Military & Aerospace Electronics
CELEBRATING 25 YEARS 1990 2015

The evolution of networked sensors

May 12, 2015

From the dawn of military sensor networking during Vietnam to today's struggle against insurgents and IEDs, military mobile sensor networks strive for ever-higher bandwidth and resolution, and smaller more lightweight platforms.

BY **J.R. Wilson**

Technology has been the force multiplier giving the U.S. military growing superiority over its adversaries since World War II, and battlespace dominance since the Reagan build-up of the 1980s. Military technological dominance has come at a cost, however, and that cost is asymmetrical warfare.

Much of this shift started during the 1960s in Vietnam. As America gained total air dominance in South- east Asia, and precision-guided air- and sea-launched weapons decimated traditional enemy military formations. In response, adversaries turned to insurgent warfare with small units, no heavy armor, or even aircraft. Instead they relied on improvised explosive devices (IEDs) as suicide and vehicle bombs.

That, in turn, placed a growing U.S. military emphasis on the equipment and capabilities of small units-even down to the individual warfighter. The lack of a definitive "front line" during the Vietnam War created a critical need for every Army and Marine Corps land vehicle independently to sense, locate, define, and respond to high-, mid-, and low-tech localized weapons.

The WIN-T system is among the first combat vehicle networking technologies to provide reliable data, imagery, video, and voice networking capabilities to combat forces on the move.

This is no small feat; it requires significant improvement in sensors to detect dangers, situational awareness to map threat locations, and vehicle networking to ensure all other vehicle crews are aware of the dangers.

Fast-forward to today. The ability to perform technology refresh and insertion into existing vehicles became part of original design parameters after 9/11, allowing for relatively quick and on-site upgrades in many instances.

Such new technologies, however, rely on continuous research and development, funding for acquisition and fielding, training for users and maintainers, and development of next-generation vehicles, sensors, networking, and related capabilities.

That evolution has been slowed, deferred, or shelved due to declining military budgets, military downsizing, and, most significantly, sequestration. All that comes at a time of increasing geopolitical instability, rising Chinese military technology, a resumption of Russian military adventurism, and demand for U.S. Army and Marine Corps units across a wider global distribution than any time since the end of the Cold War.

U.S. and allied combat vehicles are receiving secure networking equipment at an accelerated rate for enhanced situational awareness and targeting capability.

Defense leaders testifying before Congress during this year's budget hearings were unanimous in saying the funding trends of the last few years have forced the services into quixotic choices-none of which bode well for the future of U.S. combat operations.

Vehicles as sensor platforms

On the one hand, technology makes it possible for land vehicles of all sizes to carry an array of sensors and communications equipment. On the other hand, severe funding cuts have left little money for the research and development necessary to upgrade and replace such systems.

"We know that we need a middleweight, mobile, protected firepower platform to allow early entry forces to seize and exploit the initiative," says Gen. Daniel Allyn, Army Vice Chief of Staff. "Our tanks and Bradleys are the finest fighting platforms in the world, but they're heavy. You've got to seize a major airfield to get them in. You'll see, in the future, some equipment that's not quite so heavy, but enables us to have tactical mobility."

A summer 2014 demonstration at Fort Bragg, N.C., saw six defense contractors exhibit their proposals for such a vehicle. Proposals included the General Dynamics Flyer, the Boeing-MSI Defense Phantom Badger, the Polaris Defense deployable advanced ground off-road DAGOR, the Hendrick Dynamics Commando Jeep, the Vyper Adamas Vyper, and the Lockheed Martin High Versatility Tactical Vehicle-a version of the UK Army's HMT-400 Jackal.

The U.S. Special Operations Command already has awarded a contract to General

Dynamics Land Systems in Sterling Heights, Mich., for its Ground Mobility Vehicle 1.1 (aka, Flyer) to meet a similar need, but even lighter vehicles may be necessary, says Lt. Col. Kevin Parker, light systems branch chief in the Mounted Requirements Division.

Requirements for an ultralight combat vehicle (ULCV) include a maximum empty weight of 4,500 pounds, the ability to carry a nine-man infantry squad and their equipment (3200 pounds), a range as far as 300 miles on one tank of gas, size to fit inside a CH-47 Chinook heavy-lift helicopter, air-droppable by a C-130 Hercules or C-17 Globemaster cargo aircraft, and by sling load on a UH-60 Black Hawk medium-lift helicopter. It also must have the power and computing capability for advanced sensor and communications suites.

