Everything I Never Wanted to Learn about the Network and Where We Might Go from Here

Lt. Col. J.B. Shattuck, U.S. Army, Retired

While establishing a communications network for an exercise at the Maneuver Center of Excellence on Fort Benning, Georgia, I had to roll up my sleeves, bite the bullet, and learn more than I, or most of my maneuver brethren, would ever care to learn about the current state of communications. Like many of my colleagues, I just want communications to work, and I do not (or did not) care why or how. However, the truth is that, currently, networks simply do not work (and will not work) in the way many of us expect. But, once we learn some simple fundamentals, there is potential to make networking, the verb, a reality.

The Laws of Physics and the Soldier Radio Waveform (SRW)

Radios can transmit a lot of information over a short distance or a little information over a long distance. Period. This is due to the way a radio wave carries information and propagates. Iterative technology advances and longer antennas will not change this simple rule. We can maximize the amount of data and range of a given waveform for maximum benefit only up to the limit of that particular waveform. This is important to point out as it requires a radio optimized for performance to get the most out of a limited range for a networking waveform.

Networking waveforms carry a lot of information and are short range due to the physics involved; there is no overcoming this. On the other hand, long-range waveforms, such as the SINCGARS (single-channel ground and airborne radio system) waveform we have been using for years, carry little more than voice and some very limited data. As a result, it is, technically, possible to establish local networks around platoons, possibly around entire companies, and certainly around company and higher headquarters. However, the range of these local networks is likely to be measured in meters, not kilometers. Another type of waveform with more range is required to bridge the gaps between local networks using voice, not data, due to the distance the waveform needs to travel.[1] Consequently, the idea that we can populate a single, Internet-like unifying network with our data for all to see in real time is unattainable.

A brigade commander will not routinely see the sensor feeds going to squad leaders, unless there is a preplanned event and the resources are in place to relay that signal. The relay resource most often mentioned is an unmanned aircraft system (UAS), which is touted by many as the answer to the gaps of local networks as part of the "aerial layer."[2] This may be effective given a point-to-point relay of a signal, but this fills just one gap from one local network to one other. There are, however, other significant shortcomings with this aerial layer concept.

The Myth of the Aerial Layer

While it is true that a signal may be relayed from one point to another over substantial distance using a UAS, it is not the panacea that some are led to believe.

Army communications architecture slides often show the UAS with lightning bolts linking a platoon to a company to a battalion to a brigade, and some even to a division. Normally, these slides show one representative platoon, although actually there are many, and it would be some kind of extraordinary platoon that would operate on the division's network. Such connectivity would need preplanning in order to program all the radios required to relay the signal (without exceeding the capacity of the network). Recall that with the short range of the networking radios, there is no single unifying network, only local networks operating on their own frequencies. In a three-brigade division, there could be twenty-one battalions, eighty-four companies, and two hundred fifty-two platoons. This would require a substantial allocation of the available UASs to be dedicated to relay company, battalion, and division networks.

This presents a large problem set. However, the scale and scope of the problem may often be glossed over in the reputed solution because even if a super-communication UAS is developed that relays multiple frequencies at once, it will still be subject to the same duration and weather constraints and would be vulnerable to counter-UAS. In addition, there is still the limitation of carrying the network's capacity, which would be challenged to support the number of radios required by a company's network, let alone a division's.

A soldier uses a digital Rifleman radio, part of the Joint Tactical Radio System Handheld, Manpack, and Small-form Fit (HMS) program, during a network integration evaluation 8 April 2014. The HMS program provides a radio waveform-enabled "gateway" between the Rifleman radio and the Army's satellite communications backbone, known as the Warfighter Information Network-Tactical.

(Photo by Claire Schwerin, PEO C3T, U.S. Army)

The Current State of the Army's Tactical Radios

At present, the tactical radio cure to the networking dilemma is not encouraging. Maj. Gen. H.R. McMaster, then commander of the Army Maneuver Center of Excellence at Fort Benning, Georgia, was quoted in a June 2015 article about problems with the AN/PRC-155 Joint Tactical Radio System (JTRS) Handheld, Manpack, and Small-form Fit (HMS) radio set:

> The Maneuver Center of Excellence considers the dismounted HMS Manpack radio unsuitable for fielding to brigade combat teams .... A radio that is heavier and provides less range while creating a higher logistics demand does not make our units more operationally capable. Additionally, any radio that places our soldiers at risk of being burned is unacceptable.[3]

According to the same 2015 article, from the Defense Industry Daily website, HMS Manpack has many problems:

