Andy Oppenheimer, Editor of World Security Report, looks at the parallels between modern terrorism and the CBRNE threat, and the IRA’s activity during the Troubles...

Improvised explosive devices (IEDs) have been, and continue to be, the main threat facing troops in theatre, counter-insurgency forces, and civilian victims of terrorist acts. The IRA waged the biggest terrorist bombing campaign in history, with an unparalleled level of ingenuity in the crafting and deployment of a multiplicity of IEDs. Lessons are being learned by current EOD (Explosive Ordnance Disposal) squads from dealing with over 30 years of IRA terrorism. UK EOD squads are applying their expertise and experience to current theatres of war where IEDs are prevalent, particularly to US EOD squads. But today’s threats differ in many ways from the challenges faced by the British Army ATO (ammunition technical officer) teams, who were engaged in a 30-year cat-and-mouse arms race with the IRA, but faced with threats that, although constantly changing in operational detail, were more quantifiable than the ones they and their colleagues around the world face today.

The IRA: unparalleled ingenuity
Compare the following bald statistics: Between 1970 and 2005, the Provisional IRA detonated a staggering 19,000 IEDs on UK territory – that’s one every 17 hours. But the worst single terrorist attack on British soil, the London transit attacks of 7th July 2005, which killed 53 and injured over 700, were not committed by the IRA but by a homegrown collection of jihadi terrorists. And the atrocities of 9/11 took more lives in one day (2,973) than the IRA (1,928) in its entire campaign.

These gas canisters lying in an Iraqi road form a powerful IED
However, the British EOD squads became acclimatised to a veritable onslaught of IEDs aimed at taking out troops, police, political notables and other British officials at various periods until the final IRA ceasefire in 1997. Although attacks during the 1980s and 1990s were less frequent than the 1970s, bombs grew in complexity and power. The Bishopsgate bomb, which blew up a sizeable chunk of the City of London in April 1993, caused £1.5bn in damage and exceeded a kiloton of TNT-equivalent explosive power, as did the Canary Wharf explosion three years later. Had these vast VBIEDs (vehicle-borne IEDs – car bombs) been planted by a present day jihadi group, they would have been set to go off at a time when the maximum number of people would have been killed or injured.

Following a period of experimentation at the outset of the 1970s ‘Troubles’, the Provisional IRA went on to achieve an unprecedented level of technical IED expertise. Having used the first timers in bombs decades back, these skills evolved to fitting timing mechanisms; new methods of detonation (command wire, radio control, radar and light initiation); and anti-handling mechanisms. The bomb that blew up the Grand Hotel in Brighton, aimed at assassinating the entire British Cabinet, was the first to incorporate a video recorder’s long-delay timer. Radio-controlled devices were purloined from commercially available model aircraft. The IRA also used car parking timers and bought up Northern Ireland’s entire stock. Under-vehicle IEDs, such as the one that killed MP Ian Gow and others, were fitted with a novel and deadly booby-trap device, the mercury-tilt switch.

**Then and now**

One striking difference between then and now, however, is that IRA bombs were aimed at destroying economic infrastructure and killing or injuring those viewed to be instrumental in continuing British rule in Northern Ireland, but were not deliberately aimed at ordinary civilians, which was counterproductive to the cause. Almost daily attacks in conflict zones and civilian settings are, in contrast, as much aimed at civilians as occupying forces or indigenous security and police forces.

VBIEDs remain the ‘nuclear weapon of guerrilla warfare’. But the suicide mission for both VBIEDs and hand-deployed IEDs has been the main dramatic change in terrorist bombings. Unlike the IRA, current terrorists do not leave coded warnings (even misdirected ones), which at times enabled IEDs to be disrupted by the bomb squads, their components separated and analysed, and the bomb-maker who put them together identified. The IRA, for a short time, used the deadly tactic of using proxy bombers – a kidnapped or coerced individual who would be forced to drive a bomb to its target. Occasionally, and very tragically, these bombers were themselves blown up with the bomb activated by remote detonation. But the Provisionals did not go in for sacrificing themselves – or everyone else in the vicinity of an explosion – for the cause.

The planning of suicide missions is also taking advantage of IRA timing methods, as improved detonators and timers are being increasingly used to enable the bomber to start the countdown before they reach the target. A car-bomb driver may fire a single detonator to initiate boosters, which have replaced the original mine fuses. Or a distant operator can set off the VBIED with command wire or radio signal. A modern technique, mobile phone detonation – most horrendously exemplified by the 2004 Madrid bombings – was also pioneered by the IRA but abandoned because it was unreliable.

