities (Staff, 2013).

Narrative: After events like Tom's injury at work, things change; not in huge ways, but in the subtle ways people react and interact. Inherently, after traumatic or significant events, people want to return to stability, that is, to the way things were. Unfortunately, that reality no longer exists. In the years that followed, even though the event was formally closed, it remained open for me until I chose to seek out support to sort it out.

CONCLUSION

Moving past the "you suck, suck less" conversation between the instructor cadres and learners necessitates developing better learning diagnostics and more precise language. If instructor cadres are able to step back from learners' mistakes and ask whether the mistakes are ones of recognition, reaction, response, or recovery, they have improved their chances of influencing behavior or identifying those who do not belong in a particular training pipeline.

If instructor cadres are able to step back from learners' mistakes and ask whether the mistakes are ones of recognition, reaction, response, or recovery, they have improved their chances of influencing behavior or identifying those who do not belong in a particular training pipeline.

It is also important to understand whether the larger issue is one of robustness, resilience, or mindfulness. Robustness is a term used to describe an operator's ability to continue performing even when subjected to external and unpredictable stressors (Anderies, Janssen, & Ostrom, 2004, p. 1) or, put another way, it is the ability to take a hit and not fall down. Resilience, on the other hand, refers to the operator's "positive adaptation in response to adversity" (Waller, 2001, p. 292; Weick & Sutcliffe, 2007) or, stated another way, is the ability to rapidly get back up after getting knocked down. Mindfulness is the ability of operators to go beyond just focusing on "what" they want to achieve and, instead, remaining "constantly engaged in updating 'how' to achieve it, given the evolving operational situation" (Darwin & Melling, 2011). In other words, instead of taking the hit and not falling down (robustness), or recovering from falling down after a hit (resiliency), mindfulness is a way to avoid the hit all together. To this end, given the leading threat to mission success, survivability, and sustainability are internal human factors, it is increasingly important to accelerate the instructor cadres' ability to make the tacit, explicit.

MODEL OVERVIEW

Figure 2 is a visual representation of the R4 model.

- **Period of Condensation:** This is a period of time, prior to the emergence of a radical change event, where variables slowly accumulate.
    - **Emergence:** Introduction of a radical change event.
- **Moment of Recognition:** This is the moment that an emergence, or radical change event, is first recognized.
    - **Immersion Event Horizon:** This marks a boundary in time and space that marks the transition between equilibrium and chaos.
- **Moment of Reaction:** This is the immediate trained or untrained re-

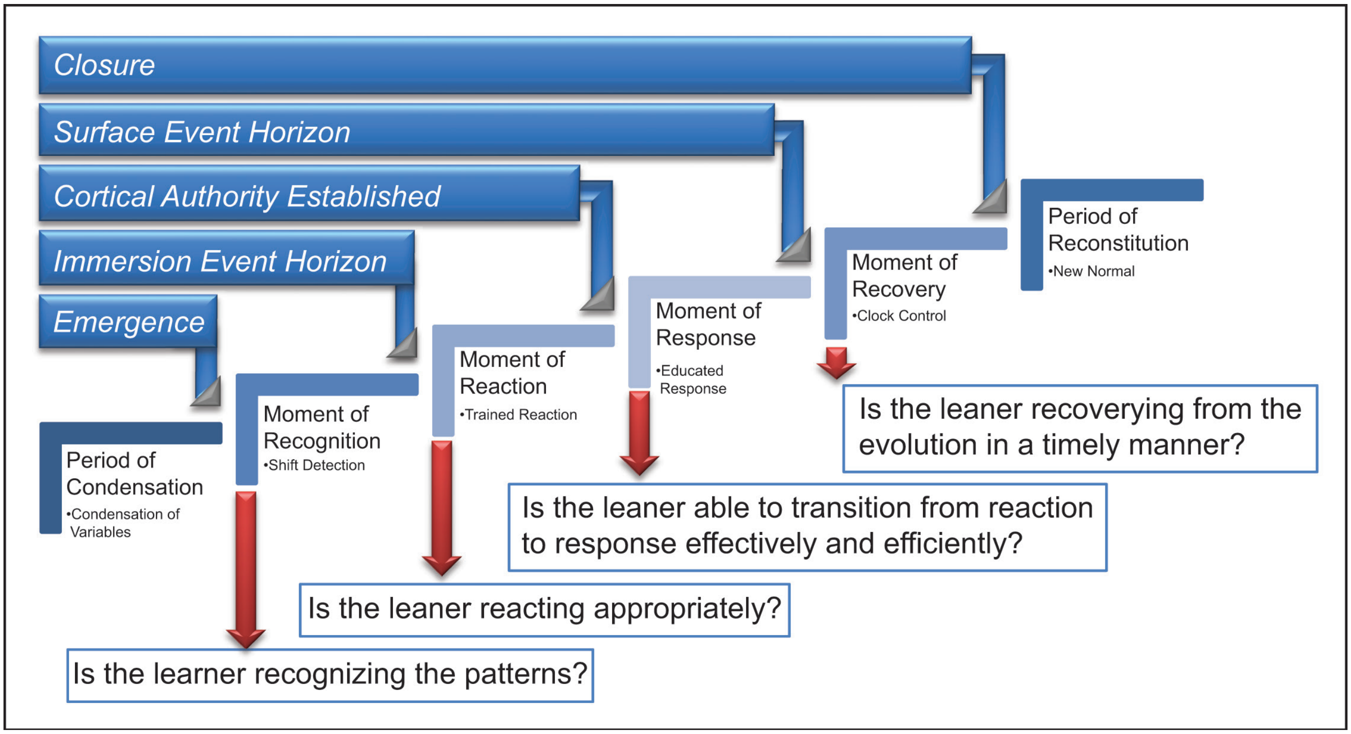

Closure
Surface Event Horizon
Cortical Authority Established
Immersion Event Horizon
Emergence
Period of Condensation
•Condensation of Variables
Moment of Recognition
•Shift Detection
Moment of Reaction
•Trained Reaction
Moment of Response
•Educated Response
Moment of Recovery
•Clock Control
Period of Reconstitution
•New Normal
Is the leaner recoverying from the evolution in a timely manner?
Is the leaner able to transition from reaction to response effectively and efficiently?
Is the leaner reacting appropriately?
Is the learner recognizing the patterns?

