

Network-Centric Warfare:

An Exchange Officer's Perspective

Major James A.G. Langley, British Army

FUTURE COMBAT systems envisage war fought in a network-centric manner with machines' observations enabling network fires to engage the enemy with or without human involvement in the sensor-shooter cycle. This network-enabled warfare will win the battle, but any war machine having no human compassion might alienate the population it seeks to liberate.

Understanding political imperatives is important to commanders at every level. Communications and information systems (CIS) providers must understand commanders' unique requirements. By overly concentrating on the needs of the joint task force (JTF) commander, the CIS provider might ignore the squad leader's needs. Network operations concepts are well suited to the higher commander's needs, but network management, information assurance, and information-dissemination methods should be examined at each level of command. Network-centric warfare requires each part of the network to benefit the whole. Applying a hierarchical priority to the network risks disenfranchising those at lower levels who are fighting the contact battle.

Each CIS user should receive the tailored high-quality services required in a timely fashion. Understanding differing capabilities allows the CIS provider to deliver appropriate services efficiently. A JTF commander's situational awareness is nearly revolutionary when it identifies the positions of key personnel and units advancing on Baghdad International Airport, but this level of granularity does little to enhance a platoon leader's understanding of the battle. The platoon leader's situational awareness is what he can see and what is over his immediate horizon and within weapons range. Even when CIS displays

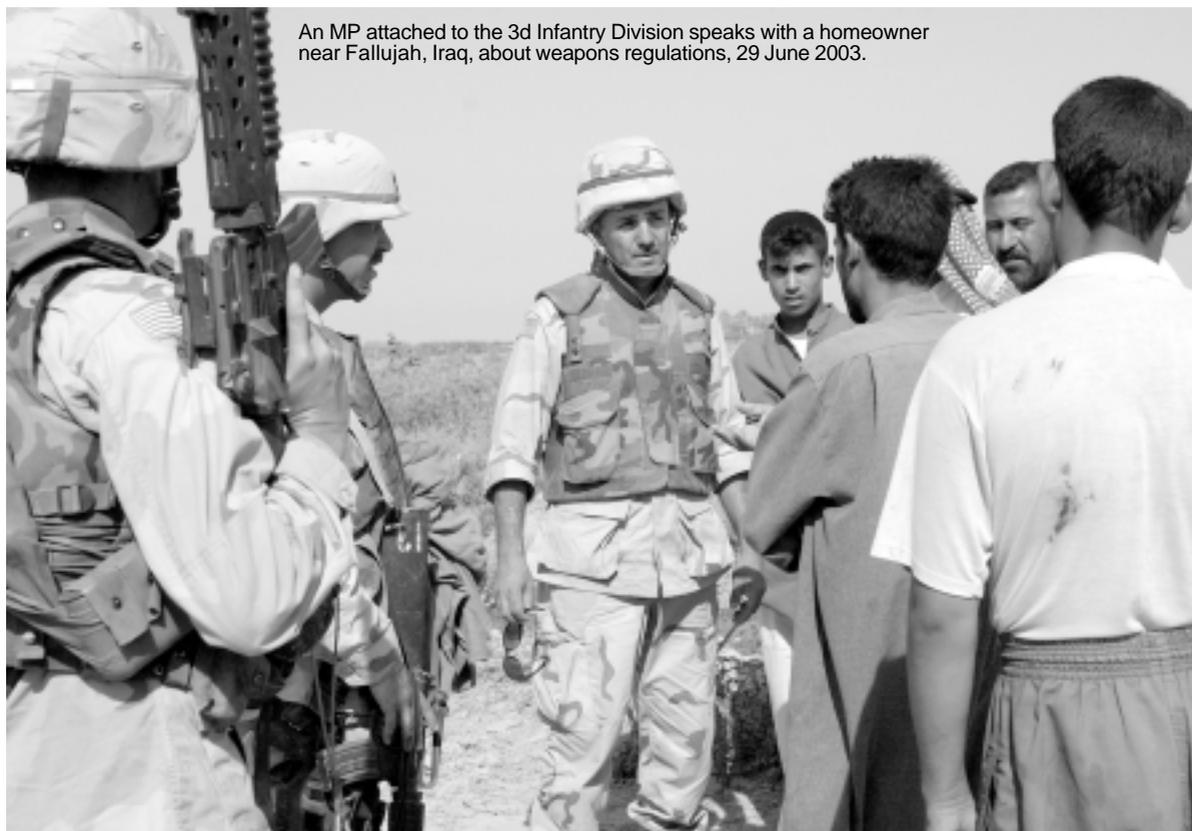
detail, every platform in the battlespace, including dismounts, will only complement the soldier's view of the real terrain.