> The Radio's seventeen pounds makes it twice as heavy as previous SINCGARS radios, its effective range is less than half as far (3 km vs. 7 km), its two batteries last less than 20 percent as long (six hours vs. thirty-three hours), and its user interface is an impediment. Adding to the fun, overheating is hazardous to the carrying soldier if it's taken out of the case against recommendations.[4]

However, this assessment is generous compared to the reality. The three-kilometer range is a stretch; perhaps the radio could achieve that distance in the open deserts at White Sands Missile Range, New Mexico, or Fort Bliss, Texas, but not in the forested hills of Fort Benning, Georgia. It would be fortunate to get three hundred meters in the complex terrain the infantry often finds itself in.

So, in August 2014, the Maneuver Center's Maneuver Battle Lab began to explore networking concepts and to exercise a cellular network and lower standards of encryption for tactical communications. For many, it was assumed network integration exercises (NIEs) would work out the bugs of the radio over time. However, the director of operational test and evaluation, J. Michael Gilmore, found the AN/PRC-155 was "not operationally effective when employed in dismount operations" at NIE 14.2.[5] Likewise, he commented on the Rifleman radio during the same NIE:

> When employed during the first phase of Nett Warrior initial operational test and evaluation at NIE, the AN/PRC-154A Rifleman [radio] provided good voice communications 'until a terrain feature blocked line-of-sight,' and 'soldiers had problems with the radio battery,' including high battery temperatures that 'caused first-degree burns and discomfort. Sixty percent of the soldiers reported that the temperature was in excess of 120 degrees Fahrenheit.'[6]

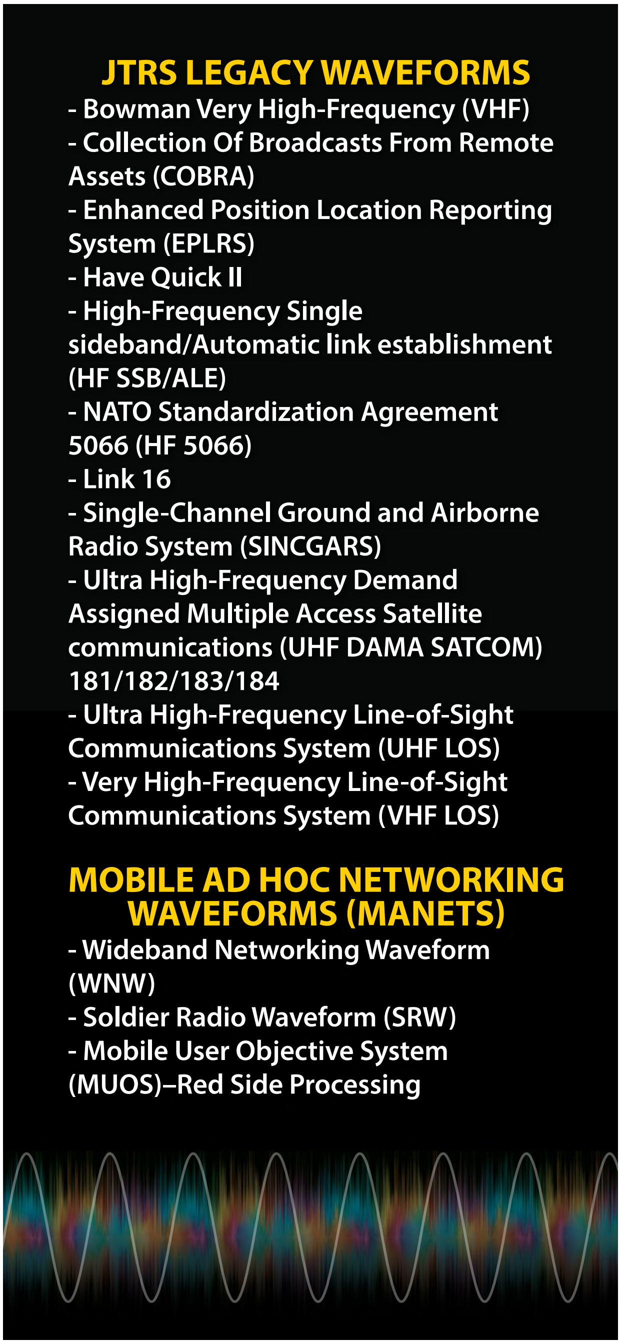
In January 2015 the Army responded to the report, defending both the radios and results of NIE 14.2, asserting that the Manpack "was successfully used to make voice calls and transport data throughout the test, with feedback indicating that the radio supported communications needed to accomplish the mission."[7] Obviously, these two conflicting positions indicate a great disconnect with the development of our family of networking radios.

