World Security Report

Issue 1 March 2009

Subscribe

Welcome

to the first issue of World Security Report.

This newsletter aims to provide military, law enforcement and security practitioners worldwide with informed and impartial analysis on the strategic, tactical and technical challenges facing them in their day-to day-struggle to keep their citizens safe.

As the Bush regime is consigned to history and the Obama era begins, the democratic nations are faced with huge challenges in the areas of economics, climate and security. While these are often interlinked at the strategic level, the first two are largely outside the remit of this publication. International security threats, however, are our core subject areas, whether they are posed by nation states or from terrorist organisations.

Radical Islamists present the chief current terrorist threat and while al-Qaeda takes centre stage in the public perception, it is in fact the loose nature of Islamic terrorist organisations – or lack of organisation and chain of command - we face that makes Islamic extremists such a difficult enemy to defeat. Intelligence or security organisations worldwide must also not forget the 'lone wolf' threat – or groups and individuals with ill intent which may not fit the current threat profiles. The Tokyo sarin attacks in 1995, waged by a non-Islamic apocalyptic cult, were testimony to this.

Whilst al-Qaeda continues to be a potent threat itself, it is as an example and inspiration to others that it is perhaps the most dangerous. Ideas after all are much harder to defeat than flesh and blood and although there is a growing number of radicalised young Islamic men and women living among us and around us it is incredibly difficult to see where the next threat is coming from.

The confrontation between terrorists and would-be terrorists and the West will not be entirely solved by soldiers or policemen - that is a challenge for politicians. However, World Security Report does aim to provide those on the front line at least some of the information and in-depth analysis they need to do the job.

In this Issue

Contact us

For more information please contact:

Tony Kingham, KNM Media
+44 (0) 7827 297465
tony.kingham@
worldsecurity-index.com
www.andyoppenheimer.com

In the Next Issue

CBRN readiness: does the US lead the way?
Counter-IED – learning from Britain
Insider terrorism and the Ivins controversy
Somalia – terrorist breeding ground
Terrorism and state sponsorship
Iran - point of no return?
Pakistan – after Islamabad, Mumbai and Lahore, where next?

Editorial *Andy Oppenheimer*

Andy Oppenheimer

Asymmetric Conflicts: the Fourth Generation

The publication of our first issue follows two events which epitomise, first, the current world terrorist threat and second, problems of asymmetric warfare: respectively, the attacks in the Indian port of Mumbai in December, and the Israeli military offensive in the Gaza strip at the end of last year – the latest episode in that country's own War on Terror.

The first incident illustrated the continued pursuance of simplistic methods by terror groups – guns and conventional explosive devices – to cause maximum mayhem and attain instant publicity. It also showed that, although such basic weapons were used, the attack was the result of sophisticated planning and training.

The second event showed the unevenness of a technologically superior, well-funded nation-state's fighting force pitted against a ruthless and determined militant movement – that even a relentless bombing campaign is still unable to destroy a terrorist infrastructure and its support system. Hamas were still able to demonstrate they could, albeit at a reduced level and for a time, fire rockets into Israeli territory.

The Israeli Air Force targeted prime Hamas targets *© Israeli Defence Force*

From sources in the defence establishment, it emerged that, even as Israel was beginning to negotiate a ceasefire agreement with Hamas, Israel's Defence Minister Ehud Barak had instructed the IDF to prepare for the operation six months in advance while intelligence was gathered to map out the security infrastructure of Hamas and other militant organisations operating in the Strip. This programme would have revealed permanent bases, weapon silos, training camps, the homes of senior officials and co-ordinates for other facilities. Many other sites were, however, hit during the three weeks of the campaign, showing that urbanwarfare – from the air and on land and at sea – is bound to be indiscriminate.

Israel's relentless offensive to crush the Hamas movement in Gaza is said to be a preamble to the country's wider campaign to confront what is seen as a mounting threat posed by arch-enemy Iran – to deal with the combined danger of Tehran's continuing support for Hamas and Hizbollah (completely re-armed by Iran since the 2006 Lebanon war) and Iran's reputed attempts to become a nuclear weapons state. Hamas militants engaged in deadly combat with Israel have been trained and equipped by Iran. Previously they had to rely on their own primitive, short-range Qassam rockets, but the Grad rockets recently provided by Iran gave Hamas the capability to hit targets deep within Israel – including its nuclear weapons plant at Dimona.

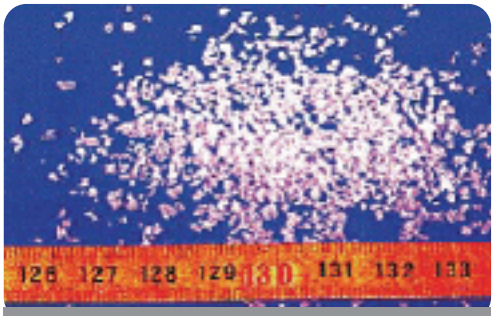
The weapons used by Israel are equally controversial and re-opened the issue of the use of borderline conventional weapons and weapons of mass effect, most notably the notorious white phosphorus (WP) smoke-screen incendiary, which continues to burn human tissue on contact and is extremely difficult to extinguish. While WP is banned in civilian areas, previous instances are claimed, such as during the effort by US forces to counter insurgents in Fallujah, Iraq in 2004. Battleground reports at the time suggested that troops firing WP shells were unaware of the nature of each target – highlighting the problem of avoiding injury to civilians in counter-insurgency operations. When the Israeli policy of bombing civilians was repeatedly questioned, observers failed to note that terrorist groups have a long record of using civilian buildings and districts to shelter personnel and weapons. In an area as small and overpopulated as Gaza, it was inevitable that innocents so closely situated to those deemed less innocent would suffer in the bombing and, consequently, the standing - already poor - of Israel in the world.

