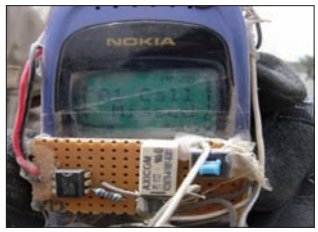
Defeating Improvised Explosive Devices

Dr Carlo Kopp

Improvised Explosive Devices (IED) have been the defining feature of the insurgency in Iraq, accounting for more personnel losses than any other single weapon, and IEDs are increasingly a feature of the insurgency in Afghanistan. While overall personnel losses to enemy action in Iraq were tenfold lower in total compared to the Vietnam conflict of forty years ago, what is much less visible is the long term legacy of maimed and otherwise traumatized Service personnel, many of whom will be hospitalised for decades to come.



Mobile phone used as an IED detonator found in Iraq. (US Army)

The popularity of IEDs in the globalised Islamo-fascist insurgency is due to the relative ineffectiveness and high cost of more conventional insurgent tactics, in which insurgent losses generally exceeded Coalition personnel losses by a large margin. Suicide bombers have also proven an expensive and only infrequently effective tactic. IEDs on the other hand provide the attacker with opportunities to stand off and evade, or if these are unattended, simply egress the area before Coalition troops even arrive.

The technology of IEDs is diverse. The explosive component of most IEDs in Iraq comprised cached or otherwise dispersed military munitions, ranging from Russian FAB-500 aerial bomb bodies at the high end, to 155 mm artillery rounds, landmines, and smaller calibre artillery shells at the low end. The most sophisticated explosives technology seen in Iraq were Iranian supplied self-forging plate warheads, based on similar technology to the US Sensor Fused Weapon, and arguably a conventional anti-vehicular/anti-personnel mine rather than IED in the conventional sense of the term.

The triggering technology used to initiate IEDs is no less diverse. The simplest designs use traditional mechanical triggers such as wires, landmine pressure plates and other mechanical devices, which rely on the victim to perturb the IED and set it off – this is the traditional 'booby trap' approach.

Far more effective have been remotely triggered IEDs, where an observer chooses the most advantageous time to set off the IED. This might involve waiting until the escort vehicles in a convoy pass over the IED, setting it off when a truck carrying personnel or combustibles passes the device, or waiting till the scouts in an infantry unit pass and the main body of the unit is exposed.

The least sophisticated technology for remote triggering is to bury a telephone cable or similar wire, connecting the triggering device to an electrical detonator in the IED. This method is time consuming but can provide the best concealment.

More sophisticated wireless technologies have since emerged, improvisations that first appeared in Northern Ireland, and later in terrorist bombings in Israel and its occupied territories.

Cellphone technology has been a favourite, as mobile telephony has been the predominant consumer end communications technology in most developing nations. A disposable cellphone is opened up and an electrical detonator of suitable sensitivity attached across the speaker terminals. The ring tone sets off the device.

Aftermath of an IED detonation in Iraq. (US Army)

Other wireless technologies have also been applied to IEDs. Microwave remote control devices for toys, garage or shopping centre door opening sensors and similar infrared beam devices have all been adapted for IED applications. Cheaply available as consumer goods globally, such devices are impossible to control and thus readily available in the retail and wholesale market.

Defeating IEDs is complex and difficult, in a large part due to the sheer diversity in triggering systems and explosive devices used, as well as creative thinking in IED emplacement – road-kill carcasses being one of many clever ideas applied. Technologies and tactics effective against one category of IED may be quite ineffective against another.

Mine resistant hardened vehicles are arguably the most effective of all the technologies, but are inherently limited to IEDs set up to ambush road vehicles. Once the troops dismount from the vehicle, they are vulnerable to IED attacks.

Another technology that has proven highly effective against remotely initiated IEDs has been cellphone jammer technology, which can effectively cripple all cellphone triggered IEDs within the footprint of the jamming device.

Cellphone jammers emerged during the terrorist bombing campaign conducted by Palestinian radicals against civilian targets in Israel, especially in densely populated urban areas. Public access areas where large numbers of civilians gathered, such as cinemas, shopping centres, hotels and transportation stations were favourite targets. Other than hapless members of the public, VIPs became a preferred target.