The Fact of the Matter

The physics of the problem dictate that a networking radio is going to be short range. Unfortunately, when authorities knowledgeable of the science of radio waves take issue with the radio, they are dismissed as having a lack of understanding regarding its range limitations. Consequently, such dismissal represents a missed opportunity to address root-cause problems.

Yes, the networking radio needs to be short range, but not as short as we are currently experiencing; it merely needs to be optimized for the networking waveform currently being used. Any new equipment or technologies are going to have some bugs to work out, but changing to longer antennas is only a helpful step toward a greater solution.

To further compound the networking radio issue, in November 2014 the Army reported that the vehicle-mounted Manpack met the mounted-leader requirements, which account for 64 percent of total program requirements.[8] The report indicated that the Army would review requirements and technology to improve the radios for the remaining 36 percent



JTRS LEGACY WAVEFORMS

- Bowman Very High-Frequency (VHF)
- Collection Of Broadcasts From Remote Assets (COBRA)
- Enhanced Position Location Reporting System (EPLRS)
- Have Quick II
- High-Frequency Single sideband/Automatic link establishment (HF SSB/ALE)
- NATO Standardization Agreement 5066 (HF 5066)
- Link 16
- Single-Channel Ground and Airborne Radio System (SINCGARS)
- Ultra High-Frequency Demand Assigned Multiple Access Satellite communications (UHF DAMA SATCOM) 181/182/183/184
- Ultra High-Frequency Line-of-Sight Communications System (UHF LOS)
- Very High-Frequency Line-of-Sight Communications System (VHF LOS)

MOBILE AD HOC NETWORKING WAVEFORMS (MANETS)

- Wideband Networking Waveform (WNW)
- Soldier Radio Waveform (SRW)
- Mobile User Objective System (MUOS)–Red Side Processing

(Graphic by Arin Burgess, *Military Review*)

Figure 1. JTRS Legacy Waveforms, Ad Hoc Networking Waveforms, and Network Enterprise Services

"associated with dismounted operations."[9] For context, in the most current active and National Guard brigade-combat-team numbers, there are thirty-five infantry brigades, sixteen armored brigades, and nine Stryker brigades. Yet, even within armored and Stryker brigades, infantry squad leaders up through company commanders have to be prepared to dismount. So, how then does the vehicle-mounted Manpack radio meet 64 percent of the program requirements? Perhaps it is time to update the concept of operations that drives analysis of leader radio requirements.

Additionally, the Army neglects to adequately address the radio's user interface issue with the range issue. One defense-oriented website, the Defense Industry Daily, reported, "Its user interface is an impediment."[10] Indeed. To use the radio system, the network is built on a laptop first with a name assigned to each radio using an ISP-equivalent naming convention. Then, the laptop joins with each radio so that the network program can be physically uploaded.

This complex and time-consuming task becomes operationally untenable when the task organization changes during an operation. To attach or detach an element, or to communicate with a diverted enabler, is not a matter of simply uploading the network to new users. Instead, the system is designed in such a manner that it must be completely rebuilt and uploaded again into every radio in the network.

Fortunately, every radio in the network is actually not very many. Though the carrying capacity of the network—the number of radios on the same frequency communicating and networking with each other—is advertised to be a maximum of forty-five, it is necessary to keep the number of networked radios to fewer than twenty-eight. More than that begins to bog down the data transfer rate. And, with more than thirty-five radios on the network there is a danger of crashing it.

How has the Army come to a point where our twenty-first-century radio is twice the weight, half the range, a battery burden, and a burn hazard as compared to our twentieth-century radio? The answer resides in well-intentioned but overly complicated requirements that result in industry trying to comply with exceedingly complex JTRS standards and National Security Agency (NSA) Type 1 encryption.