Figure 2. R4 Model

action to an emergence.

- ◦ **Cortical Authority Established:** This is the moment when the Prefrontal cortex asserts cortical authority over the limbic system.

- **Moment of Response:** This is the assertion of cognition over reaction.

  - ◦ **Surface Event Horizon:** This is the moment in which the event stabilizes.

- **Moment of Recovery:** This is the moment the team starts to understand the outcome of the event and begins to clean up, drink water, sit down, etc.

  - ◦ **Closure:** This is the formal recognition that the evolution is complete, which should bring a feeling of resolution or conclusion.

- **Period of Reconstitution:** This is the new normal, where the team is restored to effectiveness, commensurate with new knowledge, personnel, technology, threats and opportunities. (JP 3-35)

REFERENCES

Anderies, J. M., Janssen, M. A., & Ostrom, E. (2004). A framework to analyze the robustness of social-ecological systems from an institutional perspective. Ecology and Society, 9(1), 18.

Army, US (2012, January 4, 2012). Principles of Command and General Staff College. Retrieved from http://usacac.army.mil/cac2/cgsc/principles.asp

Arrow, H., Poole, M. S., Henry, K. B., Wheelan, S., & Moreland, R. (2004). Time, Change, and Development: The Temporal Perspective on Groups. Small Group Research, 35(1), 73-105. doi:10.1177/1046496403259757

Barwood, M. J. (2006). Breath-Hold Performance During Cold Water Immersion: Effects fo Psychological Skills Training. Aviation, Space, and Environmental Medicine, 77(11).

Bell, C. (1997). Ritual: Perspectives and dimensions: Oxford University Press.

Bezzola, L., Mérillat, S., & Jäncke, L. (2012). Motor training-induced neuroplasticity. GeroPsych: The Journal of Gerontopsychology and Geriatric Psychiatry, 25(4), 189.

Bishop, R. (1999). Collaborative Storytelling: Meeting Indigenous Peoples' Desires for Self-Determination in Research.

Bracha, H. S. (2004). Freeze, flight, fight, fright, faint: Adaptationist perspectives on the acute stress response spectrum. CNS spectrums, 9(9), 679-685.

Capra, F. (2005). Speaking Nature's Language: Prinicples for Sustainability. In M. Stone & Z. Barlow (Eds.), Ecological literacy (pp. 18-29). San Francisco: Sierra Club.

Carlos, C. (1968). The Teachings of Don Juan. A yaqui Way of Knowledge. New York: Bal-lantine Books.

Clancy, T. (2002). The sum of all fears (Vol. 6): Penguin.

Clausewitz, C. V. (2004). On war: Digireads. com Publishing.

Cline, P. (2017). Mission Critical Teams: Towards a University Assisted, Mission Critical Team Instructor Cadre Development Program. Dissertation for Doctorate in Education. University of Pennsylvania Graduate School of Education.

Connelly, F. M., & Clandinin, D. J. (1990). Stories of experience and narrative inquiry. Educational Researcher, 19(5), 2-14.

Csikszentmihalyi, M. (1990). Flow: The psychology of optimal performance: New York: Cambridge University Press.

Darwin, J., & Melling, A. (2011). Mindfulness and Situation Awareness. Retrieved from

Dass, R., & Goleman, D. (1990). Journey of awakening: A meditator's guidebook: Bantam.

Ebeling, B. (2016) 30 Years After Explosion, Challenger Engineer Still Blames Himself/Interviewer: R. Siegel. The Two Way, National Public Radio.

Endsley. (2000). Training for Situational Awareness.

Frankl, V. E. (1985). Man's search for meaning: Simon and Schuster.

Gladwell, M. (2007). Blink: The power of thinking without thinking: Back Bay Books.

Goldstein, J. (1999). Emergence as a construct: History and issues. Emergence, 1(1), 49-72.

Huls, S. (2016, 12/1/14) Personal Communication/Interviewer: P. B. Cline. Director of Sports Science and Reconditioning, The Philadelphia Eagles.

Kalyuga, S., Rikers, R., & Paas, F. (2012). Educational implications of expertise reversal effects in learning and performance of complex cognitive and sensorimotor skills. Educational Psychology Review, 24(2), 313-337.

Koch, M. (1999). The neurobiology of startle. Progress in neurobiology, 59(2), 107-128.

LePine, J. A., LePine, M. A., & Jackson, C. L. (2004). Challenge and hindrance stress: relationships with exhaustion, motivation to learn, and learning performance. Journal of Applied Psychology, 89(5), 883.

Luft, J., & Ingham, H. (1961). The johari window. Human Relations Training News, 5(1), 6-7.

MacCoun, R. (1993). What is known about unit cohesion and military performance. Sexual orientation and US military personnel policy: options and assessment, 283-331.

Murakami, H., & Gabriel, J. P. (2006). Kafka on the Shore: Vintage.