IAF aerial photo of alleged Hamas training centre *© Israeli Defence Force*

That the campaign has provided yet another recruiting sergeant for jihadi-inspired terrorism at home and abroad is a leading concern for all agencies involved in protecting our security.

And returning to the UK, the end of last year also saw unsatisfactory conclusions to several terrorist trials, showing how proving guilt is becoming increasingly difficult in these cases. The most controversial was the September verdict delivered on eight British citizens at the London 'liquid explosives plot trial: that the jury decided that the ingenious devices they had constructed were not intended for deployment on transatlantic aircraft – despite being shown extensive evidence that the men had gathered hydrogen peroxide and other bomb-making materials, had made 'suicide videos', and had downloaded airline schedules.

Intelligence efforts, however, are gaining ground and are increasingly focused on rooting out further homegrown terrorist plots, mostly involving homemade explosive mixes acquired from jihadi and other Internet sources and, sometimes, overseas training. So far, attempts – such as the failed deployment of car bombs in London and Glasgow Airport in June 2007 – have either fallen short of the ruthlessly high standard achieved by the IRA, Hamas and Al Qaeda abroad, or are being pre-empted. But the terrorist learning curve may not last long, so vigilance – especially within communities – must be eternal.



Crystalline tri-acetone tri-peroxide (TATP)

Is the nuclear threat 'so last century'?

This international threat analysis round-up focuses on nuclear proliferation hotspots. The second article in this issue assesses with the threats from civilian non-state actors.
In subsequent issues of World Security Report we will examine in depth aspects of CBRN readiness to counter such threats in the field and in the civilian sphere.

Pakistan – a failing state

It has long been predicted that Pakistan's country's political and domestic instability would put its nuclear weapons at risk, and this has intensified considerably in recent months. Its precarious alliance with the US in waging the 'global war on terror', the long-standing dispute over Kashmir, together with the chaos following the Benazir Bhutto assassination and recent escalating internal terrorist threats makes the country a veritable powder keg in terms of continuing volatility.

The Mumbai attacks of December 2008 which killed more than 190 people and injured at least 300 have heightened tensions between India and Pakistan, bringing to the fore once again one of the world's potential nuclear flashpoints. Although the attacks were carried out through simplistic weapons, they involved sophisticated planning and training and the use of modern technologies - from Blackberries to GPS navigators to anonymous e-mail accounts – and, with increasing evidence from Indian and US authorities, Pakistani involvement. A new period of instability was ushered in by the assassination, one year earlier, of Pakistan's opposition leader Benazir Bhutto. The massive bomb attack on the Marriott Hotel in Islamabad, on 20 September 2008, which killed 52 and injured many more, came only days following the inauguration of Bhutto's widower, Asif Ali Zardari as the country's new president.

The alliance with the US has done much to enhance the country's internal vulnerability. Islamabad has been receiving military assistance from the US to the tune of a billion dollars a year. Washington's heightening aggression against militant targets beyond Afghanistan's frontier has led to attacks on civilians, provoking angry reactions from Pakistani leaders, generals, and the general public. Divisions are growing over how to contain a growing Islamic militant insurgency as well as deal with a crumbling economy.

'Loose nukes' - reality or scare story?

Pakistan's past record of disseminating nuclear information and technology, together with enhanced power of the Taleban and the continued training and recruitment of Al-Qaeda in Pakistan, makes the country arguably the world's number one nuclear proliferation concern. The transcontinental 'nuclear Walmart' run by its 'father of the bomb' A Q Khan, by which Pakistan covertly developed its first nuclear weapons also enabled programmes in Iran, North Korea and Libya to advance. Pakistan's nuclear secrets could not have been exported by Khan without the knowledge of members of the military and the Inter-Services Intelligence agency (ISI), especially as Pakistani military aircraft were used to ship materials.

In January leading nuclear expert Professor Graham Allison of the federally appointed bipartisan Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism said: "When you map W.M.D. and terrorism, all roads intersect in Pakistan. The nuclear security of the arsenal is now a lot better than it was. But the unknown variable here is the future of Pakistan itself, because it's not hard to envision a situation in which the state's authority falls apart and you're not sure who's in control of the weapons, the nuclear labs, the materials."

The 'loose nukes' issue has long prevailed - that an Islamic extremist group could take over power, and hence, control of Pakistan's nuclear arsenal. Nuclear insecurity in Pakistan is not only focused on proliferation of expertise and materials, but also on problems of sustainable control of materials stewardship. Trading in fissile materials and bomb components by nuclear facility workers seeking to earn money is also a high risk in increasingly dire economic times. Infiltration of the military by Taliban elements and consequent interference with its stewardship of the nuclear arsenal will enhance the danger of unauthorised use of nuclear weapons.

There are 20 facilities in the nuclear complex, including uranium mines; gas-centrifuge plants (set up by A Q Khan) to produce highly enriched uranium (HEU); light and heavy water research reactors; and plutonium reprocessing facilities. Nuclear information has also been disseminated: you can't build bombs [other than the crudest devices, which would be more in the 'dirty bomb' class] without the precise specs. Designs for a sophisticated nuclear weapon small enough to fit on existing North Korean or Iranian missiles were found on the computers of three Swiss nationals who were part of the Khan network. One kept designs in his office desk drawer. Many foreign scientists and companies involved in the network have escaped prosecution.

