The Integrated Tactical Network

Pivoting Back to Communications Superiority

Maj. Matthew S. Blumberg, U.S. Army

While U.S. forces were focused on Iraq and Afghanistan over the past two decades, our nation's most dangerous adversaries set their sights elsewhere. Russia, China, North Korea, and others prioritized investments in advanced communications equipment, cyber capabilities, and exploitive electronic warfare technologies. At the tactical level, the advances made by those adversaries cast serious doubts on whether the U.S. Army has maintained its technological or communications edge. Because the Army's current and future combat systems, munitions, and mission command are interwoven with and heavily dependent on tactical networks, there is justified concern regarding its ability to maintain the tactical advantage. This is not a new phenomenon but is repeated in historical studies and assessments, including the 2018 National Defense Strategy Commission's *Providing for the Common Defense*.[1] Currently, the U.S. Army's ability to apply tactical communications is far from ready for the next major war and is in urgent need of transformational change.

Maj. Matthew Blumberg, U.S. Army, is a signal officer serving as the group communications officer for the Asymmetric Warfare Group, Fort Meade, Maryland. He holds a BA from Stony Brook University and MS and MBA degrees from the University of Maryland. He has been assigned in strategic communications, light infantry, Stryker, special operations aviation, combat training center, and airborne units. His past overseas assignments include Korea and Germany with multiple operational and combat tours to the Pacific, Europe, and Middle East.

Future tactical communications must increase network mobility; decrease reliance on satellite services; make greater use of terrestrial and aerial relays and transport; and significantly reduce size, weight, and power requirements. This approach demands a simultaneous blending of multiple layers of communication transport and integration of consolidated mission data and network services. Systems should be technically and procedurally interoperable with joint, interagency, intergovernmental, and multinational (JIIM) partners and create a wholly integrated tactical network (ITN). When implemented, the ITN construct must be technically flexible, resilient, and adequately robust for all foreseeable future operations and programmatically sound for future acquisitions. If properly resourced, prioritized, and executed, the new network would mitigate threats and provide excellent expeditionary and on-the-move (OTM) communications.

Going forward, the ITN efforts should parallel Department of Defense and joint force requirements for collective benefits. Currently, the joint staff J6 (command, control, communications, and computers/

A forward observer with the 508th Parachute Infantry Regiment, 82nd Airborne Division, uses integrated tactical network components 24 January 2019 during a live-fire exercise at Camp Atterbury, Indiana. (Photo courtesy of the U.S. Army)

cyber) is working on the requirement with the Army's Futures Command, the Network Cross-Functional Team and other cross-functional teams, select Army program executive offices (PEOs), and other stakeholders. Early indications are positive, with initial requirements established through joint capabilities documents. Separately, the Army's vice chief of staff pushed a directed requirement in June 2018 that validated the ITN's operational need.[2]

Overall, the proposed ITN architecture is fundamentally sound and offers significant advantages over existing tactical communications. However, the current ITN concept is plagued by an extreme lack of awareness across the Army and the joint force. Additionally, there is overconfidence and there are incorrect assumptions that technical solutions can solve nonmateriel doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) deficiencies.

What Does History Tell Us?

The tactical Army habitually relies on satellite-based communications for beyond line-of-sight (BLOS) connectivity. This reliance severely degrades the training, expertise, and equipment required to operate when satellite services are not available and to seamlessly communicate across BLOS expanses during expeditionary and OTM operations. Communications equipment is often complex, not operator friendly, and typically requires specific training for initial configuration, real-time changes, and performance of basic functions. When new technology is problematic or too complex, it is routinely pushed aside, put in storage, or not used to its full potential. Many soldiers expected to operate new communication systems are neither communicators nor are they leaders. A simple solution for the force does not translate into a simple solution for those working the problem.

"When new technology is problematic or too complex, it is routinely pushed aside, put in storage, or not used to its full potential. Many soldiers expected to operate new communication systems are neither communicators nor are they leaders. A simple solution for the force does not translate into a simple solution for those working the problem."