Ochsner, K. N., & Gross, J. J. (2005). The cognitive control of emotion. Trends in cognitive sciences, 9(5), 242-249.

Öhman, A. (2005). The role of the amygdala in human fear: automatic detection of threat. Psychoneuroendocrinology, 30(10), 953-958. doi:http://dx.doi.org/10.1016/j.psyneuen.2005.03.019

Ploran, E. J., Nelson, S. M., Velanova, K., Donaldson, D. I., Petersen, S. E., & Wheeler, M. E. (2007). Evidence accumulation and the moment of recognition: dissociating perceptual recognition processes using fMRI. The Journal of Neuroscience, 27(44), 11912-11924.

Potter, S. S., Woods, D. D., Roth, E. M., Fowlkes, J., & Hoffman, R. R. (2006). Evaluating the effectiveness of a joint cognitive system: metrics, techniques, and frameworks. Paper presented at the Proceedings of the Human Factors and Ergonomics Society Annual Meeting.

Saunders, T., Driskell, J. E., Johnston, J. H., & Salas, E. (1996). The effect of stress inoculation training on anxiety and performance. Journal of occupational health psychology, 1(2), 170.

Skinner, Q. (1969). Meaning and Understanding in the History of Ideas. History and theory, 3-53.

Staff, J. C. o. (2013). Deployment and Redeployment Operations.

Taleb, N. (2007). The black swan: the impact of the highly improbable (1st ed.). New York: Random House.

Turner, V. (1995). The ritual process: Structure and anti-structure: Transaction Publishers.

Van Gennep, A. (2011). The rites of passage: University of Chicago Press.

Waller, M. A. (2001). Resilience in Ecosystemic Context: Evolution of the Concept. American Journal of Orthopsychiatry, 71(3), 290-297. doi:10.1037/0002-9432.71.3.290

Ward, J. (2015). The student's guide to cognitive neuroscience: Psychology Press.

Weick, K. E., & Sutcliffe, K. M. (2007). Managing the unexpected: Resilient performance in an age of uncertainty: Jossey-Bass.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: Processes of collective mindfulness. Crisis management, 3, 81-123.

Wlodkowski, R. J. (2011). Enhancing adult motivation to learn: A comprehensive guide for teaching all adults: John Wiley & Sons.

Woolley, A. W., Chabris, C. F., Pentland, A., Hashmi, N., & Malone, T. W. (2010). Evidence for a collective intelligence factor in the performance of human groups. Science, 330(6004), 686-688.

Preston B. Cline (EdD) is the Director of the Mission Critical Team Initiative at The Wharton School, University of Pennsylvania.

SUCCESSFUL TACTICAL JOINT FIRES INTEGRATION TRAINING IN A RESOURCE-CONSTRAINED ENVIRONMENT AT FORT SILL

Senior Airman Nicholas Ward, left, and fellow 3d Air Support Operations Group Tactical Air Control Party specialist Airman 1st Class Jaron Maddox, record target threat areas to relay to pilots during a close air support exercise as part of a Fort Irwin, California National Training Center rotation, February 20, 2018. During the month-long rotation, 93d Air Ground Operations Wing units embedded with approximately 4,000 Soldiers in the largest force-on-force live-fire exercise in the world. The 93d Air Ground Operations Wing provided tactical air control party support to enhance interoperability for major combat operations downrange. Photo by SA Greg Nash, USAF

By Lt Col Nick Sargent, RA

INTRODUCTION

Fort Sill, Oklahoma hosted almost daily live artillery training on its East and West Ranges. Adjacent to West Range is Falcon Range, the busiest range in the Air Force. In fiscal year (FY) 2017, Falcon Range hosted 3,026 aircraft sorties with 561 involving joint terminal attack controllers (JTACs). This begs the question: is it possible to synchronize any of this training?

Over the past 15 years, the number of JTACs, FAC(A)s, and JFOs has increased as the number of CAS-capable aircraft has decreased.

RESOURCES

There is a perception across the United States' (US') Services and US Special Operations Command, that there are insufficient close air support (CAS) sorties available for JTAC, forward air controller (airborne) (FAC(A)) and joint fires observer (JFO) certification and qualification training to meet the minimum standards articulated in the Joint Fire Support (JFS) Executive Steering Committee (ESC) Memoranda of Agreement (MOA). When considering training beyond the minimum standards required to achieve proficiency in these perishable skills, this perceived shortfall is even greater. The statistics are plain to see. Over the past 15 years, the number of JTACs, FAC(A)s, and JFOs has increased as the number of CAS-capable aircraft has decreased. This statistical mismatch is exacerbated by a disconnect that exists when planning training among JTAC, FAC(A), JFO, and CAS-capable aircraft communities.

Coming from a much smaller military in the United Kingdom (UK), but having had the good fortune to work as an exchange officer for the United States Marine Corps (USMC) (2009–11) and US Army (2015–present), I look at the number of CAS sorties the US Services can generate for training with envy. As an outsider looking in, I suggest the US Services could be more efficient with the assets that are available. Planning is the key, the challenge is identifying common training objectives among all CAS players, airborne and ground based alike, then synchronizing the training audiences in time and space.

