LtGen Bernard E. "Mick" Trainor Military Writing Award 2018: Honorable Mention

Technology

Revolutionary in moderation, fatal in excess

by Capt YiCheng Garrard

>Capt Garrard has served as a S-6 (Communications) Officer with 1st Reconnaissance Battalion and as an Operations Officer with the G-6, 1stMarDiv. He is currently assigned as a Foreign Area Officer–Japan/China.

Military technology is revolutionary, leading to battlefield innovations previously unimaginable and saving lives in the process. However, the Marine Corps, rather than using it to enhance its expeditionary communications, moved toward a complete reliance on network connectivity in the form of share point, share drive, chat, email, video teleconferencing, and countless data-heavy applications and software to conduct operations. Such demands are only feasible through large and complicated equipment strings requiring an army of Marines with weeks to prepare, install, and maintain. Not only is this logistically taxing, but the far greater threat of signals emissions makes its users increasingly vulnerable to enemy detection and targeting. One only needs to look at the massive fleet of vehicles, generators, and communications equipment that plague every headquarters combat operations center. Moreover, communicators often arrive days before the unit to install the network. This is unrealistic in war. Fortunately, such vulnerabilities are at the forefront of commanders' minds today, with an increasing emphasis from commanding generals to battalion commanders on conducting operations in communications-denied and- degraded environments against a peer or near-peer adversary. While the solutions of some units garnered success, the problem is that largely, the institutional mindset remains firmly in the camp of operating with full network connectivity. Any reductions are viewed as intolerable. This is unacceptable, unsustainable, and dangerous.

Establish minimum information and exchange requirements. *(Photo by LCpl A.J. Van Fredenberg.)*

I contend that the most pressing challenge facing the Marine Corps in future operating environments—and that exposes it to detection and targeting—is its over reliance on network-enabled command and control (C2). Controlling the physical terrain is meaningless if one's C2 systems either fail the commander or create an existential vulnerability. The appropriate response is to reduce operating requirements that rely on network connectivity and reimagine the way we employ existing C2 gear. I am *not* advocating for a complete abolition of network-enabled C2 but rather a paradigm shift in both its *usage* and *installation*. This can be achieved by both establishing minimum information exchange requirements and simplifying the equipment string through alternate but existing transmission means, such as the Broadband Global Area Network (BGAN), Rapid Response Kit (RRK), Mobile User Objective System (MUOS), and Secure Mobile Anti-Jam Reliable Tactical Terminal (SMART-T). This equipment must then be tied directly into the Marine Corps Enterprise Network (MCEN). To understand its application, I will apply this criteria to the headquarters of company, battalion, regiment, major subordinate

commands, and MEFs. As with any physical footprint, the total elimination of signals emissions is unrealistic; while alternate and even technologically superior solutions may exist for acquisition, time is of the essence, and—most importantly—this proposal is the impetus for the institutional change required to sustain future technologically dependent solutions.

With today's threats creating increasing demands on units to operate in dispersed formations across the globe—combined with the joint nature of contemporary military operations—the desire and need for commanders to maintain situational awareness has never been greater. Unfortunately, equipment solutions have not kept pace, and the expectation of constant, high-speed network access further exacerbates this problem. No longer is a simple and visually unappealing yet small text file sufficient. Instead, detailed and bandwidth-consuming PowerPoint slides by the dozens-filled with high-resolution imagery and graphics paired with crystal-clear video teleconferences are now the norm. A decade and a half of combat in the stationary outposts of Iraq and Afghanistan bred the toxic practice of establishing sprawling and intricate communications networks more suitable for Army-like static and enduring operations. This runs completely counter to the expeditionary nature of the Marine Corps.

Such an expectation of garrison-like capabilities for expeditionary operations comes at a heavy cost. The first is in the form of an almost unmanageable labyrinth of equipment and software layered upon one another from different commercial sources that are not compatible or introduce vulnerabilities and problems requiring endless hours of troubleshooting. More problematic, however, is the emissions footprint of both signals (from satellite terminals) and electronic noise (from generators and vehicles). The detection of either can quickly and easily betray the location and disposition of a unit with no warning that it has occurred. In essence, our electronic footprint becomes a virtual aiming stake for the enemy.

The first sticking point in the successful implementation of C2 systems is its complexity and technical difficulty. The days of slapping an antenna on a radio and flipping on a switch are long past. Instead, units bear a heavy load for providing services including unmanned aerial system feeds, full motion video, exchange (email), and web-based applications, all of which require extensive networking expertise and time-consuming installations. Additionally, new software applications claiming to simplify tasks inadvertently introduce issues to the network, requiring even more manhours to fix. Oftentimes, bits and pieces of the network will work at random, creating a maddening situation and compelling units to conduct weeks of strap exercises and communications exercises in preparation, only to find out it no longer works when they set up for execution. In essence, our expectations are that of a garrison-replicating network in austere environments for expeditionary operations using a fraction of the resources. This limitation underscores the massive, self-induced friction we create in our endless demand for information.