Baseline Requirements for Brigade Combat Team Communications

The military must understand our operational environment. High-intensity, large-scale combat does not promote stationary operations but favors at-the-halt and OTM operations in a decisive action environment. A commander's critical communication requirements must factor the technical and practical limitations of the most demanding parts of conflict, which are at-the-halt and OTM operations in a contested environment. Based on this notion, there are specific requirements that provide brigade combat team (BCT)-and-below commanders with the information they need when they need it.

First, tactical networks must enable synchronous and asynchronous, real-time, and interoperable communications. Synchronized systems rely on network timing, are critical for digitally networked systems (mesh networks), and help mitigate external threats. Asynchronous network attributes allow isolated systems (and units) to rejoin the larger network when timing is lost. Real-time, low-latency links are critical for mission data and a fire mission's immediate and automated information exchange.

Additionally, future conflict will require more than the U.S. Army. Its ability to operate in a joint or coalition environment, no matter the scale, requires interoperable systems. Interaction with anyone, at any time, with little delay, requires technical interoperability. The Army must also make certain that procedural and personal interoperability does not negate its technical ability. During operations, interoperability efforts should be prioritized as (1) Army-to-Army, (2) Army-to-joint, and then (3) Army-to-coalition (order is mission dependent). However, to drive innovation and "muscle memory" during training, commanders can deliberately flip the priorities (coalition, then joint, then Army).

Next, commanders should establish precedent where only mission-critical services are allowed. This does not mean the Army must limit bandwidth-intensive services or video feeds. Instead, the Army must prioritize what mission

command and intent require, not luxuries. Luxuries during combat operations often include social media and associated video streaming. Limiting these luxuries will improve network performance and directly reduce a BCT's operational risk. BCT networks must be configured to limit luxuries, to alleviate congestion, and to isolate (in addition to geographic isolation) when necessary to mitigate internal and external threats.

External communications should be limited with sparing support or contingency higher headquarters communications. Exceptions to this network concept include situational awareness (SA) and position location information (PLI), fires, and intelligence data. Commanders must determine the right mix for sharing of SA and PLI data, and to specific levels. A conservative approach will limit the effectiveness of adversarial offensive actions after friendly information compromise. On the contrary, poor or nonexistent planning can lead to significant risk after system compromise.

The SPM-622 Squad Power Manager will reduce power limitations and the battery weight carried by dismounted soldiers by enabling military forces to manage and prioritize power use for various electronics devices—including portable radios, GPS systems, medical and explosive ordnance disposal equipment, and computers—from any available power source. (Photo courtesy of Revision Military)

Finally, baseline communication capabilities must be identified and units should be fully proficient in their use. Based on direct observations of armor, Stryker, and infantry BCTs at multiple training centers and during multiple combat tours, the three capabilities are highlighted with a requirements-driven mindset. The list roughly parallels the three key elements of interoperable communications identified by retired Lt. Gen. Ben Hodges, the U.S. Army Europe commander from 2014 to 2017.[3] Each capability should be encrypted to at least Advanced Encryption Standard 256 and should be interoperable across the Army and JIIM community.[4]

Voice via radio. Voice communications have been, and should always be, the bedrock of tactical communications. They must be seamless, BCT-wide, and at minimum down to team level. The ability to communicate in real-time, with full mobility regardless of terrain, is critical. While units are often proficient using line of sight (LOS) radios, they are just as often inept when using anything except tactical satellite communications (TACSAT) for beyond-line-of-sight (BLOS) communication. The ability to bounce or relay transmissions for BLOS capability includes TACSAT, high frequency (HF), and terrestrial and aerial relay. Types of relays are aerial, which includes unmanned aircraft systems (UASs) tethered drones, manned rotary and fixed-wing aircraft, aerostat, and high-altitude balloons, each with persistent versus nonpersistent capabilities; mobile (vehicle-based); dismounted; and Radio over Internet Protocol (RoIP).