Pakistan has never signed the 1968 Nuclear Non-Proliferation Treaty (NPT), which is not taken seriously by nuclear proliferators, as evidenced by a statement by Dr Khan in a rare interview conducted while under house arrest: "There are no international laws that force anybody to comply." Indeed, the country's proudly held achievement of nuclear weapons status attained mainly through Khan's illicit procurement of materials diverted from civilian-based nuclear energy research has provided a model for future nuclear 'wannabes'.

Islamabad and in the past has not ruled out a nuclear strike against India if its territorial integrity were to be threatened and its nuclear arsenal serves primarily as a deterrent against a conventional Indian attack. India and Pakistan have gone to war three times since the 1947 partition. But in the decades following their last conflict in 1971, over the birth of Bangladesh, both nations have acquired nuclear weapons.

Pakistan objects to the impending nuclear technology transfer deal being finalised between the US and India, which will enable the US to supply India with nuclear technology provided that 14 out of Pakistan's 22 reactors are opened up for inspection by the International Atomic Energy Agency (IAEA) – but not its military nuclear production facilities. This, Pakistan fears, will enable India to expand its weapons production capability to as many as 50 weapons per year, compared to the current ten, from the fissile material produced by the eight unsafeguarded reactors – as it will be able to re-direct domestic fissile material to the weapons programme while using foreign supplies for its burgeoning energy needs. This may negate Pakistan's efforts to catch up.

Are the weapons safe?

Since 2000, the nation's key nuclear institutions have been under the unified control of the National Command Authority, a joint military-civilian structure that includes military, political and scientific officials, with Pakistan's President having the final say. Nuclear production, research, and deployment efforts and facilities are, however, maintained by a joint military command - the Strategic Plans Division. Following the Bhutto assassination former President Musharraf agreed to security upgrades of the arsenal, as well as moving some nuclear weapons to more secure locations. US help has come in the

Is the nuclear threat 'so last century'? continued...

form of a system of controls, barriers, locks and sensors, but the programme is not complete.

In theory, the weapons are well dispersed and under tight security with the warheads stored separately from the delivery systems. But Pakistan's decision to physically separate the bomb components and isolate the fissile cores and triggers from the weapons and store them at several military bases does not guarantee their security – as some components have been relocated to insurgency-prone areas. Distributing assembled systems may make the weapons more vulnerable to seizure by terrorists or renegade national forces.

Much depends – as ever – on whether disparate terrorist groups are interested in acquiring complex materials and components for devices that they have no experience in making or deploying. While Al Qaeda may have declared its intention to wreak mass destruction, the means to carry this out are not readily available despite all the vulnerabilities outlined above. What remains a leading threat is the stand-off between two nuclear-armed nations which hover on the brink of outright conflict; terrorist outrages such as those perpetrated in Islamabad and Mumbai will test all those in government who hold the responsibility not only for unleashing military action and retaliation on its nuclear neighbour, but stewardship of all the facilities which provide the means for such action. Preventing the collapse of a nuclear Pakistan will be just another foreign policy headache for President Obama, whose intelligence briefings confirm these security concerns.

Iran: the nuclear wildcard

Pakistan has deliverable nuclear weapons; Iran has not. The former has an ongoing enmity with its immediate, nuclear neighbour, India; Iran's sworn enemy, Israel, reputedly has as many deliverable nuclear weapons as the UK. In February the IAEA estimated that Iran had enriched a metric tonne of low enriched uranium (LEU), and had therefore reached "breakout capacity" - the ability, in theory, to produce the 20-25 kg of highly enriched uranium (HEU) needed for one functioning warhead. As the LEU has less than a 4% concentration of the fissile isotope uranium-235, to make weapons-grade HEU – that is, with a uranium-235 concentration of 80-90% - the Iranians must further enrich the LEU in massed centrifuge cascades. Some 1,500 additional centrifuges had been installed by January and were "under vacuum", a preparatory step before enrichment can start. But they will need many more.

Centrifuges smuggled via the A Q Khan network. Iran was one of the main beneficiaries

One bomb does not a nuclear weapons state make – they would need to have enriched at least three times that amount of HEU and have the means to threaten delivery of their warheads. But it's the obfuscation and non-disclosure that is of utmost concern, as Iran is also refusing to tell the IAEA where it is manufacturing the centrifuges used to enrich the uranium, so the agency cannot confirm how many are being produced and where they are being installed. As the Natanz pilot centrifuge plant is under scrutiny, it will be somewhere else deep underground.

Also reported in February was a highly publicised successful dummy run of the long-delayed, Russian-built Bushehr reactor, which will become operational in 2009. Iranian authorities are also planning to build two new 1,000-MW nuclear power plants instead of completing the second power unit of Bushehr. But of even greater potential concern is Iran's prevention of IAEA personnel from carrying out ground inspections of the IR-40 40MW nuclear reactor at Arak. The plant is claimed to be for producing medical radioisotopes, but which has no other feasible use than producing plutonium. Once operational, the nuclear chain reaction at Arak will be moderated by deuterium oxide (heavy water), that is, ordinary water enriched in the hydrogen isotope deuterium. In order to make bombs a plutonium-reprocessing facility would have to be built. If it is, once up and running the Arak plant will be capable of producing 9 kg of weapons-grade plutonium per year – enough for two bombs. The acquisition of weapons designs, allegedly from the A Q Khan proliferation network, is likely to aid Iran in building the more complex implosion weapons out of plutonium.