The IRA especially mastered the deadly art of troop convoy ambush with hidden or disguised devices. Present day ambush methods have come straight out of the IRA manual, with current roadside IEDs disguised as rocks and all manner of other commonplace objects. Command wire or radio signal (from garage door openers) are increasingly used for remote detonation. A commonly used tactic today, pioneered by the IRA, is to place one bomb as a ‘come-on’ to divert vulnerable EOD operators as prize targets for a second bomb, or a sniper – and also disrupt emergency services.

A chief difference is the acquisition of information. Whereas IRA bomb-makers learned their skills over many years, today’s terrorists acquire theirs from overseas training camps and the jihadi internet network. ‘Kitchen lab’ apparatus set-up and basic mixes can be surfed alongside more advanced IED making and cyberterror techniques. Terrorists, such as the December 2008 Mumbai attackers, now benefit from commercial technologies – from Blackberries to GPS navigators to anonymous email accounts.
**Explosives – do it yourself**

The IRA used more types of explosive than any other group and obtained supplies from many sources over decades. In one year alone, 1993, they detonated 14,540kg of explosive. They did not have to resort to making makeshift homemade explosives (HME) such as TATP (triacetone triperoxide) and HMTD (hexamethylene triperoxide diamine), which is believed to have been used in recent outrages such as the London 2005 transit attacks. Instead, they had the advantage of acquiring stable and even more powerful explosives, most notably Semtex from Libya. The IRA’s prime HME was vast quantities of ammonium nitrate for car bombs, milled in a laborious drying process to the correct consistency in the dampest part of Europe.

Homegrown terrorists are making HME chiefly from unrestricted materials. TATP, one of the most dangerous and sensitive explosives known, may be liquid or solid. Consisting of acetone (nail polish remover), hydrogen less than peroxide (hair bleach of 15-25 volume content) and a common acid, less than 1kg is needed to breach the body of an aircraft. The other main peroxide-based explosive, HMTD, is equally unstable and can be set off by heat, movement and even contact with metal. But only one bottle-sized bomb could rip a hole in a plane’s hull. Like TATP; HMTD TATP is normally created as crystals, HMTD, as a powder. It can be prepared in five hours – that is, within the span of a long-haul flight. Mixing concentrated hydrogen peroxide (CHP) with a fuel can also create a liquid explosive. Fuels such as acetone and ethanol may be used, and even things like black pepper and sugary drink powders. Gas canisters may be used to enhance the incendiary effect, as in the London and Glasgow airport car-bomb attempts; these attacks failed only because only 1mm between the mobile phones and the detonators broke the circuit.

**Dealing with the threats**

This was just one example of the many attempted attacks being planned in the UK and the US. Intelligence continues to be of prime importance in pre-empting further attacks. This includes infiltration of groups, which proved invaluable in the war against the IRA. Surveillance and CCTV help to pre-empt attacks and gather evidence. But bringing suspects to trial is costly and may be inconclusive, as in the September 2008 verdict on the ‘liquid explosives plot’ trial – in which the accused, now being retried, were acquitted of intending to actually blow up the aircraft with peroxide-based explosives hidden in soft drinks.

As the IRA pioneered IED technologies, so the British army and security forces brought in pioneering countermeasures to deal with the many hundreds of devices before they could destroy property and lives. Remote handling – including robots with cameras – was invented at the height of the IRA campaign and advanced forms are now used to preserve the lives of EOD operatives, who used to have to disrupt and dismantle bombs by hand. Water-jet disruptors were invented to deal with IRA car bombs remotely by breaking the detonation circuit. Methods are in constant evolution to react to unpredictable targeting, novel materials, and means of delivery. Today, smaller, lighter types of bomb detection robots are being introduced, as established robots are too heavy for regular soldiers on patrol and convoy missions, or for police and military civilian support responding to terrorist IED incidents.

Whatever the methods used, the immense bravery needed for all EOD missions remains undisputed – and with today’s devices likely to incorporate a CBR (chemical, biological, radiological) component, the challenges can only intensify. This will require getting to the root of the mentality, aims and doctrines of terrorists and ‘lone wolf’ threats. This was achieved with the IRA, but we have a long way to go with the current threat. Terrorists are adapting in a way modern conventional organisations lack. So countermeasures have to be based on even more ingenious levels of adaptability and improvisation.