"Nobody had ever asked industry for a 4,500-pound vehicle that can carry nine guys and still be highly mobile and have a long range," Parker notes. "We had requirements that are hard, but that's what we need the vehicle to do."

Meanwhile, development of the ULCV's sensors, situational awareness, and networking equipment also is moving apace, subject to further funding restrictions.

The Army's WIN-T technology makes use of a sophisticated infrastructure of vehicle antennas and rugged on-board networking routers to keep warfighters abreast of battlefield developments as they unfold.

Third-generation FLIR

At a Washington conference in March, Army Acquisition Executive Heidi Shyu said the Army is ready to convert 16 years of research on a third-generation Improved Forward Looking Infrared (IFLIR) electro-optical sensor into a program of record for Abrams tanks and Bradley infantry vehicles. The IFLIR is expected to enable troops to discriminate between

shovels and rifles, tanks and commercial trucks.

In April, Raytheon and DRS Technologies announced they have teamed on development of the IFLIR in anticipation of the procurement announcement. An Army request for proposals is expected in this month, leading to an engineering and manufacturing program and production award in the early 2020s.

"The new third-gen technology will dramatically improve the range performance of ground combat vehicle sensors, allowing greater standoff range and identification capability," says Clay Towery, senior manager for business development at Raytheon EO Innovations in Richardson, Texas. "It's very important to the Army and it will provide a significant combat advantage and it's critical that we field this technology to maintain combat overmatch."

The current second-generation FLIR, fielded on more than 20,000 Army, Marine Corps, and Navy platforms in the past decade, uses a linear scanned array that sweeps across its field a view. The third-gen will use staring focal plane arrays that do not sweep but use several detectors on an image plane, thus gathering significantly more information. It also is capable of simultaneous detection in mid- and long-wave bands.

"The Army and our team have a strong track record of delivering state-of-the-art, next-generation FLIR technology on our nation's premiere ground vehicle combat platforms," Sally Wallace, DRS C4ISR group president, said in a statement. "Our experience integrating a common FLIR across the Army's combat vehicle platforms is critical to synchronizing the Army's modernization strategy."

Sensors also are key to improved situational awareness. Blueforce Development Corp. in Salem, Mass., offers this definition of the complexity of field-level situational awareness:

"The asymmetric threat has moved us to a network-centric concept of operations where chaos and non-predictiveness replaces past eras of order; where today's coalition or interagency workgroup presents a different membership tomorrow. Operational approaches require the complete and total embrace of tactics and technology that address the ultimate in complex adaptive systems where we operate and interoperate in denied, dysfunctional, and disparate last tactical mile environments. These operating environments require complete mobility, but also agility given the non-predictive nature of disasters and manmade incidents."

The latest increments of the Army WIN-T program make use of lightweight, fast, and maneuverable vehicles to ensure that networking capability keeps up with leading elements on the battlefield.

Vehicle situational awareness

One situational-awareness initiative at the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., is the Ground X-Vehicle Technologies (GXV-T) program to improve the survivability of ground-based armored fighting vehicles through crew augmentation-improved physical and electronically assisted situational awareness for crew and passengers.

GXV-T also involves semi-autonomous driver assistance and automation of key crew functions similar to capabilities found in modern commercial airplane cockpits to reduce onboard crew and training requirements.

According to DARPA's GXV-T program office, potential approaches include:

- a closed cockpit that would use visualization technologies to provide high-definition, wide-angle visibility of external conditions;
- path planning that would display optimal routes;
- sensors that would use a variety of technologies to visualize surroundings and identify and track allies and adversaries;
- terrain classification that would evaluate surroundings for optimal travel surfaces; and
- autopilot capabilities that would automate routine driving tasks to enable drivers to focus on more strategic activities.

"Ground-based armored fighting vehicles and their occupants have traditionally relied on

armor and maneuverability for protection. The amount of armor needed for today's threat environments, however, is becoming increasingly burdensome and ineffective against ever-improving weaponry," the Agency reports.