PLANNING IN COMBAT

Planning is a skill that has atrophied during recent campaigns, over nearly two decades in the United States Central Command area of responsibility. While CAS has been the most prevalent air mission on the air tasking order (ATO), preplanned CAS has been the exception; immediate CAS has been the norm. Where preplanned CAS existed, it was, essentially, airborne alert close air support (XCAS) waiting for a higher priority, immediate request; particularly as its ubiquitous nature and reach compensated for the limited range coverage of organic land component fires assets. There is, of course, the contention that some missions, while identified as CAS, were not CAS as defined by Joint Publication 3-09.3, *Close Air Support*. As transition back to large-scale combat operations occurs, leaders must take a more proactive approach to CAS planning. CAS, in the context of counter-land operations, will compete with air interdiction for its apportionment of resources. Counter-land operations, also, will compete with other air missions for assets (e.g., strategic attack, offensive counter air, and defensive counter air), as it will likely be the same multirole aircraft flying these missions. All this takes place in the context of a contested, or highly contested, operational environment. Proactive planning for, and requesting, CAS to compete with the other tasks the joint forces air component commander is required to accomplish, becomes a necessity.

PLANNING IN GARRISON

ATO planning in combat is driven by a multitude of factors which generate an air asset in time and space, including mission and targeting requirements. However, when planning in garrison, it is frequently a unit's maintenance schedule, established a year in advance to support a training or deployment cycle, which drives the availability of aircraft. Understanding this maintenance schedule reality, and other home-station factors, like approved takeoff and landing times, should not be overlooked by those planning CAS training from a ground perspective and can be accounted for by:

1. Identifying potential joint fires partners in the local area. (Account for flying units that are in proximity to the local range facilities) establish a network, and build relationships.)
2. Identifying common training objectives, desires, and goals based on higher headquarters' tasking and guidance.
3. (With all parties involved), simply asking "what can I offer you?"

By way of example, here is what was accomplished when these factors were considered recently at Fort Sill.

In 18 ½ weeks, the Field Artillery (FA) Basic Officer Leadership Course (FA BOLC) teaches Army second lieutenants the critical tasks required of a platoon leader, fire direction officer, and fire support officer (FSO). Since September 2016, the FSO syllabus has included JFO MOA tasks. The FA BOLC's capstone exercise, Red

preplanned CAS has been the exception; immediate CAS has been the norm.

As transition back to large-scale combat operations occurs, leaders must take a more proactive approach to CAS planning.

Leg War, sees student FSOs plan and execute Army and joint fires integration with company-level maneuvers.

After a 10-year absence, the Air Force once again routinely supports institutional training at the Army's Fires Center of Excellence, at Fort Sill. At the time of writing, there has been fighter and bomber support to four Red Leg War exercises since October 2017, with support planned for each of the 17 exercises out to the end of FY19.

During Red Leg War, student FSOs put their JFO skills to the test by requesting, adjusting, and controlling cannon artillery fires; providing target information to JTACs and FAC(A)s in support of CAS missions; and by conducting terminal guidance operations. So far, live and dry CAS missions have been executed by F16s, T38s, and B52s controlled by JTACs and FAC(A)s, and supported, concurrently, by live artillery suppression of enemy air defenses (SEAD).

HOW THIS WAS ACHIEVED WHEN RESOURCES WERE PERCEIVED TO BE SCARCE

The planning technique used the combined lines of effort, network and relationship building, identifying common training objectives, and asking "what can I offer you?" Planning was collaborative; involving all stakeholders, the training audience, and training enablers. Notably, training enablers played a critical role: Fort Sill Range Operations developed new weapon danger zones for CAS targets outside the existing target set. The two local airspace control agencies were also critical, ensuring nonexercise participants could continue training with the minimum of impact and exercise participants (air and ground) could optimize the use of local military operating areas and restricted airspace.

The foundation for planning this level of joint integration started with establishing a network of, and relationships among, joint fires players within a 200-mile radius of Fort Sill. From an Army perspective, this included the

A 2.75-inch, high explosive rocket fires during close air support drills from a UH-1Y Venom helicopter at Ban Chan Khrem, Thailand, February 21, 2018. United States Marines, with Marine Light Attack Helicopter Squadron 369 "Gunfighters", conducted close air support training to increase their readiness and proficiency with live fire shooting during Exercise Cobra Gold 2018. Exercise Cobra Gold is an annual exercise conducted in the Kingdom of Thailand for about 10 days. Seven nations participated this year. Photo by Cpl Andy Martinez, USMC

Army Multi-domain Targeting Center, US Army Field Artillery School (USAFAS), Fort Sill Range Operations, and Fort Sill Army Radar Approach Control. From an Air Force perspective, this included the 80th Flying Training Wing, 138th Combat Training Flight, and 457th Fighter Squadron. This is an ever-expanding network.

Once the network was established and relationships built, the JTAC, FAC(A), and JFO discussed aspirations and objectives for training opportunities. They identified training objectives by cross referencing the three JFS ESC MOAs and Service training regulations. Examples included:

- Live CAS attacks with JFOs providing targeting information to JTACs and FAC(A)s, while integrating live-artillery SEAD.
- Lateral and altitude separation techniques to mass fires on a common timeline using USMC SEAD procedures.
- JTAC-FAC(A) battle handover.
- FAC(A) live artillery call for fire.

Finally, having asked "what can I do for you?", the Battalion Commander of 1-30th Field Artillery (part of the USAFAS) offered a dedicated firing unit for one hour per day with 50 rounds in support of JTACs and FAC(A)s conducting call for fire training as the primary training audience. On two occasions, the 138th Combat Training Flight integrated contract CAS night sorties scheduled to support their pre-JTAC qualification Course instructor cadre work up. The result has been the establishment and continuation of some outstanding tactical joint fires integration training.

CONCLUSION

Although resources are finite, better planning can, and will, lead to better tactical joint fires training opportunities for JTACs, FAC(A)s, JFOs, and CAS-capable aircraft. This planning must account for the training schedule of each community, endeavor to synchronize these schedules where resources are available in the same time and space, and consider the common training needs of each community.