Ongoing non-disclosure

Prevention of access to the plant follows Iran's long-established pattern of on-off co-operation and disclosure and means that the IAEA are not being permitted to see what was being done at the facility. While all nuclear material at its uranium enrichment plant at Natanz as well as all installed cascades remains under IAEA containment and surveillance, Iran has not fulfilled requirements on the early provision of design information, nor has it implemented the IAEA Additional Protocol, which is essential for the agency to provide credible assurance about the absence of diversion for nuclear weapons construction.

A September 2008 IAEA report said that Iran continues to defy UN Security Council resolutions and enrich uranium while refusing to answer IAEA questions regarding possible nuclear weaponisation activities. According to the report, Iran needs to provide the IAEA with substantive information to support its statements and provide access to relevant documentation. And contrary to the decisions of the Security Council, Iran has not suspended enrichment, having continued the installation of new cascades and the operation of new-generation centrifuges for test purposes.

All options are 'on the table'

Speculation abounds as to whether Israel will repeat – on a larger scale – its air attack on the Al Kibar reactor in Syria in September 2007 - or at least take out the Arak reactor. Having set a precedent by bombing the Iraqi Osirak reactor in 1981, this cannot be ruled out, especially since the recent Israeli elections and the country's recent form in launching offensives against its enemies. If the internal debate in Israel ultimately comes down on the side of an Osirak-Al Kibar-style attack, it risks retaliation followed, most likely, by further Israeli attacks on Iran – with strike and counterstrike eventually backed up by US attacks. The Israelis will also have to factor in a possible repeat of Saddam Hussein's response: consequent dispersal and hardening of new facilities and protection of them with air defences.

But with a new US president having made initial overtures to Iran for negotiations, an Israeli attack is growing less likely, given the country's continuing and growing dependence on US funding and support. President Obama has not been short on advice as to how to deal with Iran - among which will be to give the Iranians full clarification on likely response if nondisclosure and enrichment persist. His appointment of veteran diplomat Dennis Ross to oversee efforts to address the Iran issue points in the direction, for the first time, of negotiations rather than threats.

But neither the United States nor the UN Security Council has told Teheran how they would react if Iran admitted to past nuclear weaponisation violations. If the UNSC clarifies that Iranian admission of past activities would not necessarily lead to further sanctions or punitive sanctions, Iran will feel it is has been, once again, let off the hook. The nuclear effort is indeed advancing, albeit in fits and starts - hampered by both technical problems and diplomatic efforts to rein them in – and so long as the current President remains in power it appears to be making every effort to get there in the end.

CBRN terrorism: crying wolf?

In early December 2008 a report by the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism concluded: "It is more likely than not that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013." In recent years warnings like this by government and other authorities that terrorists are likely to use chemical, biological, radiological or nuclear (CBRN) weapons in the near future have become so frequent that outside observers are becoming sceptical. Attacks continue to feature conventional explosives that they have favoured by terrorists and insurgents for several decades. The three-day shootings in Mumbai in November 2008 involved even more basic weapons, albeit in a sophisticated attack in terms of preparation and training. Insurgency attacks in Iraq have, with the exception of a string of incidents involving chlorine tanker hijacks, been primarily IEDs of varying levels of lethality. The main danger to troops in Afghanistan is the roadside bomb.

Drowning in acronyms

if you take a 'WMD' in its original meaning as a weapon that will cause at least thousands, if not hundreds of thousands of deaths, only a nuclear bomb – and possibly a biological pandemic such as smallpox or avian influenza – can achieve this. But 'CBRN' actually means 'nonconventional' means of warfare rather than weapons of mass destruction and possibly even weapons of mass effect (which include some conventional bombs, such as fuel-air explosives and thermobarics). Tacking on the E for explosives, making CBRNE (pronounced see-burrr-nee by our American colleagues) can now be taken to mean the entire gamut of nonconventional weapons, including borderline conventional examples which have been improvised (improvised chemical devices, improvised biological devices, radiological dispersal devices) – plus the traditional conventional explosive devices, the E. It may be that a new term will evolve without the 'N' – as CBRE or CERB, or whatever. This may more accurately reflect the nature of the weapons rather than their effects or magnitude, and as used by terrorists and insurgents, rather than the military-grade NBC [the original term – nuclear biological chemical] weapons programmes of nation-states.

Intent and capability

There is no doubt that the 'franchise' that is now Al-Qaeda and its many sympathisers and affiliates worldwide intend, by and large, to kill as many people they view as the enemy as possible in whatever way they can find. Video propaganda continues to pour out of Al-Qaeda and disparate jihadi sources, such as in May 2008: "Nuclear Jihad: The Ultimate Terror", which calls for the use of nuclear, biological or chemical weapons against the United States. Whether they succeed is open to conjecture, and intelligence information is the only reliable means we have to truly assess the progress of both groups and individuals, many of whom are non-affiliated.

Buried chemical weapons in Iraq. The WMD threat has extended from countries to non-state actors adapting IEDs to include a CBR component. *© OPCW*

Although no one except the terrorists and their supporters would wish such terrible events to take place, in preparing for a CBRN attack a main problem is lack of precedent. Lessons have been learned from the few examples of nonconventional attacks on record, most notably the Aum Shinrikyo attacks on the Tokyo subway system in March 1995, which killed 12 and injured many hundreds, including emergency responders who were insufficiently protected to deal with several simultaneous chemical attacks. More recently, the response to the poisoning of the former KGB agent Alexander Litvinenko with polonium-210 served as an example of response to a radiological dispersal event (RDE). The anthrax mailings in the US in October 2001, which killed five but caused many thousands to seek preventive treatment with strong antibiotics, have taken seven years to be concluded, albeit unsatisfactorily with the suicide of the more recent prime suspect, government scientist Dr Bruce Ivins. Although 'only' five people died, the attacks produced panic and fear among large sections of the population who sought prophylactic treatment, and necessitated extensive and expensive remediation of affected premises.