Timeliness of situational awareness for junior commanders is measured in seconds; for commanding generals, it might be in minutes or hours. The CIS provider must understand these differing requirements and ensure end-to-end service is appropriate. To do this, the supporting CIS commander must be empowered to effect change across the network for the supported maneuver commander, not just tweak the communication transport layer.

When senior commanders discuss complex issues with advisers, decisions are deliberate and require a vast amount of necessary information gathered by many people. The demand to move complex data will be high, and whether commanders communicate via telephone or video teleconference (VTC), they must draw on a wide range of knowledge that spans the global information architecture.

Conversely, a platoon leader or company commander makes decisions quickly based on a lesser amount of information from a smaller number of people. Decisions need to be executed in a timely fashion, which affects CIS services significantly. Junior commanders in contact will continue to rely less on data services and more on voice communication. The communications unit providing CIS services must understand the different needs of commanders and ensure users receive appropriate end-to-end services with the right quality of service (QOS), not a one-size-fits-all technical solution.

As the phase of battle changes, the service that users require will also change. Units in contact are likely to depend more on voice services because



An MP attached to the 3d Infantry Division speaks with a homeowner near Fallujah, Iraq, about weapons regulations, 29 June 2003.

US Army

voice services convey the immediacy necessary in battle. Conversely, the volume, precision, and nonrepudiation available from data services will be more in demand during planning, regrouping, or nationbuilding.

Clansman, Bowman, and Ptarmigan

The CIS lessons the United Kingdom (U.K.) and the United States (U.S.) learned from Operation Iraqi Freedom (OIF)/Operation Telic were quite different.¹ A British Ministry of Defence publication said CIS infrastructure in Iraq could not easily support the information exchange requirement, relied on numerous gateways, and did not interoperate well with the United States in coalition planning.² The communications system Clansman, to be replaced by Bowman, was not criticized as it had been during operations in the Balkans.³ Surprisingly, no mention was made of Ptarmigan, the primary telephone system from division to battalion and the only secure mobile telephone service available in significant numbers at the tactical level. Personal observation suggests Ptarmigan provided (with some expectations) a reasonable QOS to mobile and static subscribers. Ptarmigan met most user expectations, facilitated command and control (C2), and

received relatively little criticism—not bad for a system based on 1970s technology.

In its lessons learned, the 1st U.S. Marine Division was highly critical of its more reliable digital equipment, such as the single-channel ground and airborne radio system and digital telephone switches because they depend on line of sight (LOS) communications. The division also criticized the do-more-with-less procurement policy that maintained or, in some cases, reduced previous radio scalings, in contrast with experiences in Iraq that demanded a significant increase in radio scaling. Because of the less dense maneuver operations battles, the division had a greater need for high frequency (HF) radio and tactical satellite (TACSAT) services than envisaged by those procuring the equipment.

The 3d U.S. Infantry Division's (ID's) lessons learned concluded that mobile subscriber equipment (MSE) cannot support a division's on-the-move requirements while the division is conducting continuous operations and moving its elements.⁴ The lessons learned also identified the need for more TACSAT and similar range-extension systems.

The marked contrast between the performance of MSE and Ptarmigan (two apparently similar systems) is somewhat surprising. However, Ptarmigan

has the advantage of having been adopted for use in an expeditionary context (in Bosnia in 1995 and Kosovo in 1999). It has routinely had VSC501 (a Landrover-deployable system), satellite-communications (SATCOM) links under tactical command for network range extension, and a permanent switching hub in the U.K. for rapidly establishing mobile subscriber access and headquarters communities—often in less than an hour.

Because the 1st U.K. Division's mission was effectively a relief in place of the 1st U.S. Marine Expeditionary Force, communications assets could remain within a "Ptarmigan tactical bound" of combat units, ensuring near-continuous coverage. Conversely, MSE had no satellite links under such immediate control, and the distances involved in reaching Baghdad, not Basra, were considerably more challenging. The differing operational demands placed on the two systems were more of a factor in their performance and provide a lesson for the future. This does not mean that LOS communications cannot work, but that the mix of systems must be appropriate to the mission, and expeditionary tactics, techniques, and procedures (TTP) for supporting maneuver warfare must be in place and practiced.

