

# Defeat IED Missions

## Defensive Electro

By John Haystead

Although “booby traps” as a weapon of warfare and terrorism have been around since the beginning of human conflict, the term, Improvised Explosive Device (IED), has now become firmly entrenched in the public lexicon and become synonymous with asymmetric warfare. The Radio Controlled IED (RCIED) is a term equally familiar to anyone in the EW community. Today, however, the nature of the threat and, in particular, the opportunities and challenges presented by the incorporation of advanced and readily-available commercial technology are forcing military planners to think beyond just the deadly devices themselves and adopt a much broader view of the “improvised threat.” Add to this the reality that improvised threats are not just confined to asymmetric warfare environments, they can also be widely-implemented and highly-effective in full-scale, state-to-state conflicts between modern, top-tier forces.

Of necessity, the Services have developed, funded and fielded counter-IED systems in multiple ways depending on urgency of need, as well as individual Service requirements and preferences to include established acquisition channels and Quick Reaction Capability (QRC) fast tracking. That situation continues today and, in fact, is further complicated by the expanding requirements of the task.

As the result of the widespread use and effectiveness of IEDs in Iraq and Afghanistan, the Joint IED Defeat Organization (JIEDDO) was established in 2006 to lead and co-ordinate all DOD activities involved in work aimed at defeating the devices. Although the Navy initially

managed the DOD's Joint CREW program for JIEDDO, in November of 2013, most of that responsibility was transferred to the Army under its Program Executive Office for Intelligence, Electronic Warfare and Sensors (PEO IEW&S).

Also, in July of this year, in recognition of its expanding mission area, the JIEDDO was reclassified as a Combat Support Agency and its name changed to the Joint Improvised Threat Defeat Agency (JIDA). Says RDML Brian Brakke, JIDA Deputy Director for Operations, “The JIEDO was originally stood up to provide a zero to two-year time frame response to immediate needs on the battlefield, but what the Department has seen is that this threat is enduring, it's a global threat, and so we needed to make the organization enduring as well, with the initial focus on improvised explosive devices, but also looking at the threat in a larger sense and understanding and trying to anticipate the improvised threat as a whole.”

### RADIO CONTROLLED IEDS (RCIEDS)

No-one is more threatened by IEDs than the soldier on the ground. Noting his personal experience working counter-IED missions during two deployments to Afghanistan, COL Jeffrey Church, Army EW Division Chief, HQDA G-3/5/7, says, “From a user's perspective, I would say that the IED is here to stay. I don't think that we're going to fight in any future conflict, at any level, from non-state actors to nation-states, where you don't see IEDs, and that's because they have proven to be extremely effective against a very modern army. They're not new, but



they've become more effective and more lethal, and we will continue to see them.”

Specific to the RCIED threat, the Army has fielded a number of Counter RCIED EW (CREW) systems including the mounted CREW 2.1 Combined Vehicle Receiver/Jammer (CVRJ) and Mobile Multi-Band Jammer (MMBJ) systems, both produced by Exelis Electronic Systems, now Harris (Clifton, NJ). The CREW CVRJ systems are also in service with the US Marine Corps. The Army's latest mounted system is the AN/VLQ-12 CREW Duke V3 system built by SRC Inc. (North Syracuse, NY). Although a once-planned CREW 3.2 system has not been advanced, the Duke system has been undergoing continuous upgrades.

SRC is currently working with the Army to upgrade a select number of VLQ-12 (Duke V3) systems to the ULQ-35 (Duke V5) configuration. According to Jim Periard, SRC Assistant Vice President, EW & Communications, “this hardware upgrade of the Duke Primary Unit is the culmination of the first phase of the on-going

# n Expands to nic Attack (DEA)



Duke Technology Insertion (DTI) hardware upgrades to primarily address technology obsolescence and improve system capabilities. A similar hardware upgrade to the Duke Secondary Unit is in its initial requirements and definition phase. In parallel, software, firmware and loadset upgrades are continually in development for insertion into the full family of fielded Duke systems from Duke V2 through Duke V5.” Periard explains, “Since SRC’s EW systems are software defined, they are continually developing and demonstrating other missions that the baseline hardware can support. Examples of complementary functions that have been implemented and demonstrated include counter-UAS, advanced ES and EA techniques, embedded communications and EM sensing and mapping.”