Earlier in 2008 reports indicated that support for jihadism and that most vital support for terrorism – community back-up, which provides safe houses and a supply chain - may indeed be waning in some countries and communities, necessitating would-be attackers to 'self-start' and acquire their own expertise and weapons. Even with the heightening of intelligence efforts it is difficult to calculate the level and, more important, the direction of intent – particularly within certain elements and individuals who may not be affiliated to any named organisation.

In all cases, the most difficult aspect of assessing terrorism is capability. Terrorists in general lack traditional military supply chains - so they are forced to improvise their weapons and to resort to the Internet and sundry publications. There is also the issue of command and control. The current crop of UK-based attacks and attempted attacks seem to have no discernible command structure (unlike the IRA and other 20th-century nationalist groups with clearly defined organisational doctrines). More easy to assess are the state-sponsored groups like Hezbollah, which have a sizeable arsenal of regularly exercised rockets from a proven source, Iran, and who could likely obtain assistance from that sponsoring nation should they choose to deploy chemical warheads on them. But groups with ill intent are not short of intelligence; MI5 in late 2008 highlighted the dangers of infiltration following the trial of suspects who attempted a car bomb attack on Glasgow Airport the previous year, two of which were NHS employees.

Nuclear terrorism – an exaggerated threat?

Many written and spoken statements emanate from the US about the threat of a terrorist nuke. This is classed as a 'low probability, high effect' threat – very unlikely to happen but if it did, the consequences would eclipse anything else that has occurred in warfare since World War II. But even nation states with substantial resources and outside help have taken years to go nuclear. Iran, which has had a nuclear programme for almost two decades, is still possibly 1-2 years away from developing a small number of nuclear bombs. Most of today's non-state actors – with the possible exception of the Provisional IRA, whose bomb-making expertise and ingenuity was and still is unsurpassed – have or had neither the expertise nor the wherewithal to construct a fully functioning fission device. They are more likely to steal one, but even this would be extremely difficult without extensive insider help along with the key to the device's activation codes. Also, its use would almost certainly expose the state sponsor to retaliation.

The more realistic nuclear terrorist threat is of terrorists acquiring fissile material, nuclear components and expertise from nations of concern with a history of proliferation, such as Pakistan – exemplified by the A Q Khan nuclear network of front companies (see previous article), which transferred nuclear materials across continents to Iran, Libya, and North Korea (which has its own abysmal record of nuclear and missile proliferation). Southeast Asia

CBRN terrorism: crying wolf? continued...

has become an increasing focus for proliferation: centrifuge production facilities in Malaysia supplied nuclear equipment via the Khan network to Libya's covert weapons programme.

Piracy and smuggling of nuclear materials appear from IAEA database statistics to be on the rise, but it is not clear where the materials end up. Much contraband follows the same routes as for narcotics and conventional arms, particularly in South and Southeast Asia; smuggling (often of very small amounts of radioactive material, some of it weapons grade) often involves criminal gangs in the former Soviet Union (FSU) and beyond. Those countries and Russia, having presented a 'loose nuke' threat in the chaotic post-Cold War years of the 1990s, still present security and insider risks at poorly guarded facilities despite millions of US dollars having been poured into schemes to secure them.

Dirty bombs – hot debate

The likelihood of terrorists deploying a radiological dispersal device (RDD) – an IED with a radioisotope incorporated – is still regarded as the more likely nuclear threat. The RDD question continues to attract a wide range of opinion, both in terms of risk and effects. At the top end of the scale a bomb containing partly enriched uranium or reactor-grade plutonium, while not usable for a fission weapon, would make a very dirty bomb indeed – necessitating a potentially massive clean-up, economic disruption and short- and long-term injury and illness. At the other end, a small radioisotope component – such as, from a domestic smoke alarm – may not kill outright or produce radiation injury other than if handled by the bomb-maker. But it would necessitate extensive cleanup of the affected area where the explosion took place.

Nuclear power plants and dismantled former Soviet nuclear submarines are of considerable concern. Chechen separatists have unsuccessfully attempted a NPP attack, in October 2005, which would have involved hijacking an aircraft and flying it into a nuclear power station at Nalchik in Russia. If targeted at cooling ponds full of high-level radioactive waste, such an attack would produce a weapon of mass effect, with radioactivity spread across national borders. But it would involve vast resources of planning, training and co-ordination, and would depend very greatly on insider help.

Many experts believe, however, that the radiological threat is exaggerated and that the effects would be mainly psychological (due to the public's fear of radiation). However, without precedent it is impossible to assess possible impact. The only example of a publicised radiation incident in London – the Litvinenko poisoning – was a non-explosive event, not a RDD - and was not intended to spread contamination. But it did, and required an extensive interagency response, tracing of hundreds of potential contacts of the victim and his associates, careful management of the media, and remediation of properties in the heart of the capital.

Bioterrorism – the invisible threat

Bioterrorism is difficult to attribute as it is hard to trace the source and origin of disease - to identify which agent caused which symptoms, and track its progress within a population and potentially across borders and continents. The main modern civilian-based precedent is the anthrax mailing incidents that followed the 9/11 attacks in October 2001, and a deliberate spread of Salmonella food poisoning by a religious cult in Oregon in 1984.

