Picture credit: Crown Copyright

SEARCH AND DESTROY

Will Higham *explains how a layered approach can be used to successfully counter IEDs*

Improvised Explosive Devices (IEDs) are a prevalent threat in almost all modern conflicts. Their improvised nature, readily available componentry and easily accessible manufacturing guidance make them a flexible and comparatively cheap weapon. They consist of five main elements: a main charge, an initiator, an explosive, a trigger and a power source; with one or all of these elements being homemade (or improvised) for the device to be classed as an IED. The main charge can be commercially available, homemade or recovered from unexploded munitions. Historically, IEDs have made use of almost any available commercial technology that can pass a signal or complete a circuit – a good example of the use of Commercial off-the-shelf (COTS) technology to reduce design and delivery risk.

This vast range of design options gives IEDs the flexibility that makes them both a pertinent threat and increasingly difficult to counter. Consequently, there should always be numerous layers of protection measures. By discussing a number of these layers in the context of wider counter IED considerations, this article aims to highlight one often under considered layer: RF Signal Distribution.

As the measures used to counter IEDs will vary depending on the design and make-up of the device, it is therefore necessary to group IEDs into types, so that effective countermeasures can be implemented. One way of doing this is to group IEDs via their Delivery and Trigger mechanisms; the former being how the IED is delivered to its target and the latter being how the device is initiated or triggered.

This highlights two central counter IED approaches: protecting the target and preventing detonation. The former aims to prevent getting the IED close enough to the target (ie stopping the delivery mechanism), and the latter aims to stop the device from exploding (ie disabling the trigger mechanism). The UK's National Counter Terrorism Security Office builds on this definition by expanding on the trigger and delivery mechanisms to support the implementation of specific countermeasures.

Behavioural measures that prevent predictable repetition are a primary countermeasure that makes the effective positioning of an IED very difficult

Potential targets can be grouped into two categories based on the applicable IED countermeasures: static and mobile. Static targets are permanent (or semi-permanent) locations such as military or government buildings and are typically protected through measures such as physical barriers. These barriers are positioned a safe distance away from the target so can mitigate vehicle borne delivery mechanisms.

Mobile targets are typically specific people such as soldiers who, by nature, often change location making fixed barriers unsuitable. Consequently, behavioural measures that prevent predictable repetition are a primary countermeasure; for example, regularly changing travel routes and times makes the effective positioning of an IED very difficult.

Even with effective target protection measures, there are still occasions where IEDs will impact on the populace and therefore need to be dealt with; in these cases preventing IED detonation becomes key. The remote nature of an RCIED trigger mechanism makes it a favoured method of detonation for adversaries, meaning Electronic Counter Measures (ECM) – a primary RCIED countermeasure – are essential.

ECM is equipment that prevents the use of Remote Controlled (RC) triggers to detonate an IED and is often integrated onto vehicles and carried by soldiers to provide protection at all times. The UK's National Counter Terrorism Security Office describes RC triggers as commercial electronics, including: radio, wi-fi, Bluetooth, personal mobile radios, mobile phones, cordless phones etc.

Generally ECM delivers its effect through jamming, which is where the ECM equipment emits a Radio Frequency (RF) signal to interfere with the detonation signal from the RC trigger such that the IED cannot correctly interpret the signal and does not detonate.

IEDS' FLEXIBILITY MAKES THEM BOTH A PERTINENT THREAT AND VERY DIFFICULT TO COUNTER.

Complex algorithms are often used for this interference, with more advanced ECM equipment supporting more complex algorithms that ultimately deliver improved IED detonation prevention capabilities. However, an illustrative and open-source example of jamming, taken primarily from Radar ECM, is barrage. This is where the ECM equipment emits RF signals of sufficient power over a sufficiently broad frequency range that the trigger signal is indistinguishable – in essence, it raises the noise floor. This requires a significant amount of RF power, noting that signal strength exponentially reduces with distance.