Common operating picture. Tactical communication must provide for a common operating picture (COP) that is accessible, shareable, and relevant. Preferably, COPs would include a topographic map with personnel and event PLI, enduring messages and chat functionality, and real-time overlays with over-the-air exchange. Ideally, BCTs only use one mission command or COP system. Too often, however, units use multiple systems for perceived improvements to overall SA and as a last-resort solution for interoperability and integration failures. Multiple systems create confusion, increase lag, invite errors, and give inaccurate and questionable data to the commander.

Fires and mission data. Fires and mission data must be seamlessly exchanged between all partners,

Soldiers from the 3rd Brigade Combat Team, 82nd Airborne Division, train on a new inflatable satellite communications system known as Transportable Tactical Command Communications on 21 February 2020. The system enables expeditionary mission command and situational awareness during evolving battles. (Photo by Amy Walker, PM Tactical Network PEO C3T public affairs, U.S. Army)

with emphasis on air-to-ground integration and joint, special operations forces (SOF), and coalition interoperability. To meet this requirement, communications systems must be low latency, digital and analog, and BLOS capable. Real-time video feeds are highly beneficial but not an absolute requirement.

BCT Communications: Looking in the Mirror

Regardless of BCT, variations exist in communication support, effectiveness, and resident expertise. For the few exceptional units, success is dependent on unit culture, supportive leadership, and collective efforts. Low-performing unit leaders often profess the inadequacy of their communications equipment. This rationale is how many leaders explain their unit's technical difficulties and lack of effective communications. This notion is commonly shared by many leaders within the Signal Corps; this is important because it is highly inaccurate.

Advantages of technology. From a technical perspective, Army BCTs have been well equipped with communications equipment for the counterinsurgency (COIN) environment since their inception. The Army has taken care to keep current technology within its ranks, from the Warfighter Information Network-Tactical (WIN-T) program for network transport to incremental capability set modernization efforts for tactical radios.[5] However, despite the Army's best materiel solutions, a lack of expertise, common knowledge, nonoperational equipment, and missing components often underlie poor performance. While some BCTs are very capable and may be fortunate enough to receive guidance from an extraordinary division signal officer, many BCTs only use their communications equipment for basic functionality, or not at all. If units do not fully understand and make use of their current communications equipment, how will they benefit from new equipment? If units continue to receive the

latest and greatest technology but continually neglect the equipment's full potential, the evidence points to a problem with our personnel, not the technology. Here are a few visible and recurring examples:

HF radio. Enough HF radio equipment is allocated to BCTs to provide BLOS capabilities to the brigade and battalions, with some units having systems down to the company level. However, minimal use of HF occurs at combat training centers (CTCs) and during home-station training. Units are routinely unable to set up an area of operation (AO)-wide voice or data network. While some units are adept with HF, and its use is trending upward, success is often isolated across BCTs and their headquarters. Deficiencies in the use of HF radio equipment include

- an inability to understand and implement the systems;
- small allocations of HF compared to very high frequency and satellite radios;
- failure to maintain historical knowledge;
- lack of HF-specific training and field craft;
- failure to properly account for, issue, and maintain radio cables, accessories, and software; and
- a lack of leader emphasis requiring HF use.[6]

Wideband technology and higher data rates are now possible with HF. New radios are BLOS voice and data assets as capable as most OTM satellite terminals but without some of the vulnerabilities or airtime cost. Wideband HF radios, such as the PRC-160, should be rapidly incorporated as replacements to legacy PRC-150 radios. *HF radios have been in use since prior to World War II but quickly fell out of favor with the introduction of satellite radios.*

Legacy, mesh networking radios. Mobile, ad hoc networking (MANET) radios combine mobility (e.g., mounted, dismount, aerial), a flexible architecture (e.g., point-to-point, point-to-multipoint), and range extension via radios acting as repeaters. BCTs rarely integrate their MANET radios for anything other than basic voice functionality. Moreover, many units urgently request approval and funding for cutting-edge MANET radios (e.g., PRC-148c, PRC-163, TSM 900/950, MPU5), despite existing, capable radios. When existing radios have long been neglected for data networking, why would the receipt of new equipment suddenly change the existing mindset and standard practice? To be fair, significant technological improvements with newer MANET radios include increased total node count, greater bandwidth, improved network management, and more capable waveforms. The increased data throughput and relay capability of newer MANET radios should be the foundation for the BCT-and-below tactical network. However, this does not negate the fact that existing radios are capable but are routinely underutilized or collect dust on a shelf.