The Army’s dismounted RCIED systems include the Thor III and Baldr CREW 3.1 systems, both built by Sierra Nevada Corp. (Sparks NV). Originally fielded through the Quick Reaction Capability (QRC) pathway, the systems were ultimately retained as formal Programs of Record (PoR). In 2014, Sierra Nevada and Northrop Grumman Information Systems (Herndon, VA) both received contracts from the Marine Corps for CREW Marine Expeditionary Unit Special Operation Capable (MEUSOC) dismounted systems.

As stated by USMC Systems Command, “The Marine Corps has a requirement for both dismounted and mounted CREW systems. The current Thor III dismounted system will be replaced by the CREW MEU dismounted system, which is currently in

source selection. The current mounted CREW system used by the USMC is the CREW Vehicle Receiver Jammer Version 2 (CVRJ (V)2). The Mounted CREW requirement is currently being updated by the Deputy Commandant, Capabilities Development and Integration. Upon receipt of the validated updated requirement and associated funding, the Marine Corps will pursue the acquisition of a replacement mounted CREW system.”

Meanwhile, late last year, Northrop Grumman received Milestone C approval for its JCREW 3.3 or Increment 1 Build 1 (I1B1) system from the Naval Sea Systems Command (NAVSEA). The JCREW I1B1 system is being developed for mounted, dismounted, and fixed-installation use through a common open architecture.

Colonel Church describes the Army EW Division’s role in defeating RCIEDs as helping to get requirements validated so that a material solution can be fielded, beginning with working through the Training and Doctrine Command (TRADOC) Capabilities Manager (TCM). “They produce the requirements for the kind of system that will be needed to defeat an RCIED. For example, when we fielded the Duke CREW system, it went through a requirements process. Although a lot of these systems first came on as quick re-

action capability, Duke has been able to transition from a QRC to a program of record. So, we work with the TCM to establish the requirements, and they come to Headquarters Department of the Army to get those requirements validated. Once validated, they go to PEO IEW&S - PM EW & Cyber (previously PM EW), who then work with industry to get the material solution that meets those requirements. That’s our role in the counter-RCIED fight and, with the Duke system, it continues to be improved, the PM continues to work with industry, and there is continual improvement and expanded ways to use system.”

## BEYOND THE DEVICE

As observed by Colonel Church, “Because we’ve become very good at defeating the RCIED, the enemy has transitioned to a whole variety of other IEDs – victim operated probably being the most effective (see “Multi-Sensor Approach to Pressure-Activated IEDS” on p. 38). The EMS doesn’t provide an opportunity to defeat that signal, because there is none. But, can the EMS be used to do other things to aid in the process? Sure, we ran programs in Iraq and Afghanistan targeting other components of IEDs, some funded by JIEDDO, and some proved effective. What we’re focused on now with the TCM is future Defensive Electronic Attack (DEA). That system is designed, or will be designed, and the requirements will be to defeat more than just RCIEDs. If an adversary weapon system uses the RF spectrum in any way, then DEA is

designed to protect personnel, equipment and facilities from those kinds of RF-enabled weapons. You can sort of think of DEA as a 'Super Duke' system."

Part of the expanded capabilities of this next-generation Duke will be an ability to synergistically combine EW with cyber operations to conduct "protocol-based attacks." In this scenario, instead of jamming the communication signal between an IED or multiple IEDs and their triggering device, a fast-acting virus of sorts is introduced into the com-

munication link's software itself, rendering it useless.

The growing importance being placed by the Army on cyber operations in conjunction with EW is reflected in the recent name change of "PM EW" (within PEO IEW&S) to "PEO EW and Cyber," as well as changing the name of the subordinate Product Manager CREW organization to Product Manager Electronic Attack.