Although an open-source example linked to Radar ECM, barrage jamming highlights the importance of RF power. Therefore, effective signal distribution that minimises any losses between the ECM equipment and its antenna is an essential consideration for effective ECM equipment, especially noting the potential for long cable runs via Through Armour Connections (TAC) in military vehicles.

Traditional signal distribution is the use of analogue RF signals via copper coaxial cables, which gives significant losses in RF power over anything other than short distances. Therefore, in instances such as integrating ECM onto platforms, the use of alternative signal distribution methods should be used to reduce RF losses. This is especially pertinent as the RF losses increase with frequency, and the current trend is to use ever-increasing frequencies.

There are two main alternatives that provide improved RF signal distribution: digitised RF signals over fibre and analogue RF signals over fibre. Both of these approaches use fibre optic cabling instead of coaxial, but have different pros and cons making each more suited to different use cases.

Analogue RF over fibre is a comparatively simple approach that converts electrical signals from the ECM equipment into an optical signal for transmission along the fibre cable, then reconverts at the antenna for emission (noting this process is reversed for receive applications). Digital RF over fibre is the same approach as analogue RF over fibre,

but includes additional analogue-to-digital and digital-to-analogue conversion steps at the ECM equipment and antenna(s) respectively.

The digitisation step in the digital approach packetises the analogue data so that a networking function, typically a network switch, can manage the distribution of the data to the intended destination. As this distribution is typically managed using Ethernet and Internet protocols, digital RF over fibre is often referred to as RFoIP. One of the key benefits of Ethernet and IP is that it decouples the network architecture of a system from its components, so there is no upper limit in terms of growing the size of the system. A secondary, but notable, benefit is that RFoIP inherently supports the time stamping of data, which can be particularly important in specific use cases such as direction finding.

Although analogue RF over fibre is often only considered in a point-to-point network topology, there is a number of commercially available and proven technologies that provide an analogue networking function. Examples of this include PPM Systems' range of COTS products from ViaLite Communications; the AR1-K, AR2-K and AR3-K product suite that can support tree or bus network topologies or the AR4-K product that supports a star network topology through its fan-in fan-out networking capability that is software controlled for dynamic re-configurability.

This type of analogue networking uses physical routing mechanisms, so there is an inherent limit on how large the system can grow once the number of connections has been set. However, this is less of a constraint where the physical size of the platform or location puts an inherent constraint on the potential size of the system.

Analogue distribution additionally has the benefit of being frequency agnostic, in that the upper frequency limit is set by the electro-optic conversion, whereas the components for digitising and networking in the digital distribution approach can very quickly become the limiting factor for larger frequency ranges. This is due to the digitising and networking functions requiring larger, more complex and more costly equipment as the frequency range increases. In turn, this typically makes the digital approach less suitable for wideband frequency applications and/or in space constrained environments, such as platforms.

Regardless of the chosen distribution approach, even if this is a hybrid of the two, the type of fibre optic cabling is also an important consideration. Single-mode fibre optic infrastructure provides a versatile foundation as it is suitable for both approaches, whereas multimode fibre (that is often used in digital networks) is only suitable for the digital approach.

Fundamentally, there is no 'silver bullet' for effectively Countering IEDs, there should always be several layers of protection with decision makers never relying too heavily on any one layer. As a minimum, these protective layers should include procedures / tactics to avoid IED's, physical protection measures to disrupt IED delivery mechanisms and if required, ECM to inhibit remote controlled trigger mechanisms.

Where ECM is required, although the capability of the ECM equipment will play the primary role in its effective implementation, the type of signal distribution is also significant, so should always be given due consideration. As part of the signal distribution, the pros and cons of the two approaches should also be considered to select the most appropriate one, noting that this could be a hybrid of the two ●

Will Higham is PPM Systems Director of CEMA. Having worked in both the MOD and industry, Will has a wealth of experience of delivering complex mission systems and platform integration, with recent focus on the MOD's next generation CEMA capability delivery.

ECM prevents the use of remote controlled triggers to detonate an IED and is often integrated onto vehicles and carried by soldiers to provide protection at all times

Picture credit: US Dept Defense