Shadow UAS. The BCT-level Shadow UAS carries payload slots for two common BCT MANET radios. These radios provide aerial voice and data relay from thousands of feet above ground level. When compared with standard ground relay sites, aerial platforms reduce equipment and personnel overhead, lower the risk of compromise, greatly increase coverage area, and improve unit security. Despite the Shadow's prioritization for intelligence, surveillance, and reconnaissance missions, relays can be used without impact. Unfortunately, Shadow teams and communicators rarely work together to implement these relays.

Tactical Operations Center Intercom System (TOCNET). Army battalions and brigades outfitted with most increments of WIN-T have TOCNET equipment, including the E-Micro Central Switching Unit. The unit is an RoIP server that allows geographically isolated areas to connect local LOS radio traffic, through BLOS network connectivity, to distant AOs. Radio use is also extended to computer users with computer software. Despite BCTs being equipped with RoIP capabilities, units use their TOCNET for basic, single-hub functionality (like a local intercom but through isolated crew access units) or not at all. Even worse, they neglect systems and request other RoIP capabilities to fill the requirement.

Planning shortfalls. The BCT standard for communications planning is a PACE plan that develops a primary (P), alternate (A), contingency (C), and emergency (E) method. The plan's premise is to have multiple redundancies through different transport options. Units rely on their primary method until it is jammed or suspected of compromise and then shift to an alternate method. Within COIN, a single transport method for radio or network traffic is typically adequate. However, with the rise of more capable adversaries and advanced jamming and detection threats, the current PACE method for tactical communications is

no longer suitable. The future solution involves multiple, simultaneous transport methods that will make communications more agile, adaptive, and resilient to threats. ITN use should include the necessary transport required for all missions into a single plan (e.g., LOS, BLOS, spread spectrum, bandwidth needs, urban and subterranean factors). The goal for tactical communications should be an automated integration of the existing radio and network transport options into a single, unified transport. Based on current and future threats, this approach negates most of the unit-level and AO-wide jamming.

Ignoring layered communications. The proliferation of highly capable satellite communications (SATCOM) to lower echelons causes BCT leaders to ignore the benefits of a layered communications architecture. As such, BCTs lose the expertise to communicate in the absence of SATCOM, often overlook system limitations, and place less priority on prudent planning and training. This is a serious vulnerability. In a future peer fight, combat operations will likely lead to degraded or denied satellite services, with the few hardened and jam-resistant satellites prioritized to higher echelons. The recent trend is toward smaller, less costly, highly proliferated, and coherent low-earth orbit satellites. Some leaders argue that this approach is better suited for the future and reduces overall risk. There is a solid foundation for this argument; however, there are inherent risks with interconnected and meshed networks. Meshed satellite constellations are no different and care must be taken to help mitigate these new risks.

Training shortfalls. There are distinct differences between a BCT's combat operations and training. Specifically, because greater resources are available for deployed forces, the most capable equipment is often the norm in combat operations but not available for training. Adding to the equipment disparity, the Army's adaptation to the future fight (as outlined in Field Manual 3-0, *Operations*) cannot be fully evaluated based on its current operations in a COIN environment. Moreover, if decisive-action training events and CTC rotations are not realistic, or the threat is "throttled down" to ensure a baseline training value, BCTs will not accurately predict whether they are ready for future combat. Future training objectives must take into account the shifting operational environment, where technical considerations will likely gain prominence (electronic warfare, electromagnetic signatures, information operations, unmanned systems, offensive and defensive cyber, and the communication systems that connect everything).