"GXV-T seeks to develop revolutionary technologies to enable a layered approach to protection that would use less armor more strategically and improve vehicles' ability to avoid detection, engagement and hits by adversaries. Such capabilities would enable smaller, faster vehicles in the future to more efficiently and cost-effectively tackle varied and unpredictable combat situations."

While some efforts to improve situational awareness are complete system proposals, some defense contractors have developed independent components, such as the BAE Systems CHECK-6 Rear-View System, which uses thermal or color cameras embedded into military-style LED taillights-thus offering commonality across military vehicle types-to provide ground vehicles with a rear vision system.

"This innovative solution provides a streamlined path for vehicle installs that can be accomplished as a field-upgrade kit requiring few tools and minimal vehicle downtime," according to BAE. "Check-6 delivers needed battlefield situational awareness during all weather, day and night operations. (It) is in production and currently supporting 40,000 armored combat and tactical wheeled vehicles across the Joint Armed Forces."

This British Army Combat Vehicle Reconnaissance (Tracked)) being operated across the harsh desert terrain of Afghanistan by soldiers of the 9th/12th Royal Lancers.

Small, fast movers

Providing each vehicle with independent sensor suites and situational awareness is a major step forward, but new battlefield environments-with fast-moving small vehicles, threats from hidden IEDs and two- or three-man insurgent teams with rocket-propelled grenades (RPGs),

sudden attacks from the cover of civilian crowds, hospitals, schools, etc.-make real-time sharing of each vehicle's (and individual warfighter's) information even more critical. But networking on the move involves a number of problems, from jamming and spoofing to encryption and available, reliable bandwidth.

"Bandwidth is probably the biggest problem with all that data. LOS [line-of-sight] is another issue, trying to reach the soldier over the horizon. If you use a satellite, you're going to have a latent connection. Crunching big data numbers strikes me as more a software issue. As far as our wired network, Gigabit Ethernet is more than sufficient to handle most traffic, with 10 Gigabit Ethernet coming on fast and 100 Gigabit Ethernet also developing rapidly. Wireless is needed to connect everyone on the battlefield," says Ronen Isaac, general manager of military Ethernet specialist MilSource in El Segundo, Calif.

"The requirement is two-fold. One is interoperability and flexibility, where systems need to share information. Flexibility comes in with open architecture; where things are inherently interoperable, everything speaks the same language, so getting them to speak together is a software issue rather than the much more difficult physical. Which is much easier to do in the software- defined world we're moving to.

"The second is SWaP-C [size, weight, and power-cost]. Because IP is an open platform, the commercial world is able to provide lower cost, high reliability products that are not necessarily specialized. So you can take advantage of COTS with an open standard. And with our current budget situation, cost is a major driving factor. SWaP goes back to leveraging the commercial aspects of IP and having various vendors using IRAD [independent research and development] to come up with devices that are smaller, lighter, and require less power, but meet the same specs as their larger counterparts."

The next generation of on-board systems also will require multi-task rather than specialized systems, he added, in order to further reduce SWaP and leave more room in the vehicle for crew and passengers.

"So instead of having a mission computer and a router, you would put those together. Same with GPS-all saving space, weight and power. There is a push for that now and we have answered it with some of our technology, but we will see a lot more of that in the future-which, in turn, means a growing demand for more compute power, more capacity," MilSource's Isaac says.

"We're starting to see a connected battlefield where you have soldiers and vehicles on the ground, UAVs, and command stations all needing to share video, voice, situational

awareness, etc. The only way to connect all those is via IP networking because we can use currently available routers and switches. We're seeing some companies mounting radio hardware, with core-switching and routing hardware, inside autonomous vehicles and essentially using those as giant moving antennas. But a bigger problem, in the short term, is security. If the platform is captured, how do you get its data off, then destroy it, before the enemy can use it?"

Power over Ethernet allows for the reduction of cables on a mobile platform. A MILTECH 910 POE Ethernet switch can provide connectivity and power to sensors, cameras, and other devices.

Common sensor networks

Since 2009, the Army has been working under a directive to develop "as is" and "end state" network architectures to guide network development, procurement and enhancement. The Army Network Architecture Strategy-Tactical version was crafted in response to this directive, with the Common Operating Environment (COE) architecture serving as a key component of that guidance.