Although the Army has fielded a number of QRC stand-alone counter-IED and other EW systems, the next planned

stage for DEA is to integrate these capabilities into a more efficient and effective next-generation capability called the Multifunctional Electronic Warfare System (MFEWS). As envisioned, MFEWS will enable a major shift from the primary use of EW as a counter-IED tool for convoy and dismounted squad-level protection to an offensive weapon to be used against an enemy's overall command and control systems. The Army is also interested in collecting and consolidating data from IED attacks into an intelligence database that can be used to locate and identify signals-of-interest, such as those used to trigger IEDs remotely. Duke systems, for example, have an event log that can be used for this purpose.

The Army is now at the "very beginning" of an Analysis of Alternatives (AoA) for DEA. Says Colonel Church, "The Material Development Decision (MDD) has been written by the TCM, and the MDD is a precursor to the AoA, but right now, I don't have a timeline for an Initial Operating Capability (IOC). It's still 'FYXX,' but in the meantime we have Duke."

#### ATTACK THE NETWORK

Beyond the IED itself, the larger mission of defeating improvised threats encompasses the entire development infrastructure, or the network behind their manufacture, deployment and control. For example, as described by RDML Brakke, "When you look at ISIL, they're using IEDs differently than anyone has used them in the past. They're using massive amounts of IEDs that require mass production. It's a well-orchestrated organization and they're not just limiting themselves to the Syria/Iraq area. We see them expanding globally, working with other terrorist organizations such as Boko Haram and the establishment of Islamic State Khorasan (ISK) in Afghanistan. What we've found is that, if you look at the network behind IEDs as a cone, at the apex of that cone is the IED. Then if you work out in concentric rings, you see that there has to be someone that emplaces that IED, someone that builds it, places to store the materials to build them, and pathways over which they are brought in. There also has to be an R&D phase and a list of components and dual-use electronics



JAMMING SYSTEMS

GERMANY



[www.hp-jammer.de](http://www.hp-jammer.de)

that have all had to come through this illicit framework.”

The Army’s G-38 Office for Adaptive Counter-Improvised Explosive Device/ Explosive Ordnance Disposal Solutions (ACES) Division manages the train of Overseas Contingency Operations (OCO) funds needed to sustain new counter-IED capabilities and systems once they have been proven in theater and until the Army decides whether they will make them programs of record, sustain them, or terminate them. It is also the Army’s lead organization to JIDA.

Says Colonel Dick Larry (ret.), prior chief of, and now Senior Technical Advisor to G-38, “Remember there are three lines of effort: Attack the Network; Defeat the Device; and Train the Force. As we look to the future, the whole idea of attack-the-network is truly where we are all going. At the end of the day, the whole discussion of anonymity, identity operations and identity activities, are all targeted at attacking the network. We’re all recognizing that if you go after the network, and you can get the financier, the builders, all those things, you can

prevent the IED or whatever other disruptive technology.”

In terms of planning for improvised threats beyond the traditional IED, the Unmanned Aerial Vehicle (UAV) has to be considered. While UAVs offer tremendous promise as platforms for counter-IED systems and missions, they also have very real potential to be used as improvised threats themselves.

Says RDML Brakke, “The enemy adapts and improvises as he needs to, so as long as the counter to what he’s using currently isn’t there to force him to change into another area, he’s probably not going to do it. But, for example, DAESH (acronym of ISIS/ISIL/IS in Arabic – al-Dawla al-Islamiya fi al-Iraq wa al-Sham) used vehicle-borne IEDs as a very precision methodology to strike against the Iraqi Security Forces (ISF). If that was taken away from them, what would they use next for precision? A logical next step would be to turn to an aerial platform to maintain that precision strike capability.”