While much is said and written about needing only cheap, easily concealable, small-scale facilities to make BW, the main obstacles to successful bioterrorism remain weaponisation and delivery, as multiple factors affect dissemination to human hosts. Refining lethal bio-agents, preventing self-infection, and assuring delivery to the intended targets are beyond the capabilities of most terrorist groups. Individuals with microbiological expertise and laboratory access, who may lend their services to groups for ideological or financial motives, however pose a significant risk. The possible use of genetically modified organisms (GMOs), which could create untreatable diseases, or 'stealth' viruses, is heralded as a major future risk but the present danger is concentrated more on 'white powder' attacks and hoaxes sent through the mail to selected targets or simply to cause chaos at postal facilities and other public buildings.

The main biological threat, however, still comes from naturally occurring outbreaks – avian influenza being potentially the most devastating threat, when viewed as causing the highest death and sickness toll of any pandemic in the past century. The most effective way to spread disease deliberately, therefore, would imitate Nature: self-infection of a disease with high infectivity and mortality, which spreads through inhalation. Air travel is the obvious means to infect people across continents. But this must be measured against the customary desire of the terrorist to attain instant attention for his actions; biological terrorism is a 'slow burner' which lacks instant impact. When people fall ill, they rarely want to ascertain who or what caused their illness – they simply want to be cured. Medical workers, and later governments, may be alerted to a breakout of unusual symptoms or disease clusters – but the time taken to confirm their cause may stretch to weeks, if not months. And there may be a brake on the idea of spreading disease to friend as well as foe.

Chemical – getting closer

Chemical attacks are the most likely to occur in the nonconventional range of weapons, particularly using toxic industrial chemicals (TICs). Sporadic attacks involving chlorine took place in Iraq in February and March 2007 – mainly hijacked trucks carrying canisters blown up with easily purloined explosives. Recipes for chemical bombs are found on the Internet and chemicals are the cheapest and arguably the easiest of non-conventional weapons to acquire and assemble. Chemical plants and transportation are generally not well guarded. While security measures are in place to scan passengers going 'airside', airports are vulnerable - particularly in the terminals - where toxic substances and explosives could be brought in without detection and dispersed easily and rapidly to create a mass casualty event at the airport itself. We will be dealing with the chemical threat in greater detail in our next issue.

Many call-outs for first responders turn out to be false alarms or hoaxes, but must be regarded as potential CBR attacks.

The intent to mount a weapon of mass destruction or mass effect exists. But in the hope not to be tempting Providence, it may be said that the probability of terrorists launching a true WMD attack, particularly in the short term, or a CBRN attack, is substantially lower than their relentless use of conventional weapons and explosives and employing the means of ambush and attack witnessed almost daily in Afghanistan, and in terms of basic guns-and-grenades insurgency and hostage-taking, in Mumbai. It may be that terrorists prefer not to choose the extremely complex and expensive route to CBRN when E and its related forms of causing mayhem have proved so successful in the past, particularly in producing instant attention. Let's hope the sceptics about CBRN terrorism are right, and the doomsayers are wrong.

IEDs: the new generation

IEDs – improvised explosive devices – have been, and continue to be, the main threat facing troops in theatre, counterinsurgency forces, and civilian victims of terrorist acts.

Around 70% of all combat casualties in Iraq are from IEDs and large areas of Afghanistan are becoming off-limits to all but the best-protected troops.

The IED is the tried and tested tactical weapon that terrorists have used for decades. The most devastating terrorist weapon, the car bomb, has been reliably deployed by terrorists thousands of times since the first vehicle bomb in a horse-drawn carriage blew up on Wall Street in 1920 detonated by an Italian-American anarchist, Mario Buda. How UK explosives ordnance disposal (EOD) teams can lend their long experience of dealing with bombs, gleaned over several decades during the relentless campaign waged by the IRA and other Irish terror groups is leading the way in today's conflicts where insurgency and civilian terrorism are constant threats.

Car bombs continue to be the prime terrorist weapon.

The recent tally of 4 terrorist bombs detonated (on 7 July 2005 in London) and other attempts at car bomb attacks weighed against the 19,000 bomb attacks waged by the IRA during 'the Troubles' alone would seem to demand a sense of proportion in assessing the current threat. In one year alone (1993) – the IRA detonated a staggering 32,000 lb (14,540 kg) of explosive. But the 9/11 Al Qaeda attacks took more lives in one day (2,973) than the IRA did (1,928) in its entire campaign. The 7 July 2005 bombings took more lives than any single IRA attack. The IRA caused one billion pounds' worth of amage at Bishopsgate in the City of London in April 1993 and killed one unfortunate person; had this been a jihadi attack, the bombers would have likely killed far more, along with themselves.

A case in point of terrorists on a 'learning curve', at least in the UK, was the trial in December of the two British Muslims accused of attempting to attack London and Glasgow Airport with cars loaded with gas canisters. The attacks failed because an overseen gap of less than 1mm between the phones and detonators broke the circuit: a simple loose connection saved hundreds of late-night revellers from death and injury. Only one detonator sparked, but even that was quickly snuffed out because the ambitious terrorists had simply filled the cars with too much petrol and gas. However, the Glasgow attack caused mayhem and injury when passengers tried to escape; this situation may well change as soon as disparate groups and individuals begin to perfect their techniques and achieve something akin to 'joined up terrorism'.

The attempted car bomb attack in London in June 2007 failed because mobile phones failed to trigger the explosion.

Then and now

One striking difference between the IRA campaigns and the current threat is that IRA bombs were chiefly aimed at destroying economic infrastructure. The organisation also targeted members of the British armed forces, police, judges and others viewed to be instrumental in continuing British rule in the province, but its bombs were not deliberately aimed at ordinary civilians. When civilians died in IRA bombings and shootings it was counter-productive to the republican cause. Certain weapons were abandoned: the IRA deliberately abandoned one type of device, the blast incendiary, after the La Mon restaurant bombing killed 12 in February 1978. The group never espoused or attempted to use nonconventional weapons.