"With a COE, the Army can establish a framework similar to industry best practices. One of these Army COEs is the Sensor Compute Environment (CE), which addresses the sensor interoperability questions of: (1) am I using the right sensor standards, (2) am I exchanging data with the correct format, and (3) am I exchanging relevant data. Sensor CE will provide a common sensor interoperability layer, implementing standards and technology for specialized, human-controlled or unattended sensors. This effort is applicable to future UGS

[unmanned ground systems]," says Clair Guthrie, sensor computing environment chair at the U.S. Army's program executive office for PEO intelligence, electronic warfare & sensors.

Without the operator having specific knowledge of the available networked sensors, Sensor CE enterprise services include the ability, subject to mission priorities, to:

- identify the existence and determine the capabilities of sensors on a network to support a mission requirement;
- distribute summary event information from sensor observations to the network with a pre-defined distribution and level of priority;
- obtain full motion video streams from sensors;
- request specified sensors on a network to perform operations; and
- request specified sensors for remote management of sensor operations.

In the expanding paradigm of military adaptation of commercial developments, one of the top requirements is for faster military acquisition and fielding of new sensor, networking, and situational awareness technologies-and doing so before potential adversaries accomplish the same goal using the same openly available technologies.

"Science and Technology Trends 2013-2043: A Review of Leading Forecasts," sponsored by Deputy Assistant Secretary of the Army for Research and Technology Mary Miller, aggregated and analyzed trends from multiple sources and identified, at a macro level, 16 megatrends of significance to the military, including robotics and autonomous systems, human augmentation, big data, 3D printing, the Internet of things and ubiquitous nanotechnology.

Commercially developed technology

"One observation from the report was how sensors-including detection technologies, measuring tools and self-aware feedback mechanisms and their supporting technology development areas, such as data fusion, algorithm development, energy harvesting and networking-were consistently identified as key science and technology (science and technology) enablers across most of these trends. It is imperative to the Army's future effectiveness and efficiency to accept and adapt to the rapid pace of change driven by these global commercial trends," according to Susan Harkrider, deputy director of the Modeling, Simulation & Netted Sensors Division at the Communications-Electronics Research Development and Engineering Center's (CERDEC's) Night Vision and Electronic Sensors Directorate (NVESD).

"Known as the Integrated Sensor Architecture (ISA), this framework identifies the critical capabilities to be adopted for sensor interoperability. This strategic approach enables program management offices to instantly refresh their programs with the latest technology and adapt existing Army portfolio assets to this new environment. Thus the Army could leverage the often very fast development cycle of cheap commercial sensor technologies (like those on cell phones) and integrate them into cross-domain solutions with existing, expensive and unique military sensors (like those on satellites and military platforms)."

Harkrider views sensors as "the glue that enables the Army to embrace the global trends shaping warfare in 2025 and beyond".

"How the Army chooses to embrace global changes and commercial trends will determine in many ways how successful it is in maintaining technical superiority. Concepts like ISA are but one approach to helping the Army maintain agility in a rapidly changing world. Establishing the adoption of common standards and protocols can be very challenging when working with so many different communities, all of which have different opinions on what 'right' looks like," she says.

Achieving those goals has become an increasingly difficult circle to navigate: Today's warfighters must have vehicles of all types that offer integrated sensor suites and networking to facilitate enhanced situational awareness, for that vehicle and its occupants as well as all other friendly forces in the area. That must be achieved at the lowest SWaP-C possible, which requires funding of new research and development to adapt commercial technologies-and, in some cases, create military-specific elements. All of which need to be accomplished under severe budget restrictions-especially the possible return of sequestration-and a backdrop of fielding urgency to enable the U.S. military to maintain its technological edge over any potential adversaries.

The shrinking of components and platforms has allowed the consolidation of multiple platforms. The Techaya MILTECH 9012X contains an Ethernet switch, an embedded single-board computer, and a GPS receiver.

Budget constraints

But as the Army's budget director, Maj. Gen. Thomas Horlander, told reporters in February, funding for research and development is at its lowest point since the turn of the century. At that same briefing, deputy budget director Davis Welch added that while the Army has not terminated any programs, continuing to allocate science and technology funding through 2025, several programs have been delayed-including the future infantry fighting vehicle and full-on-the-move tactical networking.