G-38’s Larry points out that dealing with the UAV/UAV-IED threat is “truly an interagency effort. DHS is leading

an effort involving a number of agencies including DOD on the whole issue of these threats. DHS is really focused on the Homeland piece, with the DOD more focused on the Outside the Contiguous US (OCOUS) piece, and then collaborating on what we both see as best practices and lessons learned. The Army’s Asymmetric Warfare Group (AWG) has been working for a number of years looking at how Unmanned Aerial Systems (UASs) and UAVs can be used at the tactical level. It’s an increasingly prevalent threat and people are talking about it more and more, but it truly is a combined effort between multiple agencies within the federal government.”

SRC’s Periard notes that SRC has supported a variety of counter-UAV demonstrations with prototype EW capabilities over the last several years including the Joint Integrated Air and Missile Defense Organization’s (JIAMDO) “Black Dart” exercise (a two-week test of tactics and technologies to combat hostile drones). SRC software ties together the company’s AN/TPQ-50 counter-fire radar with the CREW Duke counter-IED



Our products and systems cover the full range of Electronic Support (ES) and Electronic Attack (EA) disciplines for tactical and strategic environments.

**gew** technologies

INNOVATIVE INTELLIGENCE

marketing@gew.co.za www.gew.co.za

system and AeroVironment's (Monrovia, CA) "Switchblade" drone.

### EXPANDED ROLE FOR JIDA

As described by RDML Brakke, JIDA's focus right now is on addressing the requirements laid out by the Joint Requirements Oversight Council (JROC) in its memorandum of 2013 which divided the counter-IED area into six operational capabilities and a number of operational tasks. Three of these capabilities are the familiar: Detect IEDs and IED components; Neutralize IEDs, and Mitigate the effects of IEDs, but the others are to: Identify the threat networks, Distribute IED related material, and Train on the counter-IED capabilities.

"That training piece is also very important," he explains. "The JROC, in understanding the interoperability of the systems, came out with what they call the 'convoy planning tools,' where operators could plug in the different systems, whether you had active or reactive systems, understand how big the bubbles of protection were, whether or not you had systems on each one of your vehicles or not, and you could determine the spacing to have protection for your entire convoy. The other thing that they have taken into account is the need to map the electronic environment, to understand how our systems would respond and react in a given situation or an environment. This is something that we will try to continue to partner with industry to try to gain

a better understanding globally of the environments that our systems will be going into, so that we can ensure that the warfighter understands the actual capabilities of the system as it moves through the environment."

Sensors and system miniaturization are another focus for JIDA. "Particularly for airborne systems," says Brakke, "we're looking at ways to make payloads smaller to put multiple sensors on a platform or make them suitable for UAVs. We're doing a lot with UAVs, but from the sensor perspective, not the platform. Although, initially, the organization did get into some vehicle purchases, Congress said 'you don't need to be buying the platform, you need to be buying the sensors and developing the sensors.' So that is where we have refocused our efforts. We let the Services decide what the platform is, and then we see how we can miniaturize the capability to support that."

IEDs and other improvised threats are not restricted to the battlefield. They are also a major threat domestically. And, as a result, JIDA is also now finding itself working with other US government agencies, such as the Department of Homeland Security (DHS) and other border security and law enforcement agencies, in providing support for the DOD's role in homeland defense. In this theater, Brakke again emphasizes the need to attack not just the actual threat devices, but the entire network supporting them. "You need to map up that network and then recog-

nize that, although our authorities within Defense can't counter that entire network on our own, we can leverage the community of action within the other government agencies that do have authorities in those areas, whether commerce, treasury or someone else. We can then get them to apply leverage against that network and have effects as well."

### QUESTIONS REMAIN

One big question regarding JIDA and how its counter-IED efforts will be conducted in future surrounds the conversion of JIEDDO to a Combat Support Agency (CSA), its future funding sources, and particularly how this may impact its ability to provide for rapid development and delivery of essential new counter-improvised-threat capabilities and systems to the battlefield.