Today's groups and individual fanatics, however, will not hesitate to blow up, gas, poison, irradiate, or otherwise harm as many of their perceived enemies as they can. Also, unlike the IRA, current terrorists do not leave coded warnings (even misdirected ones). IRA warnings were intended to keep civilians away while commercial infrastructure was destroyed and maximum inconvenience achieved. Warnings sometimes enabled initially deployed devices to be disrupted by the bomb squads and their components separated before the timers ran down. The EOD squads and intelligence units could then analyse the contents. Before remote-handling robots, manual dismantlement – which often took the lives and limbs of EOD operators – would retrieve valuable forensic evidence. But this difference pre-dates 9/11. As far back as July 1995 an al-Qaeda related organisation, the Algerian terror group GIA, bombed a Parisian underground station, killing 7 civilians and wounding 117. The attack three months earlier by a non-Islamicist apocalyptic group, Aum Shinrikyo, on the Tokyo subway with sarin nerve agent, which injured almost a thousand commuters, had no devices and no warnings - and hence, no chance to cordon off an area, let a device 'soak' or render it safe with civilians safely out of the way.

Chiefly, however, the major difference between the IRA and today's Islamist terrorists is the suicide mission. While not necessarily possessing the technical skill of the Provisionals – but learning fast – the jihadi terrorist is willing to die along with his (and increasingly, her) victims. There are no warnings given and therefore no opportunity to diffuse or isolate bombs. Suicide bombings also remove the opportunity to acquire evidence through interrogation and trial of the perpetrators.

continued…

IEDs: the new generation continued...

Insurgents in Afghanistan, Iraq and elsewhere have no need to manufacture or import explosives in areas where military explosive, shells, anti-vehicle mines can be found abandoned in the desert. Vehicles are now loaded with mines and gas cylinders. The detonation method varies constantly: the car 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.

Remote-control detonation and timers, along with multiple disguise methods, pioneered by the IRA are still in common use. Current roadside bombs may be hidden in many ways, such as bombs disguised as rocks. New methods have also appeared: mobile phones have for several years been a common method for remotely activating IEDs and were used in the Madrid 2004 attacks, which were not suicide bombings but used timers.

Rockets are increasingly used, such as Ketyusha rockets from Iran fired by Hezbollah at multiple Israeli locations. Shiite militants in Iraq have used EFPs (Explosively Formed Penetrators) – cylindrical roadside bombs that contain an explosive charge behind a concave metallic, usually copper, liner. When the EFP is detonated, the concave metallic disk is transformed into an extremely high velocity copper penetrator – like a giant copper bullet - that can penetrate vehicle armour with deadly effect. A typical penetrator achieves a strike velocity around 1,500m/s to 1,700m/s. EFPs fired in Iraq killed 170 US forces and wounded 620 from mid-2004 to February 2007.

EOD teams investigating an IED attack in Iraq © *HMS*

The information terrorhighway

In recent years terrorists have attempted to make explosive mixtures and detonators from readily available, unrestricted materials and to acquire expertise from overseas training camps and the growing 'jihadi' password-protected internet networks. Terror networks are increasingly using advanced information technology and the global communications network to expand their capacity and capability to wage a global insurgency against western interests and coalition forces overseas, and local terrorism against civilians at home. Jihadi websites and forums often provide accurate information about military tactics, explosives, technology and intelligence acquisition.

Information sharing is a prime purpose for using the Internet to inform on tactics and operational know-how - from 'kitchen lab' apparatus set-up and basic mixes – to more advanced IED-making and cyberterror techniques. At least one instructional jihadist video teaches the viewer to build an IED expressly designed to penetrate armoured vehicles: a 3D animation can be viewed of each part of the device, its assembly, how to employ it and how the internal mechanism works when detonated. What took the IRA and other groups many years to learn through word of mouth, stolen manuals, and trial and error can now be learnt more quickly these days through a relentless flow of material. It is now relatively easy to make a suicide bomber's belt and execute a basic attack - and in terms of cost, technical ability, target availability and materials needed, it can be achieved with minimal expertise.

Andy Oppenheimer
Defence Consultant
Specialist in nuclear, biological & chemical (NBC) weapons

oppenheimer@btconnect.com
www.andyoppenheimer.com

IEDs: Render safe

A US Congressional panel recently found that the Joint IED Defeat Organisation (JIEDDO) was "falling behind" on bombings in Afghanistan. While terrorists in some countries may still be on a learning curve, so is the US in dealing with their devices and methods in theatres of war. JIEDDO was set up in 2005 by the U.S. Department of Defense and had a proposed $4.4 billion budget for fiscal 2008. Critics are questioning how funding is spent and believe that soldiers in the field have proven quicker at adapting to the enemy than a large bureaucratic US-based organization, despite its growing expertise.

IEDs in Afghanistan are a daily threat to coalition troops. In 2008, 3,276 IEDs were detonated or detected before exploding – a 45% increase compared with 2007. *© JIEDDO*

JIEDDO spends more than $4 billion annually on attacking human networks, providing training support and in rapid acquisition of IED countermeasures, mostly jammers to prevent radio-controlled and other devices from being remotely detonated. From an ad-hoc Army task force created in 2003 JIEDDO has grown to a 3,000-person organization. The House investigators found: "It is impossible to demonstrate which of the specific initiatives and programs supported by JIEDDO are effective and to what degree..." - and that the DoD has invested billions of dollars and created a sprawling organization but IED use continues.

