COUNTER-IED MEASURES: ELECTRONIC WARFARE

By Tushar Malhotra, Aerospace & Defense Analyst, MarketsandMarkets

Improvised explosive devices, popularly known as IEDs, are the new weapons used by insurgents which have led to massive damages to the military and civilians in the past few years. These devices can be triggered from a distance via a remote control by an operator from a safe distance. IEDs can be made using complex machinery or by simple daily use objects such as a wrist watch or a mobile phone. IEDs can cause collateral damage and injuries as they may contain chemicals, radioactive materials and biological materials that are deadlier than the injuries caused from shrapnel, fire and concussive blasts.

High use of IEDs was witnessed in recent wars in Iraq and Afghanistan where insurgents used improvised explosives to destroy military bases, disturb the communication systems and in many cases caused the confusion among the military personnel as to the origin of the attack.

*CBRN: Chemical, biological, radiological and nuclear

**HMG: Heavy machine gun

***RPG: Rocket propelled grenade

Source: Defense Journals, White Papers and Newsletters.
IEDs are key threats which need to be look forward to protect against in the coming five years. IEDs are currently the major cause of fatalities of armed forces, who are primarily locked in counter-insurgency operations facing an enemy who is almost unseen, often indiscriminate, and always dangerous. The overwhelming sentiment here suggests that this type of warfare will linger for at least next ten years and will lead to continued operations in the Middle East and potential conflict in North Africa. Vehicle armor demand will be on the higher side in these regions as it is a priority for the military forces deployed there as a counter IED measure.

Counter Radio-Controlled Improvised Explosive Device Electronic Warfare (CREW) systems are vehicle mounted and man portable systems which are used to counter remote controlled IEDs. Military personnel are trained thoroughly on usage of these CREW systems to interrupt the communications links of an IED. With the success of CREW in Iraq by the American armed forces, more demand has been witnessed for such systems in the recent times.

One of the highly used CREW systems is the AN/ULQ-35 Counter Remote Controlled Improvised Explosive Device (RCIED) Electronic Warfare (CREW) Duke system. It a vehicle mounted device capable of neutralizing remote controlled IEDs providing the military with the tactical advantage. This product is manufactured by SRCTec, Inc. based in New York, U.S. The company was recently awarded a contract worth $59.3 million by the U.S. Army for the CREW Duke system. About 60,000 of these Duke systems have been provided to the U.S. Army which includes vehicle mounted and portable systems. The AN/ULQ-35 Counter Remote Controlled Improvised Explosive Device (RCIED) Electronic Warfare (CREW) Duke system features superior protection performance, low power consumption, user friendly operation, MIL-STD-810F compliant and can be used in varying temperature conditions. U.S. Army’s Top 10 Greatest Inventions included the Duke system in both 2005 and 2009. Another widely used system to protect against RCIED is the protective modular jamming system STAR V 740, developed by URC Systems. Thor III is man-portable jammer that is built by Sierra Nevada Corporation and provides the user with a wearable RCIED jammer to counter diverse threats.

CREW systems are made up of a number of components that can protect a soldier from the IED threat. The successful mitigation of a threat is the result of advanced technology, strategic tactics and knowledge about the possible insurgent locations. Following are some of the components of a CREW system that provide the requisite counter RCIED solutions:

1. Antennas: Antennas disrupt the communication link between the IED signal receiver and the remote control. Antennas can be multi-directional or omni-directional and have individual characteristics and capabilities.
2. Threat load: The techniques, controls and commands are together known as threat loads and are interfered with the communication links which is employed with the hardware. Threat loads are based on the amount of communication interference beyond which the IED can be detonated.
3. Hardware: Hardware includes the actual jammer and its components. These hardware systems provide the linkage of systems to interrupt the communication link of an IED.
4. Software: Software allows modifications and updates to the hardware. These modifications allow for improving the capabilities of the system to counter IED’s communication links with respect to range and loads.

In February 2014, U.S. Department of Defense entered into a contract with Sierra Nevada Corporation and Northrop Grumman Corporation for the indefinite delivery of dismounted CREW systems for Marine Expeditionary Unit. The contract was worth was $90,000,000. The army is also expected to upgrade the combat vehicle fleet of more than 1,600 Abrams tanks and 2,500 Bradley infantry combat vehicles. The up gradation would include Counter Remote-Controlled Improvised Explosive Device Electronic Warfare (CREW) Duke v3 for the Bradley vehicles.
The CREW systems are widely used by military and law enforcement personnel to detonate the RCIEDs. This has significantly dropped the casualties of RCIED attacks. CREW systems form a major part of the electronic warfare on today's battlefield. Rising demand for counter IED systems would strengthen and fuel the demand for electronic warfare market. The global electronic warfare market was $12.15 billion in 2014 and is expected to register a CAGR of 4.50% to reach $15.59 billion by the end of 2020.

The rise in the conflicts and territorial disputes between various nations in the Middle East and Asia-Pacific regions has increased the need for electronic warfare measures. Modern land systems are progressively more dependent on information systems comprising communications & information systems, and networks & sensors. These systems have the potential to produce significant changes in the behavior of warfare. As a result of the use of information-age systems, there has been a significant change in the nature of battle-field. North American region drives the electronic warfare market and the U.S. leads globally in the expenditure towards electronic warfare system.

Raytheon (U.S.), Alliant Techsystems, Inc. (U.S.), BAE Systems (U.K.), Rockwell Collins (U.S.), IAI Elta (Israel), and L-3 communications (U.S.) are the key players for the electronic warfare market, globally and account for more than 40% of the total market share. General Dynamics Corporation (U.S.), SAAB (Sweden), Thales (France), and Teledyne Defense Ltd. (U.K.) are other prominent players in the electronic warfare market.

Other counter-IED systems include the anti-tank, anti-personnel mine and IED detection systems for which the market is currently estimated to be worth $443.70 million and $298.61 million, respectively. They are also expected to reach $440.20 million and $278.12 million by 2020, respectively.

Tushar Malhotra
Aerospace & Defense Analyst
MarketsandMarkets