Colonel Church points this out when he says, "As a user in theater, JIEDDO always meant to us that, if it involved IEDs, we could get something we needed, that worked, right now. JIEDDO had the ability to cut through all of the bureaucracy it seemed, and they had money to accomplish the technical solutions that were needed. So, if you had a challenge, whether it was something to do with exploitation and you had to go to one of the labs, you could get that work done. If that work produced a target, and you didn't have an ability to prosecute that target, you could go through JIEDDO and get that done."

**SIGINT Sensors for Military Operations**

**Replacements for M/A Com, ComSol, Watkins-Johnson**

**FEI-Elcom Tech, Inc.**  
[www.FEI-ElcomTech.com](http://www.FEI-ElcomTech.com)  
201.767.8030 x280

- Rapid Response RFP / RFQ Support
- High Spurious Free Dynamic Range
- COTS Solutions (1U/2U)
- Exceptional Signal Sensitivity

**New 80MHz Instantaneous B.W.**

**20 MHz - 3 GHz Receiver**

**500 MHz - 18/26.5 GHz Receiver/Converter**

G-38's Larry says that part of the concern they have with JIDA becoming a CSA, is that "they are really kind of redefining their role. As their new name implies, they're aperture is broadening and they're now looking at improvised threats and improvised weapon systems and the whole idea of disruptive technologies to include IEDs. We're all trying to wrestle with what that means because, at the end of day, there are already organizations that do pieces of that between either OSD organizations or the CSAs or even the Services themselves. So, it's not quite clear yet what the future is going to be for JIDA."

Pointing out that JIDA will become operational at the beginning of next month, and will not be fully operational until next year, Larry says funding is a big part of the discussion. "[In the past,] JIEDDO has had the ability to use colorless funding, the ability to change funding levels to Other Procurement Army (OPA), Operations and Maintenance Army (OMA), or RDT&E. But, as we look to the future, they will have a base budget, which covers staff and infrastructure, but how much will they really get of colorless money? If they don't receive adequate levels, it will be really hard for them to do those things that they did in the past six or seven years. So, as we get to FY17 and beyond, that is going to be an interesting dynamic."

Larry also notes that JIDA is shrinking. "They're no longer going to be the

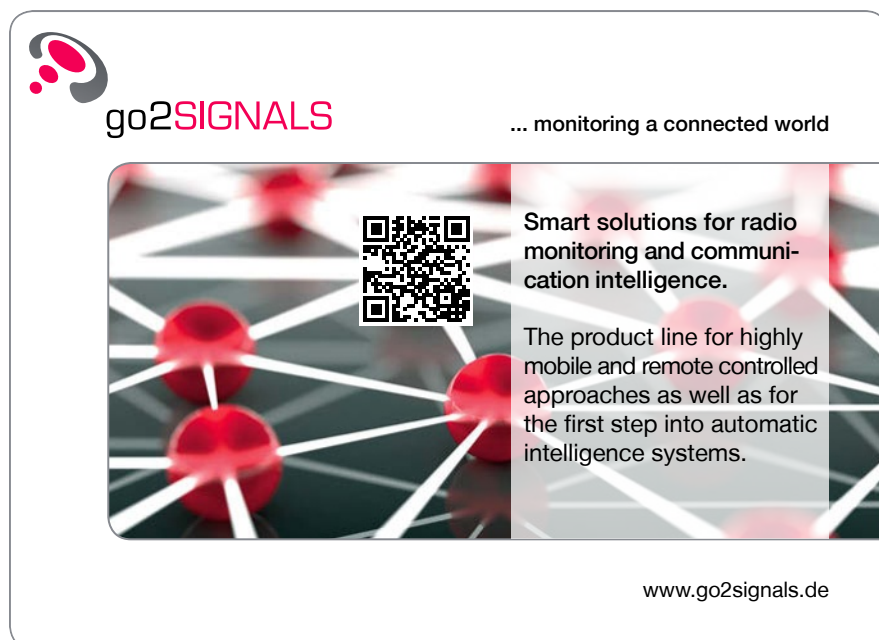
3,000 people they once were. Right now, they're down to about 975, and ultimately they have to get down to 400 people. That's a much smaller organization and they won't have the same latitude, or the people, to do these things. Again, that's where they have to go back to the Services and start leveraging what the Services and others can bring to the fight. It's really going to have to be a true cohesive 'Kabuki dance' between the Services, OSD and other organizations such as the FBI and others as to how we do this, because they're going to be much smaller."