For further information on tactical joint fires training opportunities at Fort Sill, in FY19 (during Red Leg War), please contact the author. In particular, opportunities exist for CAS-capable flying units and FAC(A)s. Red Leg War dates for FY19 are in the following table.

Class Number	Class Dates
Class 5-18	15–19 OCT 18
Class 6-18	26–30 NOV 18
Class 7-18	14–18 JAN 19
Class 8-18	11–15 FEB 19
Class 1-19	18–22 MAR 19
Class 2-19	13–17 MAY 19
Class 3-19	17–21 JUN 19
Class 4-19	5–9 AUG 19
Class 5-19	14–18 OCT 19
Class 6-19	18–22 NOV 19
Class 7-19	13–17 JAN 20
Class 8-19	17–21 FEB 20

Lt Col Nick Sargent RA, UK MPEP, Chief, Joint Integration, US Army Multi-domain Targeting Center, Fires Center of Excellence, Fort Sill, Oklahoma 73503 Office: 1 580-442-6829 | Cell: 1 202-417-4840| **nicholas.p.sargent4.fm@mail.mil**

Although resources are finite, better planning can, and will, lead to better tactical joint fires training opportunities for JTACs, FAC(A)s, JFOs, and CAS-capable aircraft.

CURRENT ALSA MTTP PUBLICATIONS

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

TITLE	DATE	PUB #	DESCRIPTION/STATUS
AOMSW *Multi-Service Tactics, Techniques, and Procedures for Air Operations in Maritime Surface Warfare* **Distribution Restricted**	15 FEB 16	ATP 3-04.18 MCRP 3-25J NTTP 3-20.8 AFTTP 3-2.74	Description: This publication consolidates Service doctrine, TTP, and lessons-learned from current operations and exercises to maximize the effectiveness of air attacks on enemy surface vessels. **Status: Revision**
AVIATION URBAN OPERATIONS *Multi-Service Tactics, Techniques, and Procedures for Aviation Urban Operations* **Distribution Restricted**	27 APR 16	ATP 3-06.1 MCRP 3-35.3A NTTP 3-01.04 AFTTP 3-2.29	Description: This publication provides MTTP for tactical-level planning and execution of fixed- and rotary-wing aviation urban operations. **Status: Project Assessment**
DYNAMIC TARGETING *Multi-Service Tactics, Techniques, and Procedures for Dynamic Targeting* **Distribution Restricted**	10 SEP 15	ATP 3-60.1 MCRP 3-16D NTTP 3-60.1 AFTTP 3-2.3	Description: This publication provides the JFC, operational staff, and components MTTP to coordinate, de-conflict, synchronize, and prosecute dynamic targets in any AOR. It includes lessons learned, and multinational and other government agency considerations. **Status: Revision**
FIGHTER INTEGRATION *Multi-Service Tactics, Techniques, and Procedures for Fighter Integration* **Classified SECRET**	16 JUN 17	MCRP 3-20.7 NTTP 3-22.6 AFTTP 3-2.89	Description: This publication is a single-source set of integration standards intended to enhance commonality when operating with multiple-mission design series or type, model, and series fighter aircraft during an air-to-air mission. It establishes baseline intercept contracts with the associated communications plan. **Status: Project Assessment**
IADS Change 1 *Multi-Service Tactics, Techniques, and Procedures for an Integrated Air Defense System* **Distribution Restricted**	9 SEP 14 Change 1 incorporated 5 NOV 15	ATP 3-01.15 MCRP 3-25E NTTP 3-01.8 AFTTP 3-2.31	Description: This publication provides joint planners with a consolidated reference on Service air defense systems, processes, and structures to include integration procedures. **Status: Revision**
JFIRE *Multi-Service Procedures for the Joint Application of Firepower* **Distribution Restricted**	21 JAN 16	ATP 3-09.32 MCRP 3-16.6A NTTP 3-09.2 AFTTP 3-2.6	Description: This is a pocket sized guide of procedures for calls for fire, CAS, and naval gunfire. It provides tactics for joint operations between attack helicopters and fixed-wing aircraft performing integrated battlefield operations. **Status: 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: Project Assessment**
KILL BOX *Multi-Service Tactics, Techniques, and Procedures for Kill Box Employment* **Distribution Restricted**	18 JUN 18	ATP 3-09.34 MCRP 3-31.4 NTTP 3-09.2.1 AFTTP 3-2.59	Description: This MTTP publication outlines multi-Service kill box planning procedures, coordination requirements, employment methods, and C2 responsibilities. **Status: Current**
PR *Multi-Service Tactics, Techniques, and Procedures for Personnel Recovery* **Distribution Restricted**	4 JUN 18	ATP 3-50.10 MCRP 3-05.3 NTTP 3-57.6 AFTTP 3-2.90	Description: This MTTP publication for personnel recovery (PR) is a single source, descriptive reference guide for staffs and planners executing the military option of personnel recovery using joint capabilities. **Status: Current**
SCAR *Multi-Service Tactics, Techniques, and Procedures for Strike Coordination and Reconnaissance* **Distribution Restricted**	31 JAN 18	ATP 3-60.2 MCRP 3-20D.1 NTTP 3-03.4.3 AFTTP 3-2.72	Description: This publication provides strike coordination and reconnaissance MTTP to the military Services for conducting air interdiction against targets of opportunity. **Status: Current**
SURVIVAL, EVASION, AND RECOVERY *Multi-Service Procedures for Survival, Evasion, and Recovery* **Distribution Restricted**	11 SEP 12	ATP 3-50.3 MCRP 3-02H NTTP 3-50.3 AFTTP 3-2.26	Description: This is a weather-proof, pocket-sized, quick reference guide of basic information to assist Service members in a survival situation regardless of geographic location. **Status: 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 discusses how advising fits into security assistance/security cooperation and provides definitions for specific terms as well as listing several examples to facilitate the advising process. **Status: Current**
AIRFIELD OPENING *Multi-Service Tactics, Techniques, and Procedures for Airfield Opening* **Approved for Public Release**	18 JUN 15	ATP 3-17.2 MCRP 3-21.1B NTTP 3-02.18 AFTTP 3-2.68	Description: This publication provides guidance for operational commanders and staffs on opening and transferring an airfield. It contains information on service capabilities, planning considerations, airfield assessment, and establishing operations in all operational environments. **Status: Revision**
BIOMETRICS *Multi-Service Tactics, techniques, and Procedures for Tactical Employment of Biometrics in Support of Operations* **Approved for Public Release**	6 MAY 16	ATP 2-22.85 MCRP 3-33.1J NTTP 3-07.16 AFTTP 3-2.85 CGTTP 3-93.6	Description: Fundamental TTP for biometrics collection planning, integration, and employment at the tactical level in support of operations is provided in this publication. **Status: Revision**