Transformational Approach: ITN Background, Strategy, and Basics

In January 2016, the Army first published Army Techniques Publication (ATP) 6-02.53, *Techniques for Tactical Radio Operations*.[7] This publication was a major doctrinal shift that indicated future change, but it was unknown to most of the Army. The ATP introduced the concept of the integrated tactical networking environment as the successor network to the lower tactical internet and combat net radio, and it was planned for use down to the lowest tactical level. The plan focused on the integration of MANET radios with existing tactical networks. As updates to doctrine continue, the February 2020 ATP 6-02.53 revises the terms upper tactical internet (Upper TI) and lower tactical internet (Lower TI) with upper tier and lower tier. Additionally, the term "integrated tactical networking environment" is now "tactical networking environment."[8]

At the BCT, the ITN seeks to bridge networks into a unified network having three parts: applications, services, and transport. The transport forms the ITN foundation and relies on emerging waveforms and legacy systems from command posts to the tactical edge of the battlefield. The network is then refined across a flattened, lower-tier architecture. Based on the February 2020 ATP 6-02.53, the lower tier is from the individual soldier to brigade and the upper tier consists of multi-channel satellite systems from battalion to corps.

The lower tier slants heavily toward LOS-focused MANET radios paired with cellular end user devices (EUDs, e.g., 4G/5G/BT/Wi-Fi) primarily running Tactical Assault Kit software. EUDs are simply cellular phones or tablets paired with special software. While MANET radios can operate independently of the EUD, they gain SA and data tools when paired. The lower tier BLOS capabilities include HF, TACSAT, and future iterations of OTM and at-the-halt SATCOM. Despite long-held notions concerning SATCOM advantages, the most capable equipment for tactical network transport is a terrestrially based MANET mesh. To link air assets, the ITN includes Link-16 and other radios capable

of enhanced SA through tactical data link networks. When wideband HF is integrated, BCTs will further benefit from reductions in satellite dependency and improved BLOS redundancy.

Connecting the lower and upper tiers are network extensions and augmentations that enable LOS MANET radios to behave in BLOS ways. Examples include the relay capability inherent to MANET radios, cellular EUDs and their paired MANET radios, terrestrial and aerial platforms for elevated MANET relays, and RoIP via SATCOM.

The tactical infrastructure portion of the ITN provides the physical connection between the tactical transport and tactical applications (software). Gateways and hubs provide modularity and consolidate, translate, and redistribute data. Tactical, cross-domain solutions connect dissimilar data and radio networks on varying classification levels. Finally, unmanned and tethered drones provide the platform for LOS-to-BLOS aerial extension. Every component is mission critical and increases JIIM interoperability and accessibility.

Overall, the network must be singular but modular, fluid, and deployed with a depth of simultaneous and varied waveforms. A singular network reduces overhead, provides ease of access, and helps reduce variance within the COP. A modular network allows for quick pivots to new technology through standardization and open architecture. Spread spectrum, with multiple and simultaneous waveforms (transport methods), offers the best protection against jamming and provides increased bandwidth.

Standardization of a secure but unclassified (SBU) network enhances JIIM and coalition interoperability

Sgt. Devon Cloud and Sgt. 1st Class Joseph Wambach, members of the 1st Stryker Brigade Combat Team, 25th Infantry Division, Tactical Electronic Warfare Team, and civilian contractor Don Behr use an integrated system of sensors 15 January 2017 on a hilltop overlooking the brigade tactical operations center to survey the electromagnetic spectrum and identify frequencies of interest at the National Training Center, Fort Irwin, California. (Photo by Sgt. Michael Spandau, U.S. Army)

U.S. and coalition soldiers monitor the tactical network and the common operational picture at the Coalition Network Operations and Security Center 3 May 2018 during Joint Warfighting Assessment 18.1 at Grafenwöhr, Germany. The Global Agile Integrated Transport network design enables units in theater and/or at home station to share mission command, network operations, and the coalition common operating picture. (Photo by Amy Walker, PM Tactical Network PEO C3T public affairs, U.S. Army)

and accessibility at the lower tier. Because SBU network security is commercial encryption in lieu of military-grade encryption, SBU only requires commercial equipment. This new standard allows for connectivity to partners without Type 1 communications security or without large quantities of Type 1 equipment. Users connect to SBU networks with Type 1 military radios (with Type 3 compatibility) and commercial radios, cellular phones, and network devices with Advanced Encryption Standard 256 or stronger encryption.[9]