Colonel Church shares Larry's concerns. "JIEDDO was very instrumental in rapidly fielding urgently-needed systems to the field, from small things that mounted on the front of your vehicle to entire tractor trailers, and going against the most current threat of IEDs in Iraq and Afghanistan. I don't work for JIDA, but I would definitely hope that as they have their role defined, and as they become smaller in size, that they don't lose the ability to rapidly affect events on the battlefield, because there are going to be more events, not less. What we don't need is another bureaucracy to go through to get solutions. We have plenty of those. JIDA's key to success for the warfighter is being able to rapidly observe, assess and apply solutions. They need to keep doing that."

For his part, RDML Brakke says that even though its organizational status within DOD is changing and its mission expanded to deal with all manner of improvised threats, JIDA will maintain its focus on providing rapid solutions to the field. Even so, however, he admits that this will be a challenge in terms of obtaining and managing their funding. "JIDA will now become part of the POM process as an enduring organization. So as opposed to, previously, when all of our funding was through Overseas Contingency Operations (OCO), now we will have to go through the process of determining a base budget and determining what is funded through base and what is funded through OCO."

As part of this, Brakke says JIDA will have to strengthen its ties with DARPA and the Service laboratories, "leveraging each others' authorities in the areas that we work in. If we can influence and help affect what is in the zero to two-year timeframe, and then help shape what is five years and beyond, that's kind of our role and responsibility - to look at our problem set and say 'can you guys start thinking about this for us, so that it can trickle down to the point that we can have an effect and change in the zero to two-year timeframe?' Although as new (QRC-type) systems transition over to the Services, and our requirement to fill that gap kind of steps away, we will still maintain an understanding of the threat and an understanding of the network and continue to be part of the CREW Community of Interest (COI) and their working groups. So, if there were a need to accelerate something that the Services were working on, that would become our responsibility, to respond and create an answer on the battlefield faster than maybe the POM process."

RDML Brakke also emphasizes that he believes DOD will continue to focus on the IED as a major threat area, "When you look across the globe, you have currently non-state actors almost trying to act like state actors, and you have state actors trying to act like non-state actors. That puts you into an area that the Services can't always be prepared for all those contingencies through the Program Objective Memorandum (POM) cycle. That's why we need to endure as an organization and be that rapid response (path) to a problem



**go2SIGNALS** ... monitoring a connected world

Smart solutions for radio monitoring and communication intelligence.

The product line for highly mobile and remote controlled approaches as well as for the first step into automatic intelligence systems.

[www.go2signals.de](http://www.go2signals.de)

that boils up that hasn't been thought of or that a solution set wasn't created for. The permanency of us as a Combat Support Agency strengthens our ties with the combatant commanders and allows us to continue to leverage the community of action that we have developed along the IED approach to look at other improvised threats as they emerge."

Ultimately, Colonel Church agrees, pointing out that his office is currently working with JIDA to accelerate the delivery of a required system in theater. "So, we can work through the normal acquisition processes, we can go through the rapid equipping force, we can do QRCs, but JIDA still has a role in fulfilling material solutions so as not to have delays due to

funding requirements. We will still have JIDA to try to accelerate the delivery of those systems to theater. They are still relevant because that system (that we are discussing with them now) will defeat RCIEDs and it will defeat other things in the RF spectrum, so JIDA can help us. And, I am sure they will continue to help us in future." ✍

## MULTI-SENSOR APPROACH TO PRESSURE-ACTIVATED IEDS

Of course, RCIEDs are not the only type of IED. In fact, the proliferation of IEDs in countries such as Chad, India, Thailand, Mexico and Colombia (to name but a few) has largely been characterized by pressure-activated IEDs buried in the ground – sometimes several feet under the surface of a road or footpath. The terrorists and insurgents who make these pressure-activated IEDs usually use whatever materials are at hand, such as metallic cooking plates, wood, wires and even plastic syringes filled with chemicals. Because of this diversity of materials, technologies and placement tactics, ground forces need sensor systems that can reveal what is in the ground.