The shortage of equipment in the 1st U.S. Marine Division, the reduced range of digitized systems, and the need for HF and SATCOM offer some lessons for Bowman. Doing more with less might work on paper, but it did not do so for the U.S. Marine Corps (USMC). Bowman is being fielded at approximately one-for-one with Clansman, so the 50- to 100-percent increase the USMC sought suggests scaling could be the first lesson learned when Bowman deploys. Indeed, scaling has been an issue already for combat service support (CSS) units that will have significantly more Bowman equipment than Clansman equipment.

Joint Tactical Radio System

The Joint Tactical Radio System seems to be heading in the opposite direction. The desire for high bandwidth is reducing planning ranges (a consequence of physics), not increasing them as experience on the maneuver battlefield requires. Consequently, it is important to understand the effects of communications systems on the passage of information in the Future Force. To assume a perfect communications network in the Future Force is to base that network-centric force on a falsehood that will undermine this preeminent concept and is contrary to lessons learned by major military powers in

recent conflicts. Communications are most likely to fail when an operation is at its most complex, compounding the effect on military capability.

During OIF/Operation Telic, both U.K. and U.S. forces demonstrated the need for an increase in SATCOM. However, need must not become dependency. Complex terrain, such as mountains or an urban environment, can obscure geostationary satellites from available ground terminal locations. Weather can render ground terminals unusable, particularly during sandstorms. Overreliance on SATCOM courts disaster during operations where the environment and latitude are different.

The Iraqi regime proved that even old technologies, when correctly employed with specific aims, have uses in modern warfare. Dispatch riders and underground fiber optics maintained communications in a secure manner when radios were unavailable or vulnerable to interception or direction finding.

Command, Control, and Communications

Commanders will need reliable information on the enemy and effective measures to command and control their own forces so they can successfully execute their plans in a faster decision loop than the enemy and with enough logistic flexibility to exploit advantages. This capability does not depend on communications systems and is even more remotely connected to bandwidth; it remains a cognitive problem that includes every soldier on the battlefield and combines leadership, mission command, battle rhythm, orders, TTP, as well as CIS. Subordinates' understanding of the higher commander's intent is fundamental to this capability, and the better subordinates' understand intent, the less dependent they will be on details that demand data and bandwidth.

Increasing the information available to commanders does not necessarily improve knowledge or help them make decisions. Much imagery is of little value without the necessary analyst skills, which are rarely found at battalion level or below. Technology has increased the volume of formal orders, briefs, and information control because of the ability to cut and paste information or attach pictures and graphics, which often add little to knowledge. With thought for the knowledge to be conveyed, many presentations could be reduced to a single page of carefully crafted text. From the military recipient's perspective, concise text would reduce strain on communications and greatly speed the assimilation of information.

Concise information is often more effective. The orders for the German Corps that stopped



3d Infantry Division soldiers secure a street during an early morning raid in Amiriyah, Iraq, 11 July 2003.

Operation Market Garden in 1944 and forced the British retreat from Arnhem required about two typed pages of information plus accompanying annexes. Produced by a small staff in about a day, the orders relied on mission commands, conveyed the message efficiently, and were flexible enough to remain extant throughout the course of the German counterstrike.

A more recent example of simple information exchange is the use of Blue Force Tracker in Iraq to pass intelligence and commands in short, succinct messages. Granted, longer messages were often sent in two or more parts, but the confines of a 100-word message length forced senders to convey meaning more efficiently. The short-message length reduced the amount of information receivers had to assimilate, which allowed them to act faster. Voluminous orders and long briefs are often indicative of poor staff work.

At Waterloo, Arthur Wellesley, the Duke of Wellington, managed well despite having limited communications. After surveying the battlefield, he wrote, two- or three-sentence notes, which a messenger then delivered. Despite the messenger's relatively slow progress on horseback, Wellington's concise, timely orders changed the course of battle. Mission command, brevity, and timely decisions are equally as important as increasing the amount of information commanders send or receive.

Some processes require large bandwidths and some current systems have areas where poor communications-on-the-move prevent command and control, but commanders can exercise command and control without using additional bandwidth. Imagery provides raw data that, if analyzed near the sensor in communication terms, can provide the same knowledge to commanders without unduly influencing demands on communication at the tactical level.

