The Technology of War: The advantages of a network-centric approach to modern warfare

Network-centric warfare provides military operations with information superiority – but it doesn’t work without a battle-ready wireless communication system. Barry McElroy is Vice President of Rajant explains.

While the reasons we go to war – land, religion, retribution, resources – have not changed much over the millennia, warfare itself has changed dramatically, especially in recent decades.

No longer is a battle a linear operation with clearly defined lines and trained soldiers in uniform firing artillery at each other, as it was for much of the 20th century. To fight a war in the 21st century means fighting an enemy who is everywhere and nowhere at the same time, who has not been trained in battle formations or military strategy, who does not wear a uniform or use WoRm formulas to calculate where to fire.

There are no battle lines – anywhere in a targeted country is a free fire zone, and the enemy is constantly moving and changing where they attack from. There is no symmetry – a solitary person can destroy a group of soldiers and their vehicles using an improvised explosive device (IED) or rocket.

Twenty-first century warfare requires that soldiers are constantly on their guard and ready to fight – and this need for always-on preparedness has changed the way the military collects and uses intelligence, giving rise to what’s called “network-centric warfare”: the use of networked technology to provide advantages on the battlefield.

The benefits of the network-centric approach

A network-centric approach to warfare links all military assets to each other and to decision makers via computer, radio and data networks, enhancing the way military objectives are accomplished because of information superiority: According to David S. Alberts, who formerly worked in the office of the Assistant Secretary of Defense for Networks and Information Integration, “A robustly networked force improves information sharing. Information sharing and collaboration enhance the quality of information and shared situational awareness. Shared situational awareness enables self-synchronization. These, in turn, dramatically increase mission effectiveness.”

A Department of Defense text adds that while war will always be characterized by “fog, friction, complexity and irrationality,” network-centric operations provide increased awareness and more informed decision making: “... Having a better near real-time picture of what is happening ... certainly reduces uncertainty in a meaningful way.”

This method requires a powerful communications network, however. A true military-grade network must provide continuous communication to in-motion and stationary personnel, vehicles and equipment, giving commanders and troops always-connected, secure access to applications and information – thus improving situational awareness and mission effectiveness. There is no room for security breaches or outages of any kind when it can mean the difference between life and death, or a war won or lost.

Communications have sometimes been a weak link between the various moving parts of the armed forces, whether between ground, airborne and seaborne forces, or between forces and
non-aligned units such as foreign coalitions or sister services within the Department of Defense. However, this has been changing in recent years as military operations and projects have begun utilizing a network called kinetic mesh.

**Kinetic mesh on the battlefield**

A kinetic mesh network combines wireless network nodes and networking software. It employs multiple radio frequencies and any-node-to-any-node capabilities to instantaneously route data via the best available traffic path and frequency, with up to 300 Mbps transfer rates.

If a certain path becomes unavailable for any reason – due to antenna failure, for example – nodes on the network use an alternate route to deliver the data, eliminating any gaps in communication and allowing on-the-fly transmission of voice, video and data to provide situational awareness, despite conditions that would cripple other networks. Routes are built automatically, and are evaluated for quality and performance for every sent and received packet.

There is no central control node and no single points of failure. These self-healing, peer-to-peer networks support Wi-Fi, integrate easily with Ethernet-connected devices and scale to hundreds of high-bandwidth nodes – in fact, the more nodes added, the more pathways are established and the more resilient a network becomes.

The nodes self-configure, making it simple to expand the network, and are built to withstand hostile environments like battlefields. Each node serves as a singular infrastructure, which enables within the network to be mobile: wireless nodes can move, clients can move, network traffic can move – all in real time and without manual intervention.

A Kinetic mesh network can be easily redeployed and expanded in multiple ways, and still operates with the same level of reliability, even in the harshest conditions. It eliminates the challenges of time-consuming, complicated deployments in the midst of battlefield pressures, challenging terrain and changing operations: All a soldier has to do is hit a power button on the radio, and the radio immediately connects to the network and is up and running. A soldier doesn’t need extensive training to learn how to set up a radio, and a company no longer needs to lay new cable every time its headquarters moves, which requires man-hours and taxpayer dollars.

Not to be overlooked is the network’s military-grade level of security (with some radios certified to “Secret and Below” interoperability). Kinetic mesh delivers end-to-end, 256-bit encryption. When encrypted information flows through the mesh and comes out another node, it stays encrypted all the way through, and is not decrypted until it is delivered to its final destination, ensuring privacy. At each hop in the network, kinetic mesh provides a per-hop authentication for each packet. Metadata also is encrypted; an attacker cannot analyze the traffic and see which nodes are communicating with other devices – which, in a battlefield situation, could give away position.

**Kinetic mesh action**

Kinetic mesh has been a part of several military programs and projects, including:

- **C-RAM:** The C-RAM program is a “system of systems” that primarily uses radar to detect incoming projectiles (rockets, artillery and mortars) fired from hostile forces. An engagement weapon then attempts to intercept the projectile and destroy it in flight before it impacts. There also is a warning component; once the radar has determined the trajectory of the projectile, it can determine what kind of shell or projectile it is, as well as estimated point of impact, to determine the blast radius. It then can send an alert to the affected area, instructing all personnel to seek cover. A soldier has about 10 seconds to find cover before detonation if the projectile is not intercepted in flight – which does not sound like a lot of time, but can mean the difference between life and death.

The C-RAM program was an important counter measure to enemy fire during the wars in Iraq, where the way the enemy fought made it impossible for troops to deploy counter fire – because there was simply no one to fire at. Instead, the enemy would set up crude stands with rockets on top and use a triggering device to deploy the rockets from afar. It was by no means a scientific method of warfare, but it was intermittently effective, killing or injuring soldiers and disabling military assets.

- **Wolfhound:** Wolfhound is a man-portable electronic warfare and cyber capability supporting kinetic operations in Operation Enduring Freedom. The system includes three networked, man-packable nodes capable of detecting, identifying and direction-finding conventional communications. It targets Very High Frequency (VHF) or Ultra High Frequency (UHF), push-to-talk, handheld radio communications, and is a counter-IED program.

The use of IEDs is an example of the unconventional military tactics seen in the asymmetrical warfare of the late 20th and early 21st centuries: By burying artillery shells strategically in roads and other areas where troops traveled, an enemy can injure or kill soldiers and damage military assets – all without needing to take aim or even remain in the area.

IEDs were used extensively against US-led forces in Iraq and were responsible for nearly 2,000 deaths between July 2003 and January 2009. Since Wolfhound’s inception, however, the program has prevented the detonation of more than 1,000 would-be IEDs and is expected to save many more lives in the future.

**The need for real-time communications in modern warfare**

Technology is constantly changing everything we do. Ray Kurzweil’s Law of Accelerating Returns asserts that the rate of change in systems – including technology – increases exponentially, not linearly, meaning that each advance doubles the rate of the next: “30 steps linearly gets you to 30. One, two, three, four, step 30, you’re at 30. With exponential growth, it’s one, two, four, eight. Step 30, you’re at a billion.”

If this theory holds true, we will continue to see lightning-fast technological progress across every part of our lives – including the way we conduct combat operations. As warfare becomes more unpredictable and asymmetrical, a network-centric approach will be ever more critical – without real-time communications enabling information superiority, all the artillery in the world won’t make a difference. Kinetic mesh networks provide the mobility, reliability, scalability, security and high bandwidth needed to ensure mission-critical intelligence is sent and received in real time, breaking new ground in wartime communications and helping to save lives.

**GMC**