JTRS Standards and NSA-Certified Encryption

Compatibility with legacy systems is among the requirements that industry must accomplish to meet the JTRS standards and field a new radio. Legacy radio

- Army Aerial Network Extension Capability Production Document (CPD)
- Airborne, Maritime, Fixed Small Airborne Networking Radio (SANR) and Small Airborne Link 16 Terminal (SALT) CPD
- Army Enterprise Service Desk CPD
- Bridge to Future Network CPD
- Common Hardware Systems (CHS) CPD
- Enterprise Wideband Satellite Communications (SATCOM) Terminal System (EWSTS) CPD
- Expeditionary Forces Information Services (EFIS) CPD
- Global Broadcast System (GBS) Multi-Echelon Broadcast Capability (MBC) CPD
- Identity Management (ID) CPD
- Integrated Tactical NetOps (ITNO) Capability CPD
- Key Management Infrastructure CPD
- Manpack CPD
- Multi-tier Networking Vehicular Radio (MNVR) CPD (replaced GMR CPD)
- Modern Cryptographic Services CPD (added 24 June 2014)
- Network Battle Command Initialization CPD
- Network Operations CPD
- Next Generation Load Device CPD
- Regional Hub Node (RHN) CPD
- Rifleman Radio CPD
- Tactical Internet Management System (TIMS) CPD
- Tactical Network Operations Management System (TNMS) CPD
- Tactical Services Management (TSM) CPD
- Transmission CPD
- Transportable Tactical Command Communications (T2C2) CPD
- Two-Channel Leader Radio CPD (to be developed)
- Unified NetOps CPD
- Wideband SATCOM Operational Management System (WSOMS) CPD
- WIN-T Inc. 2 Rev. 3 CPD

(Graphic by Arin Burgess, *Military Review*)

Figure 2. Cyber Common Operating Environment Requirements Documents

compatibility requires that the radio must be capable of operating on fourteen different legacy waveforms (see figure 1, page 91) In addition, the industry must sort through twenty-eight requirement documents that cover all the different communications applications (see figure 2). This well-intentioned requirement to ensure compatibility directly results in a complex radio and is likely the reason for the extra weight, overheating, and battery drain issues associated with the radios examined so far.

Over the life of the network, overly optimistic development decisions, compromises, and congressional input have affected how the radios are developed and implemented. For example, the Rifleman radio is now used as a leader radio; that was never its intended role.[11]

Further complicating the radio is the requirement for top-of-the-line, NSA-certified encryption. However, industry representatives indicate that an advanced encryption standard (AES)-type encryption is almost as secure, and would result in far less of an engineering challenge.

How much more secure is the NSA Type 1 versus AES? Is any encryption completely trusted, or would better radio procedures make the risk worth the payoff of a more capable radio? Key leaders at the Maneuver Center seem to think so. Bottom line, the radio now fielded seems more optimized for compatibility and security, not actual performance.

Challenges of Cellular and Wi-Fi Networks

Turning to other issues complicated by similar challenges, there is no magic to cellular and Wi-Fi. They are waveforms capable of moving large amounts of data but are still subject to the laws of physics previously described: high data, short range. Fortunately, cellular networks in our everyday lives function effectively because a cellular infrastructure surrounding us supports them. The same is with Wi-Fi; think of the Wi-Fi hotspots in our lives and the short ranges associated with them. A Wi-Fi network that establishes itself around the battalion tactical operations center (TOC) has great potential to move large amounts of data, but only for those present at the TOC.

Setting aside for a moment the proliferation of counter-radio electronic-warfare devices that deliberately jam cellular signals, cellular networks have all the performance wanted. However, a robust infrastructure must be emplaced and secured to make a tactical cellular network possible.

Where Do We Go From Here?

From a pragmatic view, I believe the solution to the Army's current radio dilemma requires four actions.

1. The Army must acknowledge what is and what is not possible according to the physics of radio waves. A single, unifying, Internet-like network is not possible; however, local networks are possible. Consequently, data recovery missions can be launched from higher to lower positions in order to push and pull data to and from the local networks and populate the higher networks. Irrespective, there will be delays in data communications using such networks that will preclude real-time transfer. Therefore, voice communication will have to suffice to bridge the gap.

2. The Army needs to adjust the requirements for its tactical radios. A single-purpose radio optimized for performance is needed, with a networking waveform on one side and a long-range waveform on the other, cross-domained. If SINCGARS is used as the long-range waveform, then we will have compatibility with much of our legacy systems. This radio should also be AES standard encrypted, and have auto affiliation built in.[12]

3. The Army should explore the use of networking radios developed by U.S. manufacturers to platoon-and-below-level operations for sale on the international market. Radios sold by these manufacturers have less stringent security requirements but may still be acceptable for those that operate with information that is often fleeting and perishable. These radios are not burdened with JTRS requirements, which result in radios too complicated to build and operate.