ITN Concerns and Future Focus Areas

Despite some ITN evaluations from 2016 to late 2018, ground-truth assessments by Asymmetric Warfare Group operational advisors and signal, electronic warfare, and intelligence personnel highlight the following enduring and significant challenges.[10]

Scalability. Despite the tangible benefits of the ITN, there are valid concerns for the equipment's scalability from SOF to the conventional force. Specifically, the overall concept and equipment might not be technically or intellectually scalable to the conventional force's size or resident expertise. For the past decade, ITN-like equipment has been in the SOF community, with most lessons learned coming from these units. However, SOF units are vastly different than conventional units, and certain SOF characteristics are likely contributors to ITN effectiveness. Such characteristics include higher personnel aptitude requirements, the knowledge base of specially selected

and trained military members, and large contingents of communication-focused contractors and government civilians. Additionally, leaders who transit from SOF to conventional units often expect similar capabilities and levels of expertise.

Next, early ITN use included small-to-midsize SOF teams with a relatively small number of MANET radios when compared to conventional Army requirements. Currently, the most capable technology only allows for simultaneous operation of approximately 300–350 MANET radios. If too many radios connect to the network, severe degradation or network failure could occur. Based on a conservative estimate of 400–450 MANET radios per BCT, gaining units need to rethink radio allocation, acquire more capable radios, or create properly sized and aligned subnetworks (unit and internet protocol schemes).

Finally, no matter how simple we attempt to make operator and user experience, the ITN equipment still requires expert-level conceptual, technical, and system-specific knowledge to engineer the network's complexity. Even with future systems, there should only be so much automation built into the foundation. Currently, the Signal Corps has an ongoing occupational specialty consolidation effort that is leading to well-versed and capable communicators. However, there should be a conscience effort that any materiel improvements made are paralleled in scope by similar increases to the nonmaterial DOTMLPF-P.

Program management and support. As of this article's creation, no consolidated Army or joint program of record (PoR) exists for the ITN. This is both positive and negative. It is positive because PoRs are notoriously slow to adapt and keep pace with technological progress. However, not having a PoR is detrimental because they are relatively proficient with back-end support and developing training programs, and they have established organizational ties to the Army's centers of excellence.

Currently, the ITN is an assortment of government-off-the-shelf, commercial-off-the-shelf, small equipment fieldings, and individual PoRs that are scattered across the Army and the Department of Defense. There is inconsistent, delayed, or withheld information and unpredictable equipment refresh, reset, and life cycles despite stakeholder efforts. By late 2018, most ITN technical support was provided by equipment vendors and contractor teams out of Army program executive offices such as PEO Soldier; PEO Intelligence, Electronic Warfare, and Sensors (PEO IEWS); and PEO Command, Control, and Communications Tactical (PEO C3T). The current timeline puts the initial fielding of the ITN capability set equipment in late 2020.

Limited equipment equals limited effectiveness. Direct observations from CTCs, large-scale equipment evaluations, and on-hand testing reveal the limited effectiveness of select ITN equipment when deployed in limited quantities. For example, if a battalion's number of MANET radios is issued to an entire BCT, the limited equipment is routinely scattered to key leaders. Filling piecemeal across the BCT also spreads individual radios past their LOS capability. This cuts off the rest of the mesh network and negates the intended operational gain. MANET radios are not complementary to legacy systems, though they are compatible. Operating MANET radios on legacy waveforms nullifies the substantial benefit the radios can provide. This is no different than using existing equipment for basic functionality. The most advantageous distribution is to fill the entire unit. If equipment is limited, fill one subordinate unit at a time.