Interoperability

Interoperability between coalition partners is an issue of policy as much as technology. Where information needs to be shared quickly, command, control, communications, computers, intelligence, surveillance, and reconnaissance systems need to be connected, which is a requirement that must be embedded in the procurement process. When high-assurance guards protect information exchange between national systems, by definition they will always bring with them a restriction of information flow.⁵ The fine balance between the security policies of nationally sensitive systems and the technological capability to meet those needs can easily be lost in a bureaucratic procurement.

To help prevent blue-on-blue attacks, situational awareness is often shared, but if security barriers prevent the timely exchange of information, this

intent will not be realized and might produce political consequences even greater than the military problems it creates. Alliances are important in modern conflict, so resolving problems in this area deserves a higher priority than it currently has. Leaders must balance policy, technology, and military capabilities to prevent coalition-compromising frictions.

Progress toward a network-centric future will not be easy. Realism is required. Military innovation is rarely concept-driven: practical blitzkrieg evolved as a result of the invention of the tank, not vice versa. During World War I, soldiers were slow to adopt the machinegun as a weapon for offensive tactical maneuver, but they quickly adopted it for defense because no concept for its use yet existed.

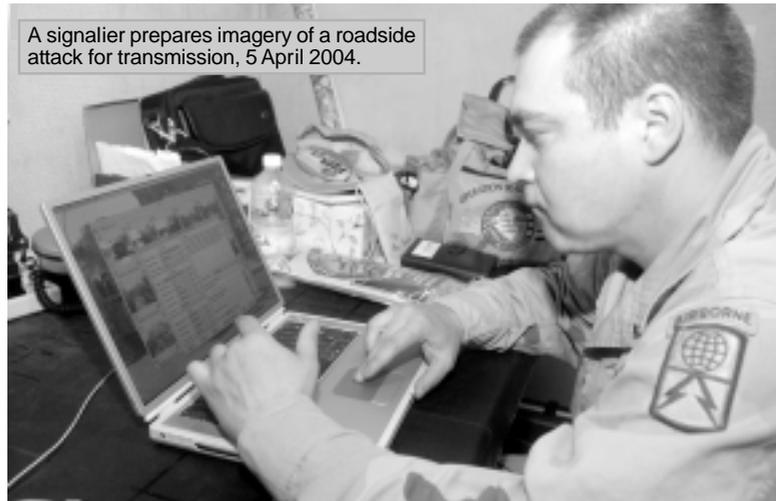
Armies have always been a network of people and capabilities. New technology offers only a route to enhanced military capability, but its adoption might not proceed as envisaged. Inevitably, concepts will change as we more fully understand technology's capabilities to enable warfare.

Moving toward network-centric warfare and leveraging technologies to this end requires investment in blue-sky research and cutting-edge innovation, much of which does not yield the military results expected. While initial aspirations might not be realized, the investment will ultimately enhance the investing country's skills base, technology, and economy.

Concepts for network-centric warfare currently focus on the sensor-shooter loop and battle command systems. The United States has focused on improving intelligence through electronic sensors; that is, intelligence-led operations, but recent conflicts in the Balkans have shown enemies are able to adapt tactics to avoid the consequences of such advances and do not seek a fight where they are sure to lose. The 3d ID in Iraq valued walk-ins because they provided the majority of hard intelligence on enemy activity, despite the 3d ID's array of sensors. Technology cannot assess every individual's will to fight or replace the human element in providing information.

Emphasis on network-centric warfare has led military planners to concentrate on improvements technology will bring to maneuver forces and their C2. Combat forces totally depend on combat support

(CS) and CSS. However, network-centric warfare has the potential to bring even greater enhancements across other functional areas. While improving sensor technology, numbers, and distribution of data will enable the network to analyze more information and provide more intelligence, for the moment such



A signalier prepares imagery of a roadside attack for transmission, 5 April 2004.

US Army

advances in collection are limited by the process in automating analysis because not all analysis can be reduced to computer models and mathematics.

Technology can make a difference in developing battle command systems to support command, but only if an operational imperative, such as tempo, remains the measure of success. Battle command systems must speed up the decision cycle if they are to improve C2 capability. This is not just a matter of technology, it is also one of process. Too often, military planners have sought technological solutions not holistic enough, consequently failing because the underlying communications or the overarching processes were wrong.