4. The Maneuver Center of Excellence and the Cyber Center of Excellence should come together to develop or update a concept of operations for an infantry brigade conducting combined-arms offensive operations. I recommend a movement-to-contact scenario to stretch the distances between units a bit more than may be the case in other operations. A concept of operations should provide an opportunity to

(Photo by Claire Schwerin, PEO C3T, U.S. Army)

Soldiers from the 2nd Brigade, 1st Armored Division at a company outpost during the Army's second Network Integration Evaluation, NIE 12.1, at White Sands Missile Range, New Mexico, and Fort Bliss, Texas. The NIEs are helping bring greater network connectivity to the company level so soldiers can communicate through voice, data, images, and video, even in complex terrain.

map out exactly who is networking with whom, when, with what radio, and on which net. We should start at platoon level (not just one representative platoon) and work back to brigade.

Conclusion

Communication networking can be realized for our forces, but we need to be honest with ourselves concerning what is possible. Consider a scenario where company commanders arriving at the battalion TOC for an orders brief find their tablet already updated with the order and graphics via the battalion TOC Wi-Fi signal by the time they grab their cup of coffee and sit down. Likewise, the common operational picture display inside the TOC is now more current, having downloaded the information from the company commanders. The supporting Apache aircraft can upload the unit's position location information and know exactly where the friendly forces are. This does not change the company commander's responsibility to inform the flight lead; it just makes their job that much quicker and easier. UAS flights can come and go on data-push missions between command posts, including adjacent units. Auto affiliation can make task organization changes and integration of enablers seamless. The "take" from the robotic sensors will be a topic for discussion among the squad leaders as they conduct priorities of work.

Ultimately, the networking efforts will likely include a mix of cellular, Wi-Fi, SRW, and now airborne and wideband networking waveforms, along with a long-range waveform to maintain at least voice connectivity.

To get there, we have to understand that lots of information only travels a short way, and a little information can go a long way. We have to optimize our radios for performance, not compatibility and security. We have to integrate into our communications systems the means to support changes to task organizations and the movement of enablers across nets. Finally, we have to work in the realms of possible, and follow the physics to workable solutions. ■

Biography

Lt. Col. John B. (J.B.) Shattuck, U.S. Army, retired, is the program manager of the Squad Foundation of the Decisive Force, Focused Assessment Exercise, at Fort Benning, Georgia. He holds a BS from the United States Military Academy and an MBA from Indiana Wesleyan University. During his military career, he deployed to Iraq twice, and to Saudi Arabia, Somalia, Haiti, and Bosnia.

Notes

1. A small amount of data over a single-channel ground and airborne radio system (SINCGARS) network is possible and currently done, just not on the scale of a data-networking radio. I use SINCGARS as an example of a longer-range waveform due to its familiarity.

2. Joint Chiefs of Staff, *Joint Concept for Command and Control of the Joint Aerial Layer Network* (Washington, DC: U.S. Government Printing Office, 20 March 2015), 9.

3. Maj. Gen. H.R. McMaster, quoted in Defense Industry Daily staff, "Soldier Battle JTRS: The HMS Radio Set + SANR," Defense Industry Daily website, 18 June 2015, accessed 3 March 2016, http://www.defenseindustrydaily.com/soldier-battle-jtrs-the-hms-radio-set-07536/.

4. Defense Industry Daily staff, "Soldier Battle JTRS: The HMS Radio Set + SANR."

5. J. Michael Gilmore, quoted in Ellen Mitchell, "Manpack, Rifleman Radios Have Heat, Reliability Problems," Inside Defense website, 19 January 2015, http://insidedefense.com/node/166763 [login required].

6. Mitchell, "Manpack, Rifleman Radios."

7. Paul Mehney, quoted in Mitchell, "Manpack, Rifleman Radios."

8. Ellen Mitchell, "Army Pondering Two Versions of Manpack in Radio Acquisition," The Insider (newsletter), Inside Defense website, 9 March 2015, http://insidedefense.com/node/167925 [login required].

9. Ibid.

10. Defense Industry Daily Staff, "Soldier Battle JTRS."

11. U.S. Army Training and Doctrine Command Capability Manager, Brigade Combat Team - Mission Command (TCM BCT/MC) website, 30 December 2014, accessed 29 March 2016, http://www.benning.army.mil/mcoe/CDID/tcm-bct-mc/index.html.

12. Auto affiliation is what we do each time we go to our local coffee shop, turn on our tablet, phone, or laptop, scan the available networks, and then connect to the network. We do not need to be concerned that units will not be able to communicate after a task organization change, or that the Apaches vectored to the company in contact will not be able to communicate with the company commander.