In Iraq and Afghanistan, the successful deployment of RCIED jammers beginning in 2005 essentially forced the enemy to begin using pressure-activated IEDs. This trend, in turn, led the US Army to fund development of a new counter-IED system that mounted a multi-channel Ground Penetrating Radar (GPR) from NIITEK (Dulles, VA) onto a Husky mine-clearing vehicle. The resulting Husky Mounted Detection System (HMDS), based on a time domain radar design, proved very successful at detecting IEDs made from all types of materials and buried at various depths. The original HMDS program was established in October 2007 in response to a Joint Urgent Operational Needs State-

ment (JUONS) from CENTCOM, and the systems were sent into Afghanistan beginning in 2009. This quick response allowed the system to support CENTCOM's critical needs, but it did not allow for proper long-term planning for the HMDS program.

In 2014, the Army re-designated the HMDS as a Program Of Record (POR), which indicated that the Army intends to keep the system over the long term. But, as the threat evolves, so must the HMDS evolve. Today, the Army is upgrading the HMDS in a three-phase program. In October 2013, the US Army awarded a sole source contract to NIITEK to transition the HMDS to a POR based on the systems fielded to Afghanistan. These systems were recently designated HMDS Increment A Configuration 1 (A1) and use NIITEK's Visor 2500 GPR in a four-panel configuration mounted to the mechanical arms at the front of the Husky vehicle. The HMDS A1 configuration is scheduled to achieve Initial Operational Capability (IOC) in early 2017. This will also become the standard export version of HMDS for the next few years. The USMC, as well as Canada, Turkey, Spain and Australia operate HMDS units acquired over the past several years. They are likely to bring their systems up to the A1 standard in order to sustain them more easily in the future.

In December 2014, NIITEK, which is part of Chemring PLC's Sensors and Electronic Systems business, won an engineering and manufacturing development contract for HMDS Configuration A, Increment 2 (A2). This effort

# ARS Products

## Communications Band Receiver Range Extension Products



ARS Model 176- Low Band VHF Co-Location Canceller

We also design & manufacture an extensive line of switch matrices & RF signal routers!



Model 701- HF Distribution System

- Adaptable Multi-Couplers
- Programmable Notch Filters
  - Selectively attenuate interfering signals
  - High power versions available
- Co-Located Cancellers
  - Referenced & referenceless versions
  - Attenuate co-located transmitters
- Non-Reflective Limiters
  - These receiver protectors do not reradiate the limited signal

**30 Crabtree Lane**  
**Woodstock, CT 06281**

**860-963-7743**  
**www.arsproducts.com**

will upgrade the radar, which was originally optimized to operate in desert environments like Iraq and Afghanistan, and improve its performance across a wider variety of environments and soil types. The A2 configuration will also add a metal detector to provide better detection of metallic objects, especially those buried deeper in the ground. For the Husky operator, the A2 will also fuse the sensor inputs from the GPR and the metal detector onto one screen to reduce operator workload. The program also provides embedded training for operators. Increment A2 will go through Critical Design Review (CDR) next year and see a Milestone C production decision in 2017. Full-rate production is slated for late 2018 and IOC is expected in 2020.

HMDS Configuration B, which is still in the planning stages, calls for a "Semi-Autonomous Capability" (SAC) for the HMDS. The goal of this effort is to allow the HMDS operator to sit in a Buffalo Mine Protected Clearance Vehicle (an MRAP hull that is fitted with large tires and equipped with a long arm to dig for located IEDs) positioned at the front of a convoy and remotely operate the Husky vehicle and HMDS sensor suite.