By the middle of this decade a number of products, with varying sophistication and coverage, appeared.

Representative examples were the Empower RF Systems PCJ-X-1 rated at 15 Watts per band, in four bands between 851 and 1990 MHz, the EA-X-1A rated at up to 200 Watts per band, and the CCM International series of products. The latter is a suite of detection receivers and jammers intended to protect fixed targets, but also VIPs and vehicles and explosive ordnance disposal operations. Products

varied between the vehicle-mounted Bomb Ranger 330A/330B, the portable Manpack 6, and the remote control Terrorist Trap VIP-16 jammer.

Israeli manufacturer Netline marketed an entire family of cellular telephony jammers, ranging from the 19 inch rack mounted C-Guard Very High Power Cell Phone Jammer rated at 15, 30, 50, 100, 120W in the 851 to 2170 MHz bands down to the C-Guard Low Power jammer rated at 500 mW. These designs are built to defeat AMPS, N-AMPS, NMT, TACS, GSM, CDMA, TDMA, iDEN and UMTS cellphone modulations.

Thales markets the FLEAS (Flexible Light Electronic Attack System) intended to defeat 'hostile personal communication threats' encompassing 'low-power hand-held radios, PMRs and cellular telephones'. The product family included vehicle mounted and remotely operated or 'leave behind' devices.

The effectiveness of cellphone jammers led to a shift in insurgent tactics. The susceptibility of conventional cellphones encouraged the use of satellite phones, and increasingly, microwave and infrared controls. A cellphone by design operates with a standardized radio modulation at standardized frequencies, and uses an omnidirectional antenna system. Each cellphone is continuously exchanging messages with nearby cellphone base stations, making its presence easy to detect, and indeed track. From an electronic warfare perspective it is a simple target for emitter locating systems and jammers.

Satellite phones are slightly less susceptible than cellphones, as their antennas are optimized to be most sensitive in an upward direction, but they are also tied to standardised signaling formats.

Microwave remote controls present a more complex jamming target as they operate across multiple unlicensed radio frequency bands, in recent products the 900 MHz, 2.45 GHz and 5.8 GHz ISM (Industrial Scientific Medical) bands, also used for WiFi portable computer networking. By regulation such devices are limited to very low powers of one Watt or less of transmitted radio frequency power (EIRP) and employ spread spectrum modulations to facilitate sharing of bandwidth. Even in built up urban areas, using omnidirectional antennas, such devices easily achieve ranges of up to 100 metres, sometimes more if unobstructed line of sight is available. While wireless networking chipsets generate bidirectional transmissions, most remote control devices do not, with the controlled device comprising a receiver, which might be completely silent by design. The latter precludes detection of an IED triggered by such a device since the radiofrequency emission is present only when the insurgent presses the fire button on his remote control handset.

If an insurgent bombmaker wishes to extend the range of his control handset to a kilometre or more, he has the option of fitting a directional antenna, which has the additional advantage of making his transmission much harder to detect, if at all. Numerous 'do it yourself' recipes exist on the Internet for high gain 2.45 GHz band helix antennas used to extend wireless LAN operating range.

ISM band IED triggers present a more difficult challenge, with the added impediment that barrage jamming of the band would cripple much of the wireless COTS networking technology now ubiquitous in military use.

Infrared beam triggering devices have reportedly been used to set off roadside IEDs including shaped charge plate devices. When a vehicle or soldier interrupts the beam the device is set off. Infrared links of this kind are as common as the doorbell in a convenience store, using typically 0.8 or 1.3 micron band Light Emitting Diode or sometimes collimated laser devices. As they produce a very narrow pencil beam, the only opportunity to detect them arises if an object inside the beam, or dust/smoke blowing across the beam, produces a reflection. Jamming or remote triggering using an infrared light source is no less problematic, since the narrow beam receiver may not couple in much in the way of background reflections.

The problems in detecting prepared and dormant remotely triggered IEDs are technically difficult.