Rough estimates for outfitting an entire BCT with ITN equipment ranges from $200 million to $400 million. Even limited to just MANET radios, a full BCT order of kits with installation and support could exceed $20 million to $30 million. Currently, these fiscal constraints and production capacity limit quick fielding of the ITN. However, certain equipment provides gap-filling advantages to both the ITN and legacy systems. As mentioned, not enough radios equals little-to-no gain. Until that level of funding is available, a more practical choice is technology that is both complementary and legacy compatible, such as a twin-radio capable, tethered drone. The organic ability to quickly and persistently extend terrestrial communications through aerial platforms, in lieu of vulnerable, costly, and latent SATCOM, makes considerable sense. Depending on capability and model, current prices range from $80,000 to $250,000 per kit, which includes training, spares, and initial warranty. At this moment, some current models might already be designated

as government-off-the-shelf and would provide for easier acquisition and support.

User equipment power requirements and limitations. For dismounts, the use of EUDs, always-on MANET radios, GPS and video receivers, tactical cross-domain solutions, and other ITN devices significantly increase the power requirements at the tactical edge. Depending on the requirement, ITN equipment for only one person could include a Type 1 radio, Type 3 radio for SBU, handheld Link-16 radio for air-to-ground integration, an EUD, a tactical cross-domain solution, and a Defense Advanced GPS Receiver (DAGR). Dismount ITN components will require improved personal power generation, more capable batteries, and power distribution kits.

Lack of adept brigade-level, or additional-skill-identifier trained, ITN subject-matter experts. The established BCT expert for radio networking is the brigade network technician warrant officer (255N).[11] Despite the requirement, the 2017 course map for the 255N warrant officer basic course provided only seventy-two of the 952 hours (roughly 7.5 percent) for combat net radio and transmission, spectrum, and OTM planning.[12] As the future BCT network shifts to the ITN, so too should the 255N basic course. The first step is to reconsider the importance of ITN and the proper ratio for training requirements. Step two is informing BCT leaders and signal personnel that the 255N is the Army-designated subject-matter expert. Step three is the creation of a separate additional-skill-identifier-producing course for ITN, or adaptation of an existing course (such as Signal Digital Master Gunner), that would provide BCTs with the requisite expertise.

Lack of standardized training for leaders, users, and communications personnel. While select units create training plans for their ITN equipment, there is widespread misinformation, misaligned standards, variance by type of unit, and a severe lack of formalized training. Too often, units simply send their communications personnel to the training and not the leaders or primary users of the equipment. Training on communications equipment is rarely a priority in BCTs. If this approach continues with the ITN, BCTs will be unable to communicate and will be tactically ineffective in their conduct of mission command.

Increased vulnerabilities of a MANET architecture. One of the advantages to legacy voice transmission is that users can use brevity to limit outgoing radio frequency (RF) signatures and reduce the likelihood that an enemy can intercept, jam, or locate friendly forces. However, MANET radios use an always-on network. This creates a constant RF signature that enemy forces can use to locate friendly forces. Currently, users can help reduce the risk of RF or electromagnetic signature detection through terrain masking, lowering radio power levels, using directional antennas or beam forming from multiple omnidirectional antennas, or obfuscation and deception with properly placed decoys or coherent antenna arrays.

The Way Forward

There is justified concern that our future operational effectiveness will be limited by our ability to maintain tactical communications and network-dependent combat systems. Feeding this concern is an obvious increase in adversarial threats, historical credence that past standards and performance are likely indicative of future performance, and a debatable approach where advanced technology is partially meant to mitigate deficient human capital and expertise.

We must continue to outfit our tactical forces with the most advanced and capable equipment. The ITN equipment and construct is the technical solution to support JIIM interoperability and mitigate adversarial threats. While no equipment is future proof and void of complications, the ITN's inherent capabilities and modularity make it adequately robust for foreseeable future operations.

Futures Command, the Joint Staff, and other stakeholders are making significant progress. The Army's future tactical communications plan is of such consequence that parallel steps must include widespread awareness, understanding, and adoption by the force. Follow-on efforts must be feasible, adequate, and complete to address lingering DOTMLPF-P deficiencies. Army leaders should be confident in the current plan and future capabilities but must remain motivated and proactive to keep us on target. ■

Notes

1. Commission on the National Defense Strategy for the United States, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* (Washington, DC: U.S. Institute of Peace, 2018), vii, accessed 19 December 2019, https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf.