Bugles, flags, and heliography technology have advanced the means of control available to commanders. Digital mapping with situational awareness and coordination overlays will soon revolutionize control of military formations by a quantum leap comparable to the invention of the telegraph, telephone, and radio. The danger is that these time-critical services will share the same network with other command communications. This data convergence poses two risks.⁶ At lower echelons, giving priority to higher commanders' services risks their being insufficient to guarantee lower level users services they require at all times. This will result in their not being available during brief but critical periods when in contact with the enemy. Squad commanders under fire will not be happy when generals interrupt their

radio communications to hold a high-priority VTC. In addition, any network problem can affect every user and every service. The enemy need only locate this Achilles' heel to cause considerable disruption. Currently, the multiplicity of totally separate systems provides redundancy, and alternative means can be found to convey vital information.

Network-centric warfare potentially has the most to offer in the areas of CS and CSS. At the formation level and above, sustaining operating tempo (OPTEMPO) is a logistics issue as much as a kinetic one. Combat units can rotate from the front line, but to sustain warfighting, logistics must flow continuously. A formation's OPTEMPO and freedom of action depends on its logistics. In the Persian Gulf in 2003, the 1st U.K. Division suffered a shortage of basic items, from uniforms to body armor, and organic ammunition arrived late. These items were not decisive to the conflict, but having ammunition and body armor arrive late greatly affected morale and disproportionately affected postconflict politics. In another example, the U.S. 5th Corps paused during its advance into Baghdad largely because of logistics necessities. The need for logistics capable of supporting commanders maneuver desires has remained a lesson "unlearned" for many years.

In a recent British Army "Continuous Attitude Survey," the public perceived Army logistics as being more efficient and successful than that of the United Parcel Service (UPS).⁷ The truth, however, is that the British Army has little idea of what it owns and even less of where it is. UPS tracks every item it delivers through every pickup and dropoff point and makes this information available in real time to customers and suppliers. Other industries depend on just-in-time (JIT) logistics to reduce costs and maintain a competitive edge, but the Armed Forces have been lethargic in adopting such enabling technologies as bar-coding, Web-enabled databases, and satellite-based barcode tracking.

While JIT logistics does not provide the crucial reserve of capabilities a formation needs to survive the unexpected, just in time is better than the just too late logistics of recent operations. Adopting best practices from industry must be tempered by military reality. We cannot procure uniforms and ammunition from an international market without sig-

naling intent. There is also no latent industrial capacity to produce such materiel overnight in the quantities a major operation requires.

While information-gathering enhances intelligence, it must also improve understanding, but it cannot do this if the volume of information is indigestible. Without understanding, however, formations might win battles, but they will not win wars. Technology and the network are only enablers of this process. Enhancing the corporate understanding of a large army requires thought in gathering information and conveying it quickly. The CIS commander must provide the end-to-end services that enable the mission. He must understand technology's benefits and the need for knowledge, not data, to support military and political objectives.

Updating technology is an evolutionary process, which everyone in the organization must understand. A "maneuver" approach is required. We must understand the desired end state, which is not battle-winning technologies, but war-winning capabilities. Inserting technology into military decisionmaking is a challenge because change creates friction. Bowman delivers many new capabilities for network-centric warfare, but will require more than 3 years from its initial delivery until units are equipped and trained in its use. Taking full advantage of Bowman at the division level in combat, CS, and CSS organizations will take several more years. While the technology is a step change, the increase in capability will be evolutionary across the British Army.

Command and control must evolve with the communications network. The relationship is absolutely vital for network-centric warfare. Each system on the network depends on all the others, and all are linked to warfighting. Only by understanding current systems and processes can we proceed to the future with confidence. **MR**

NOTES

1. Operation Telic is the British codeword for operations in Iraq.
2. British Ministry of Defence (MOD), "Operations in Iraq—Lessons for the Future" (December 2003), on-line at <www.mod.uk/linked_files/publications/iraq/opsiniraq.pdf>, accessed 7 October 2004.
3. Bowman and the associated combat application are the new radio and battle command systems being introduced into service in the British forces.
4. The 1st Marine Division, Operation Iraqi Freedom (OIF) Lessons Learned, May 2003.
5. High assurance guards are devices that protect against the passage of unauthorized information.
6. Data convergence includes voice, video, and data on a common communications "backbone," such as the Internet Protocol.
7. The "Continuous Attitude Survey" is conducted annually by MOD's research agency, QintIQ.

Major James A.G. Langley, British Army, is the British Exchange Officer at the Battle Command Battle Laboratory (G), Fort Gordon, Georgia. He received an Electrical and Electronic Engineering Degree from Nottingham University. He has served in various positions in Great Britain, South Africa, Kosovo, Canada, and the United States.