With an endless array of power-amplified vehicles sporting omnidirectional antennas that cover the area with signals and power emissions as well as satellite terminals that produce large signal cones, the electronic footprint of even modest-sized headquarters can be strikingly large.

The second downside to today's C2 systems is its signals footprint. This is especially the case of regimental headquarters and above. With an endless array of power-amplified vehicles sporting omnidirectional antennas that cover the area with signals and power emissions as well as satellite terminals that produce large signal cones, the electronic footprint of even modest-sized headquarters can be strikingly large. This self-created vulnerability is engendered by the relentless demand of users for high-speed network connectivity, requiring garrison-like capabilities. Fortunately, this issue can be significantly mitigated by using alternate gear if users are willing to forgo some bandwidth and features they are accustomed to.

The first and smallest of these is the BGAN. A rugged satellite antenna roughly the size of a hardcover dictionary, the BGAN is powered by the same batteries used in manpack radios and extends the popular and widely used Advanced Networking Wideband Waveform (ANW2). Used successfully by the reconnaissance community and HIMARS units such as 5th Bn, 11th Marines, the BGAN is easily transported in a pack and set up quickly. When used with a PacStar, the BGAN ties into the MCEN, providing its users with further capabilities of directly accessing the garrison network without relying on a shoddy tactical one. This is especially key in today's world of dispersed operations, where a company commander or reconnaissance team leader may be operating hundreds of miles away from his battalion.

The second and perhaps most versatile is MUOS. Already in development by Marine Corps Systems Command and used heavily and successfully by 1st MarDiv during STEEL KNIGHT 2018 in the field user evaluation and by I MEF during MEF Exercise 2018, MUOS is essentially dedicated satellite communications that also allows for Secret Internet Protocol Router Network access through a radio. This is the missing link in the tactical satellite communications architecture. A game changer providing network-like capabilities through a single AN/PRC-117G, MUOS integrates programs of

record equipment such as the MAGTF Secondary Imagery Dissemination System, Advanced Field Artillery Tactical Data System, and chat. Despite its bandwidth being significantly less than a large satellite terminal such as Very Small Aperture Terminal-Large, its portability and equipment simplicity is revolutionary. By using solely a laptop with an AN/PRC-117G, a single Marine has the same capabilities as a battalion combat operations center requiring a fleet of equipment and support, albeit on a much smaller scale. For example, during STEEL KNIGHT 2018, 1st Marine Division tested MUOS in multiple configurations, including in combat operations centers, light-armored vehicles, HMMWVs, and manpack variants, with positive feedback from commanders. Such success underscores MUOS' flexibility and scalability.

Another excellent and often underused capability is the RRK. As a program of record allowing MCEN connectivity in the field, RRKs currently reside at air-naval gunfire liaison companies, reconnaissance battalions, communications battalions, communications companies, and MEUs. 1st MarDiv initially used the RRK during MEF Exercise 2018 by providing its users with the ability to access the MCEN Secret Internet Protocol Router and Non-Classified Internet Protocol Router while in the field. By extending the MCEN, users brought their work laptops and had a reliable means of fallback in the event of issues with the tactical network, including professional backups and professional battery and generator failure. This added layer of redundancy was critical during tactical network outages and shows promise in its adoption for rapid employment. It should be used at battalion headquarters and above. Altogether, the medium variant fits in the back of a compact car, a stark difference from the Very Small Aperture Terminal-Medium that requires a HMMWV with trailer. Advantages of this equipment are its status as a program of record, ease of installation, and proven reliability.

Finally, the SMART-T is perhaps the most significant component of operating with a minimal footprint while providing maximum capabilities. While still a satellite terminal, the SMART-T differs significantly from most currently in use by the Marine Corps. It operates on a higher frequency (advanced extremely high frequency) and produces a significantly smaller signals footprint that makes detection and jamming extremely difficult. Moreover, the SMART-T is built to explicitly withstand detection, interception, and jamming. If its users exercise discipline in bandwidth conservation, one SMART-T can support an entire division staff. 1st MarDiv is currently pushing for wider adoption by providing them to regiments for operating in communications-denied environments. The SMART-T has a long history and is also used by the U.S. Army with emphasis on its versatility.