CF-SOF *Multi-Service Tactics, Techniques, and Procedures for Conventional Forces and Special Operations Forces Integration and Interoperability* **Distribution Restricted**	4 APR 18	FM 6-05 MCWP 3-36.1 NTTP 3-05.19 AFTTP 3-2.73 USSOCOM Pub 3-33	Description: This is a comprehensive reference for commanders and staffs at the operational and tactical levels with standardized techniques and procedures to assist in planning and executing operations requiring synchronization between CF and SOF occupying the same area of operation. **Status: Current**
CORDON AND SEARCH *Multi-Service Tactics, Techniques, and Procedures for Cordon and Search Operations* **Distribution Restricted**	18 AUG 16	ATP 3-06.20 MCRP 3-30.5 NTTP 3-05.8 AFTTP 3-2.62	Description: This is a comprehensive reference to assist ground commanders, subordinates, and aviation personnel in planning, training, and conducting tactical cordon and search operations. **Status: Project Assessment**
DEFENSE SUPPORT OF CIVIL AUTHORITIES (DSCA) *Multi-Service Tactics, Techniques, and Procedures for Defense Suport of Civil Authorities* **Approved for Public Release**	25 SEP 15	ATP 3-28.1 MCWP 3-36.2 NTTP 3-57.2 AFTTP 3-2.67	Description: DSCA sets forth MTTP at the tactical level to assist the military planner, commander, and individual Service forces in the employment of military resources in response to domestic emergencies in accordance with US law. **Status: Revision**
EO *Multi-Service Tactics, Techniques, and Procedures for Unexploded Explosive Ordnance Operations* **Distribution Restricted**	15 JUL 15	ATP 4-32.2 MCRP 3-17.2B NTTP 3-02.4.1 AFTTP 3-2.12	Description: This publication provides commanders and their units guidelines and strategies for planning and operating in an explosive ordnance environment while minimizing the impact of explosive ordnance on friendly operations. **Status: Revision**
JATC *Multi-Service Procedures for Joint Air Traffic Control* **Distribution Restricted**	18 APR 14	ATP 3-52.3 MCRP 3-25A NTTP 3-56.3 AFTTP 3-2.23	Description: This is a single source, descriptive reference guide to ensure standard procedures, employment, and Service relationships are used during all phases of ATC operations. It also outlines how to synchronize and integrate JATC capabilities. **Status: FY19 Rescind Approved**
MILITARY DIVING OPERATIONS (MDO) *Multi-Service Service Tactics, Techniques, and Procedures for Military Diving Operations* **Approved for Public Release**	13 FEB 15	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, descriptive reference guide to ensure effective planning and integration of multi-Service diving operations. It provides combatant command, joint force, joint task force, and operational staffs with a comprehensive resource for planning military diving operations, including considerations for each Service's capabilities, limitations, and employment. **Status: Revision**
NONLETHAL WEAPONS (NLW) *Multi-Service Service Tactics, Techniques, and Procedures for the Tactical Employment of Nonlethal Weapons* **Distribution Restricted**	13 FEB 15	ATP 3-22.40 MCWP 3-15.8 NTTP 3-07.3.2 AFTTP 3-2.45 CGTTP 3-93.2	Description: This publication provides a single-source, consolidated reference on employing nonlethal weapons. Its intent is to make commanders and subordinates aware of using nonlethal weapons in a range of scenarios including security, stability, crowd control, determination of intent, and situations requiring the use of force just short of lethal. **Status: Revision**
OP ASSESSMENT *Multi-Service Tactics, Techniques, and Procedures for Operation Assesment* **Approved for Public Release**	18 AUG 15	ATP 5-0.3 MCRP 5-1C NTTP 5-01.3 AFTTP 3-2.87	Description: This publication serves as a commander and staff guide for integrating assessments into the planning and operations processes for operations conducted at any point along the range of military operations. **Status: Revision**
PEACE OPS *Multi-Service Tactics, Techniques, and Procedures for Conducting Peace Operations* **Approved for Public Release**	1 NOV 14	ATP 3-07.31 MCWP 3-33.8 AFTTP 3-2.40	Description: This publication offers a basic understanding of joint and multinational PO, an overview of the nature and fundamentals of PO, and detailed discussion of selected military tasks associated with PO. **Status: Revision**
TACTICAL CONVOY OPERATIONS *Multi-Service Tactics, Techniques, and Procedures for Tactical Convoy Operations* **Distribution Restricted**	22 FEB 17	ATP 4-01.45 MCRP 3-40F.7 AFTTP 3-2.58	Description: This is a quick-reference guide for convoy commanders operating in support of units tasked with sustainment operations. It includes TTP for troop leading procedures, gun truck employment, 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**	09 APR 15	ATP 3-52.1 MCWP 3-25.13 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**	10 NOV 15	ATP 3-55.6 MCRP 2-24A 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 *Multi-Service Brevity Codes* **Distribution Restricted**	20 JUN 18	ATP 1-02.1 MCRP 3-30B.1 NTTP 6-02.1 AFTTP 3-2.5	Description: This publication defines multi-Service brevity which standardizes air-to-air, air-to-surface, surface-to-air, and surface-to-surface brevity code words in multi-Service operations. **Status: Current**
ISR Optimization *Multi-Service Tactics, Techniques, and Procedures for Intelligence, Surveillance, and Reconnaissance Optimization* **Distribution Restricted**	14 APR 15	ATP 3-55.3 MCRP 2-2A NTTP 2-01.3 AFTTP 3-2.88	Description: This publication provides a comprehensive resource for planning, executing, and assessing surveillance, reconnaissance, and processing, exploitation, and dissemination operations. **Status: Revision**
TACTICAL CHAT *Multi-Service Tactics, Techniques, and Procedures for Internet Tactical Chat in Support of Operations* **Distribution Restricted**	24 JAN 14	ATP 6-02.73 MCRP 3-40.2B NTTP 6-02.8 AFTTP 3-2.77	Description: This publication provides commanders and their units guidelines to facilitate coordinating and integrating tactical chat when conducting multi-Service and joint force operations. **Status: Current**
TACTICAL RADIOS *Multi-Service Communications Procedures for Tactical Radios in a Joint Environment* **Approved for Public Release**	19 MAY 17	ATP 6-02.72 MCRP 3-30B.3 NTTP 6-02.2 AFTTP 3-2.18	Description: This is a consolidated reference for TTP in employing, configuring, and creating radio nets for voice and data tactical radios. **Status: Project Assessment**
TAGS *Multi-Service Tactics, Techniques, and Procedures for the Theater Air-Ground System* **Distribution Restricted**	30 JUN 14	ATP 3-52.2 MCRP 3-25F NTTP 3-56.2 AFTTP 3-2.17	Description: This publication promotes Service awareness regarding the role of airpower in support of the JFC's campaign plan, increases understanding of the air-ground system, and provides planning considerations for conducting air-ground ops. **Status: Revision**