2. James C. McConville, Memorandum for Assistant Secretary of the Army (Acquisition, Logistics and Technology); Chief Information Officer (CIO)/G6; Commander, U.S. Army Forces Command (FORSCOM); Commander, U.S. Army Training and Doctrine Command (TRADOC); and Commander, U.S. Army Test and Evaluation Command (ATEC), "Directed Requirement to Experiment, Demonstrate, and Assess an Integrated Tactical Network," 29 June 2018.

3. Center for Army Lessons Learned (CALL) Handbook 16-18, *Multinational Interoperability Reference Guide: Lessons and Best Practices* (Fort Leavenworth, KS: CALL, July 2016), 4. The handbook cites a speech by Lt. Gen. Ben Hodges in which he says there are "three key elements of interoperable communications to include: secure tactical FM radio … interoperable friendly force tracking … and a lower-unit common operational picture (COP) that shows up on a higher unit COP."

4. "Advanced Encryption Standard (AES)," TechTarget, last updated March 2017, accessed 19 December 2019, https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard. "The Advanced Encryption Standard, or AES, is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data." The number 256 indicates a system is capable of handling 256-bit blocks of information.

5. Kathryn Bailey, "The Army Ushers Capability Sets Down the Network Modernization Road(map)," Army.mil, 23 October 2019, accessed 23 January 2020, https://www.army.mil/article/228865/the_army_ushers_capability_sets_down_the_network_modernization_roadmap.

6. Asymmetric Warfare Group, *DOTMLPF HF Communications Assessment* (Fort Meade, MD: Asymmetric Warfare Group, n.d.). The author has also directly observed deficiencies in the use of high frequency radio equipment at the Joint Multinational Readiness Center and during his assignment with the Asymmetric Warfare Group.

7. Army Techniques Publication (ATP) 6-02.53, *Techniques for Tactical Radio Operations* (Washington, DC: U.S. Government Publishing Office [GPO], January 2016 [obsolete]). Additional references and information for tactical communications can be found in ATP 6-02.45, *Techniques for Tactical Signal Support to Theater Operations* (Washington, DC: U.S. GPO, November 2019); ATP 6-02.60, *Tactical Networking Techniques for Corps and Below* (Washington, DC: U.S. GPO, August 2019); ATP 6-02.71, *Techniques for Department of Defense Information Network Operations* (Washington, DC: U.S. GPO, April 2019).

8. ATP 6-02.53, *Techniques for Tactical Radio Operations*.

9. Committee on National Security Systems (CNSS) Instruction No. 4009, *National Information Assurance (IA) Glossary* (Fort Meade, MD: CNSS, 26 April 2010). The CNSS breaks down communications security into Type 1 and Type 3 equipment and keys. Type 1 equipment is used for classified and unclassified information whereas Type 3 equipment can only be used for unclassified.

10. The integrated tactical network evaluations including Exercise Saber Junction 18 and Exercise Saber Strike 18; 1st Battalion, 508th Parachute Infantry Regiment (1-508th PIR), and 2nd Cavalry Regiment training at Fort A. P. Hill, Virginia, and Bemowo Piskie Training Area in Poland; 1-508th PIR employment of the FURY network during a 2017 Joint Readiness Training Center rotation by 3rd Brigade Combat Team, 82nd Airborne Division; and the Integrated Tactical Network User Demonstration, 17–25 March 2018.

11. "Warrant Officer Basic Course 255N," Cyber Center of Excellence, last modified 8 August 2019, accessed 27 December 2019, https://cybercoe.army.mil/SIGNALSCH/COURSES/course_wobc_255n.html.

12. 442nd Signal Battalion, "Warrant Officer Course Maps" (Excel spreadsheets, 442nd Signal Battalion, Fort Gordon, GA, 1 August 2017).