To visualize the fielding and employment of the aforementioned gear, one begins with the infantry company. Each ought to receive two BGANs and MUOS access. Because MUOS and BGANs both work with the AN/PRC-117G, no additional radios are required, although a modified antenna is required to maximize MUOS capabilities. An additional point of consideration is the use of the high-frequency radio, an often neglected yet powerful tool. By employing creative field craft, a Marine can easily make a field expedient antenna capable of communicating between Twentynine Palms, CA, and Camp Pendleton, CA, on a manpack radio without vehicle power amplification. In using these means, a company headquarters can drastically increase its C2 capabilities with minimal gear additions or signals emissions.

An infantry battalion ought to rely on one RRK-Medium and MUOS. By tapping into the MCEN, the battalion frees up a significant and crushing burden on its cyber capabilities and instead benefits from the stable and arguably more secure network serviced by a vast civilian workforce required to provide near consistent connectivity. The objection that friction and stumbles will accompany this shift from operating on a tactical network to a garrison one is not without merit. However, the payoff is substantial, and III MEF demonstrated this feasibility years ago. Additionally, MUOS allows the commander to maintain network connectivity when traversing the area of operations. By combining the RRK-Medium with MUOS, the staff will have significant flexibility and sufficient data capabilities. An important takeaway is, because companies have MUOS, a battalion can maintain network connectivity regardless of location.

RRKs currently resides in air-naval gunfire liaison companies, reconnaissance and communications battalions and companies, and MEUs. *(Photo by Sgt George Melendez.)*

A regimental headquarters ought to employ one RRK-Medium, one SMART-T, and MUOS. By maintaining a second path out to the network via the SMART-T, in the event the RRK is jammed, the regiment maintains its network connectivity to its subordinate, adjacent, and higher units. As with a battalion, MUOS provides the regimental commander flexibility when conducting battlefield circulation. The regimental level is one where expectation management begins to reveal its criticality. With a large staff and multiple subordinate units, the temptation to access information instantly and in unlimited quantities must be suppressed. Information exchange baselines for both higher headquarters and subordinates ought to be codified in the unit's SOP, no different from immediate actions or battle drills. Only in this way can the equipment provide the necessary bandwidth to support the staff.

A major subordinate command is a behemoth of information requirements. With numerous working groups requiring coordination with external agencies, countless internal meetings, and a large, churning staff, the bandwidth burden strains even the most versatile communications systems. Looking at the division, it ought to use two RRKs-Large, one SMART-T, and MUOS. The staff ought to constrain its bandwidth requirements to the gear's limitations; otherwise even a dedicated high-speed fiber link can be argued as being insufficient. As a result, the significant overhauling of SOPs must likely occur. 1st MarDiv successfully codified an SOP for operating in a network-denied environment that proved critical in several exercises and forced the staff to reduce their bandwidth usage. Some examples of low-hanging fruit include eliminating visual teleconferencing and limiting email attachment sizes. To reiterate, the success of this proposal hinges on the willingness of users to radically alter their practices from the expectation of garrison-like capabilities to one of austerity.

At the MEF level, three RRKs, two SMART-Ts, and MUOS ought to be the equipment limit. If one attends a MEF exercise, he can see the gargantuan scale of a MEF headquarters. With an army of staff officers each *requiring* his own computer, the bandwidth demands appear limitless. This echelon of command likely requires the greatest efforts to force institutional change. A complete shift in operating paradigms must occur, and the challenge is immense. Of note, this prescription applies to *expeditionary* operations, not *enduring operations*. In the event that the MEF remains in a secure and rear location, such austere measures may not apply.

Combat camera uses BGAN to transmit imagery to the USS* Kearsarge *(LHD-3). *(Photo by Sgt Chris Stone.)*

In summary, the future of warfare is rapidly moving toward (and perhaps already in) a cyber and signals emissions domain where the control of physical terrain is moot if one is exposed to detection and targeting. Current Marine Corps C2 culture depends almost entirely on network connectivity—at its own peril. Moreover, such demands place an inordinate burden on commands to provide garrison-like capabilities, which are not only extremely challenging and time consuming, but unrealistic in real-world expeditionary operations. An alternative of leveraging *existing* rather than *new* technologies is the impetus to starting the long and overdue culture change. Critically, this must be accompanied by a corresponding change in information exchange. No different from noise or light discipline, Marines must apply equal rigor to their use of communications systems. In an era of seemingly unlimited military funding, the temptation to immediately seek out technological solutions to every problem is high. However, this only addresses the symptoms and not the cause. Unless behavior changes accompany materiel acquisition, the problem will persist.

Ultimately, what is at stake is deeper than purchasing new gear or even reimagining the employment of existing ones. The culture of unlimited information gathering to endlessly build perfect situational awareness in fact cripples the Marine Corps in doing what it does best—expeditionary operations. Unless this paradigm is quickly and radically shifted back toward one of comfort in uncertainty, imperfect information, and an emphasis on speed and simplicity, we risk the lives of Marines all in pursuit of a delusion because a *want* became a *need*.

USMC