Aside from NIITEK, Chemring Sensors and Electronic Systems (CSES) operates a separate GPR manufacturer named 3d RADAR. With design engineers in Norway and manufacturing in Charlotte, NC, 3d RADAR (which was an HMDS competitor until NIITEK acquired it from Curtiss-Wright in 2014) offers a commercial radar design that is more easily exported than the NIITEK GPR, according to Juan Hernandez, vice president of business development at CSES. The GPR offerings from 3d

RADAR use a step-frequency radar, which is also operated across a spectrum of environments. In the commercial world, 3d RADAR's GPR is used for a variety of applications. However, 3d RADAR's GPR is garnering attention from several potential military buyers. The British Army already operates 3d RADAR's GPRs on unmanned Land Rovers as part of its Talisman route clearance capability, and several other countries are looking at military counter-IED applications for 3d RADAR GPRs.

The acquisition of 3d RADAR enabled Chemring to strengthen its position in the counter-IED market by offering the Husky or other vehicles to international customers with either the NIITEK or the 3d RADAR products. The company is extending both product lines to address a wider array of vehicles, especially Unmanned Ground Vehicles (UGVs). Countries, such as South Korea, are looking at integrating the HMDS onto domestically developed UGVs. The UGV option is attractive because it allows the operator to perform the route-clearance mission with less risk.

Another type of counter-IED detection system that is gaining acceptance among users is handheld IED detection systems. Originally developed for the US "surge" in Afghanistan, when NATO soldiers increased the number of "off-road" patrols, the hand-held GPRs are used to detect and locate pressure-activated IEDs and metallic or non-metallic threats. As with the HMDS A2 configuration, multiple sensors provide a better picture than a single sensor. Chemring has partnered with MineLab of Australia to offer the GROUNDSHARK handheld IED sensor system, which combines NIITEK's two-channel GPR with MineLab's metal detector. The GROUNDSHARK alerts the operator to potential threats via visual cues, audio alerts and vibrations in the handle. Outside the US, GROUNDSHARK has been bought by the Polish Army, as well as the Turkish Army, and it is in trials with many other countries.

Another dual-sensor, hand-held IED detector is the Minehound VM3G, which was jointly developed by Germany's Vallon GmbH and Cobham Antenna Systems of the UK. Cobham provides the system's GPR while Vallon supplies the magnetometer. Like the GROUNDSHARK, it alerts the operator with visual, audio and vibration cues. Cobham also offers the Amulet Series Quadpack GPR System, housed on a small UGV and based on a four-channel GPR from the company. A larger version of the Amulet system is offered on a Land Rover.

Chemring's Hernandez says that countries are getting smarter about using counter-IED systems. "Some countries that are newer users still have to learn that they can't simply turn on the HMDS or Ground Shark systems and use them all the time over every inch of road," he says. The US, UK and other experienced users have learned that intelligence plays an important role in the counter-IED mission and helps to narrow down the areas where IED activity is suspected along a route. This allows the counter-IED systems to be used where they are most needed, and allows the convoys and foot patrols to move faster when they are not in a suspected IED threat zone. Overall, the technology is getting better, and a wider set of military users is gaining valuable experience. This is a good trend, because insurgents and terrorists are constantly finding new materials and new tactics for their buried IEDs. – J. Knowles

# STEATITE





## Q-PAR ANTENNAS

**EW and SIGINT ultra -wideband antennas, subsystems and consultancy**

**High performance antennas typically operating 100 MHz to 140 GHz for a wide range of applications:**

- Surveillance
- Spectrum Management
- ELINT & COMINT
- Radar & EW Threat emitters
- ECM & ESM
- Radar warning receivers

Designed and manufactured to the highest standards

Tel: +44 (0) 1568 612138 • Fax: +44 (0) 1568 616373

Web: [www.steatiteqpar-antennas.co.uk](http://www.steatiteqpar-antennas.co.uk) • Email: [sales@q-par.com](mailto:sales@q-par.com)