The latter also is a major blow to Marine Corps modernization plans, which rely heavily on Army research and development. Brig. Gen. Joe Shrader, head of the Marine Corps Systems Command, told a House Armed Services Subcommittee hearing on Army Ground Force Modernization plans that delaying development and fielding of Networking-on-the-Move "leaves two-thirds of our operating forces without the ability to conduct mobile networking in distributed environments." That deficit becomes even more dangerous if they face a future enemy that does have such a capability.

"The Army's modernization budget remains near historic lows. Still, our modernization mission-to develop and procure systems that allow our soldiers to dominate across the full spectrum of operations-remains essential. We must always ensure our soldiers have the right equipment, at the right time and at the right place to accomplish the assigned mission,"

Lt. Gen. Anthony R. Ierardi, Army Deputy Chief of Staff, and Lt. Gen. Michael E. Williamson, Military Deputy to the Assistant Secretary of the Army for Acquisition, Logistics and Technology, told the HASC subcommittee.

Among those programs they identified to lawmakers as "critical [to] provide overmatch capabilities at the tactical and operational levels of combat operations" were:

- Joint Battle Command-Platform (JBC-P), the next generation of Force XXI Battle Command Brigade and Below/Blue Force Tracking and "the foundation for achieving affordable information interoperability and superiority on current and future battlefields [as] the principal command and control/situational awareness system for the Army and Marine Corps at the brigade level and below." The Army requested procurement funding for 2988 vehicle platform computer systems, 300 command post systems, satellite receivers, encryption devices, ancillary equipment, program management support, training, fielding, publications, support equipment and post deployment software support.
- Warfighter Information Network-Tactical (WIN-T), which "provides broadband communications for the tactical Army [extending] an IP-based satellite and LOS communications network throughout the tactical force, supporting voice, data, and video." Funds were requested to upgrade 31 WIN-T Increment 1 units to enhance interoperability with units fielded with WIN-T Increment 2, procure 248 communications nodes for WIN-T Increment 2 and continue fielding and support for previously procured WIN-T Increment 2 Low Rate Initial Production (LRIP) equipment.
- Distributed Common Ground System-Army (DCGS-A), which provides integrated ISR processing, exploitation and dissemination of airborne and ground sensor platforms, giving commanders at all levels access to the Defense Intelligence Information Enterprise and leverages the entire national, joint, tactical and coalition ISR community.

The FY16 funding request supports correction of any issues identified during the May 2015 Limited User Test, support for the Increment 2 Request for Proposal and milestone decisions, including plans to begin Increment 2 development, as well as modernize and procure COTS software and hardware components for DCGS-A (fixed, mobile and data centers), integrate hardware and software and equip and train next deployers and high priority units.

Network cyber security

Each new technology incorporated into combat vehicles, especially those involving data

exchanges with other vehicles and command centers, also brings an increased need for data security and more research and development funding requirements for the growing field of cyber security-and thus a further drain on available funds.

"Network dominance and defense is an integral part of our national security. The Army is focused on proactively providing increased capabilities to the Joint force. The evolving cyber environment is forcing the Army to adapt to cyber threats by transforming processes, organizations and operating practices to mitigate vulnerabilities," the generals told Congress.

"In terms of new and emerging initiatives, the U.S. Army Cyber Command and the Army acquisition community are pursuing ways to bring 'big data' analytic capabilities to Army operations in order to improve our cyber defense capability. These efforts, as well as cyber science and technology initiatives focused on the enabling technologies for future capabilities, will generate resourcing requirements which will compete against other modernization priorities."

In an increasingly unstable world where demands on ground forces-and threats to them-grow even as the U.S. military and its budget downsize, the technology explosion that has given those forces a decisive edge in recent decades now may be turning against them.

"Army equipment modernization enables the U.S. Army to remain the world's decisive land force. Soldiers and units operate as part of joint, inter-organizational and multi-national teams that are tailorable and scalable to the mission. As we continue to examine how to achieve effective balance among force structure, modernization and readiness, we must have stable, predictable, long-term funding to modernize our force to meet evolving threats and execute our mission," Ierardi and Williamson warned lawmakers.

"The security challenges of tomorrow will be met with the equipment we develop, modernize and procure today. Because adversaries will continue to invest in technology to counter or evade U.S. strengths and exploit vulnerabilities, resource reductions and insufficient force modernization place at risk the Army's ability to overmatch its opponents."