FUTURE AIR LAND SEA BULLETINS (ALSB)

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

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

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

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

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

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

Air Land Sea Bulletin Article Requirements and Deadlines

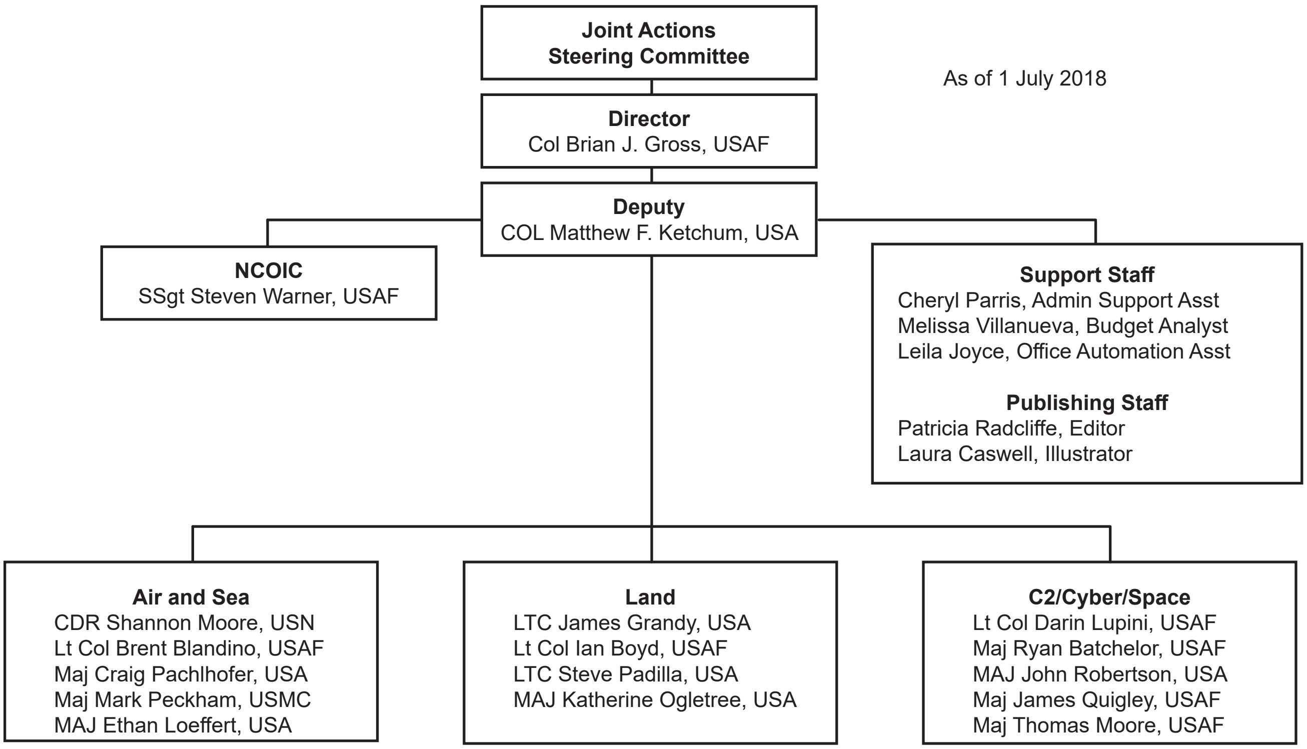
Submissions must:

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

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

Issue	Deadline	Point of Contact
Winter 2019	1 October 2018	alsaA@us.af.mil (757) 225-0967
Summer 2019	1 March 2019	alsaB@us.af.mil (757) 225-0964
Winter 2019	1 October 2019	alsaC@us.af.mil (757) 225-0903

ALSA ORGANIZATION



As of 1 July 2018

Joint Actions Steering Committee

Director
Col Brian J. Gross, USAF

Deputy
COL Matthew F. Ketchum, USA

NCOIC
SSgt Steven Warner, USAF

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

Publishing Staff
Patricia Radcliffe, Editor
Laura Caswell, Illustrator

Air and Sea
CDR Shannon Moore, USN
Lt Col Brent Blandino, USAF
Maj Craig Pachlhofer, USA
Maj Mark Peckham, USMC
MAJ Ethan Loeffert, USA

Land
LTC James Grandy, USA
Lt Col Ian Boyd, USAF
LTC Steve Padilla, USA
MAJ Katherine Ogletree, USA

C2/Cyber/Space
Lt Col Darin Lupini, USAF
Maj Ryan Batchelor, USAF
MAJ John Robertson, USA
Maj James Quigley, USAF
Maj Thomas Moore, USAF

ALSA JOINT WORKING GROUPS

Date	Publication	Location	Point of Contact
13-16 Aug 18	TAGS	Joint Base Langley-Eustis, VA	C2, Space and Cyber Branch alsaC@us.af.mil
21-24 Aug 18	AOMSW	Joint Base Langley-Eustis, VA	Air and Sea Branch alsaA@us.af.mil
27-30 Aug 18	AUO	Joint Base Langley-Eustis, VA	Air and Sea Branch alsaA@us.af.mil
11-14 Sep 18	TAGS	Joint Base Langley-Eustis, VA	C2, Space and Cyber Branch alsaC@us.af.mil
11-14 Sep 18	DSCA	Joint Base Langley-Eustis, VA	Land Branch alsaB@us.af.mil
25-28 Sep 18	AUO	Joint Base Langley-Eustis, VA	Air and Sea Branch alsaA@us.af.mil
15-19 Oct 18	Cordon and Search	Joint Base Langley-Eustis, VA	Land Branch alsaB@us.af.mil
16-19 Oct 18	DSCA	Joint Base Langley-Eustis, VA	Land Branch alsaB@us.af.mil
12-15 Nov 18	Forensics	Joint Base Langley-Eustis, VA	Land Branch alsaB@us.af.mil
14-15 Nov 18	Fighter Integration	Nellis AFB, NV	Air and Sea Branch alsaA@us.af.mil
All Dates are Tentative			

ALSA MISSION

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

ALSA is a joint 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 Combat Development Command, Navy Warfare Development Command, and Headquarters, Curtis E. LeMay Center for Doctrine Development and Education.

VOTING JASC MEMBERS

Maj Gen Michael D. Rothstein

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

MG Douglas C. Crissman

Director, Mission Command Center of Excellence

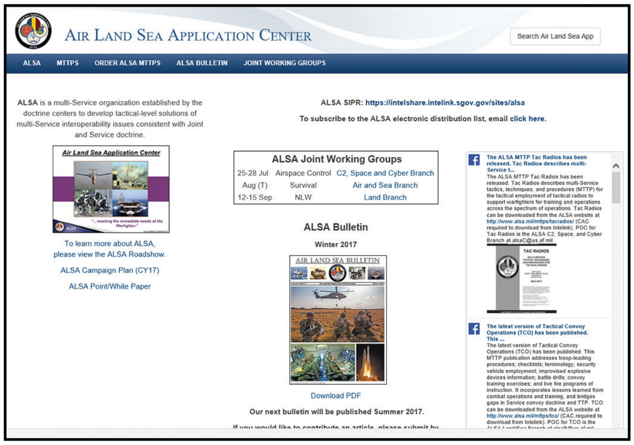
RADM M. A. Hitchcock

Commander, Navy Warfare Development Command

BGen James H. Adams

Director, Capabilities Development Directorate, Marine Corps Combat Development Command

ONLINE ACCESS TO ALSA PRODUCTS



AIR LAND SEA APPLICATION CENTER
Search Air Land Sea App
ALSA
MTTPS
ORDER ALSA MTTPS
ALSA BULLETIN
JOINT WORKING GROUPS

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

Air Land Sea Application Center
"...meeting the immediate needs of the Warfighter."

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

ALSA Campaign Plan (CY17)

ALSA Point/White Paper

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

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

ALSA Joint Working Groups

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

ALSA Bulletin

Winter 2017

Download PDF

Our next bulletin will be published Summer 2017.

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

The ALSA MTTP Tac Radios has been released. Tac Radios describes multi-Service t...

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

The latest version of Tactical Convoy Operations (TCO) has been published. This ...

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

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

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

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

ALSA CENTER
ATTN: ALSB
114 ANDREWS STREET
JOINT BASE LANGLEY-EUSTIS, VA
23665-2785

OFFICIAL BUSINESS

Scan Me

Air Land Sea Application Center

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

http://www.twitter.com/ALSA_Center

Air Land Sea Application Center
ALSA