The first is that the explosive charge and metal components may be buried sufficiently deep to make most conventional mine detection technologies less than effective. Because the device may have been buried days, weeks or months before its intended use, surface soil disturbances often detectable using infrared imaging, or X/Ku-band Synthetic Aperture Radar imaging, may no longer produce useful contrast. The US Air Force trialled these techniques in Iraq, using digital Coherent Change Detection methods. They quickly discovered that large numbers of false alarms were produced by roadside trash and tumbleweed. The false alarms swamped real IED detections.

Ground penetrating radars, high power microwave or multiband, have achieved some success in detecting buried landmines. These technologies rely on the differences in the electrical properties of landmines compared to the surrounding soil. Two difficulties have emerged: one is the electrical properties of soils and rocks, as dry and porous soils are generally much easier to penetrate compared to wet and dense soils; another is the increasing popularity of plastic encased mines, with few electrical components.

While the application of this technology to IED detection has good potential, the principal problem is in the false alarm rate and effective range of the equipment, plus the soil composition and moisture content factors.

Another technology used with some success in Iraq and Afghanistan is TNT 'sniffer' technology, which effectively emulates the capabilities of a sniffer dog. Using MIT developed detection technology it optically senses vapours released by the explosive. Its principal limitations are no different from sniffer dogs, in range and dependency upon favourable wind conditions.

A more ambitious technology is currently in development by a team comprising Winner Laser Technologies and Soreq NRC. Their design, a variation on the theme of differential absorption laser radar (DIAL), uses a high power pulsed laser to dissociate the explosive vapours, which are then excited to fluorescence by another laser of a different colour. The developers claim their technology is capable of detecting nitrate based explosives with much fainter vapour signatures than TNT, at distances of up to 100 metres with existing laser technology. DIAL lidars have been used with considerable success in remote sensing, and CSIRO was a world leader over a decade ago in this area, so this technology has great potential.

Other technologies being developed are emitter locating systems designed to find the Unintended Emissions (UE) from wireless or infrared IED trigger systems. The University of Missouri recently patented a receiver design for this purpose. Most wireless receivers are built as super-heterodynes, and use a local oscillator within the receiver to convert the received microwave signal down to frequency that is more easy to handle. Detection of local oscillator leakage has a colourful history, with this technique used by MI5 during the Cold War to locate Russian spy transmitters in the UK. But its most common use has been by traffic police to detect motorists using supernet technology warning receivers intended to detect police speed detection radars. Other sources of UE include digital switching transients in electronics, but the latter signals are very much weaker than local oscillators, to a large extent due to Western regulatory standards like CISPR 22 that put hard limits, for good reasons, on radio frequency leakage from digital equipment. UE detection has great potential in electromagnetically quiet rural areas, but will face false alarm rate challenges in urban areas.

No discussion of technologies for the defeat of IEDs would be complete without techniques intended to remotely pre-detonate or cripple remote control IEDs. High Power Microwave (HPM) technology has been in development for over two decades as a weapon for crippling electronic systems. That capability also offers potential in IED defeat, as a HPM device on the lead vehicle in a convoy could either burn out or trigger any wireless or cable controlled IED it illuminates – a field strength of 10 kiloVolts/metre is typically enough to burn out a cellphone or similar consumer electronic devices. Difficulties arise due to enormous electrical collateral damage potential in urban areas, as well as personnel and onboard electronic equipment exposure – electrical 'self kills' are a genuine risk. More practical problems relate to buried IEDs being set off at safe distances ahead of convoys, but producing collateral loss of civilian life and property.

Laser Induced Plasma Channel (LIPC) technology being developed by Ionatron in the US provides similar capabilities and faces similar challenges. LIPC was devised initially as a non-lethal 'wireless taser' weapon, using an ultraviolet band laser to produce an electrically conductive path between the weapon and the target, via which an electric shock could be transmitted.

Over the past decade, IED technology and means of defeating IEDs have produced an evolutionary arms race. Perhaps most disappointing is that Western nations were very slow in understanding the IED threat, and slow in developing viable counters. While the IED problem is not trivial to solve, it is much less difficult than countering sophisticated high technology weapons operated by nation state opponents. If the last decade of technological conflict in the IED domain tells us anything, it is that intellectual slothfulness still costs lives in shooting wars.

Talon IED detector robot sensing the roadside for munitions.