One indicator of success that JIEDDO uses is that over time insurgents in Iraq have been forced to use ever greater numbers of IEDs to inflict casualties on American troops but with a lower casualty rate. But the subcommittee report says that this is perhaps not the best indicator of the organisation's success – that the lower casualty rate is resulting from better intelligence – such as more tips from locals on IED locations and better armouring of vehicles. IED attacks in Iraq have dropped dramatically from 2007 levels mainly because of the surge, the Anbar Awakenings and Muqtada al Sadr's ceasefire. Afghan and Iraqi bomb-makers are indeed being kept on the run, meaning they have to improvise more. Although they have access to mortar bombs and artillery shells, their supply chains can be disrupted. However, the absence of a clear strategy on the part of Al Qaeda et al makes the capabilities of this loosely bound network of fanatics harder to assess and events more difficult, or impossible, to predict.

It can be assumed for many current trouble spots that suicide bomb threats and VBIEDs are prevalent, or intermittent. Suicide bombers are in plentiful supply and can create pure terror. And their methods are changing. Evidence emerged in 2003 of a smaller and lighter explosive that could be compressed into a small bag or hidden in the killer's clothes – soaked in a vest in its liquefied form. Improved detonators and timers may also be used, which enable the bomber to start the countdown before s/he even reaches the target.

EOD equipment and armouring vehicles

EOD equipment has to be designed to cope with many civilian and military scenarios. The prime EOD aim is always to save lives before property. To deal with unexploded ordnance, robots with cameras are used rather than EOD operators whenever possible; novel means of disrupting devices, such as water-jet disruptors to disable car bombs, continue in service. Methods are in constant evolution to react to unpredictable targeting, novel materials, and means of delivery. And EOD squads now also must be able to deal with improvised chemical devices or radioactive dispersal devices.

Smaller, lighter types of bomb-detection robots are being introduced as established robots are too heavy for regular soldiers on patrol and convoy missions. The machines, which regularly preserve life and limb of civilians, troops and EOD operatives, feature a manipulator arm and are built to traverse sand, gravel, and water pits, manoeuvre their arms to lift objects, and position cameras. JIEDDO has spent more than $2.3 billion on developing jammers to thwart simple trigger devices such as two-way radios or garage door openers.

Armouring vehicles against bombs and rockets is a growing defence measure in Afghan and Iraqi theatres. Some MRAP (Mine Resistant Ambush Protected) vehicles are being used to protect EOD engineers through a blast-deflecting V-shaped hull on an open-framed vehicle. Thus enables the shockwave of an IED to blow past the vehicle. Glass laminate armour may be another means of protecting tanks against EFPs by redirecting their kinetic energy laterally along laminations via a 'spiderweb' effect (shattering laterally and vertically). The glass laminate may only need to stop one fired EFP, at least until the insurgents adapt to this new countermeasure. A lighter, future solution is a 'plasma shield' which fills a space with plasma (electrically charged, or 'ionised', gas), and then confines it with a magnetic field.

Training on how to spot and dismantle IEDs has the constant pressure to keep up, and overtake, terrorist tactics. Many counter-IED specialists agree that you have to get inside the insurgents' decision cycles – attack the support network (which may include from overseas); develop intelligence; stop up funding; and kill or capture the bomb makers.

Pre-emption is better than cure

There are other means of interdicting IEDs and related attacks. In both the military and the civilian spheres we are consequently coming to rely increasingly on in-built physical security measures, such as introduction of barriers to keep potential vehicle borne bombs away from key areas and designing bomb-resistant features into new building – defensive as well as pre-emptive measures. Above all – and this was also the case with the IRA - intelligence is the key.

The Defender remotely operative vehicle robot enables IEDs to be rendered safe – and has helped to save the lives of many explosives ordnance disposal (EOD) operatives.
© Allen Vanguard

Restricting information is another countermeasure, but very difficult because of its ubiquity and speed of transmission. Counter-terrorism approaches may include intercepting and closing down funding channels or using international co-operation to track and arrest known terrorists. But the stream of propaganda videos can enable intelligence operatives to track indicators of terrorist methods, to detect changes in tactics and patterns of weapons acquisition. This can enable counterinsurgency forces and civilian services to keep ahead in the race, and enhance the sharing of intelligence among frontline operators.

Collecting intelligence on attempted and executed attacks and then passing that back through the line is critical. As with the 'dirty war' against the IRA, the careful use of informers and intelligence is a key weapon in the countermeasures race. While past informers within a host community used to be almost the sole source in supplying human information (humint) about terrorist plans and actions, tracking the propaganda of today's terrorists can help to prevent them carrying them out. Intelligence operatives therefore look for signs and traces of behaviour within local communities that could indicate a future terror incident or an increase in recruitment to extremist groups.

EOD training – a new era

John Bright & Chris Hunter

Containing bombs to effect a controlled and confined explosion is often the only way to render them safe. © *NABCO*

IEDs are a grass root problem and by their nature require dealing with at the point of delivery. The Counter-IED operator needs to be as inventive as his adversary but the difference is he should have the most comprehensive toolbox in terms of training and equipment. The increased asymmetry of global conflicts is refocusing the EOD community toward the IED threat. While the number of "conventional" weapons based confrontations is decreasing, working as it always will with whoever has the most troops, the best technology and, most importantly, the "biggest armoury" will eventually succeed.

A similar situation exists on the high street where massive superstores with the power of advertising (propaganda), economy of scale on purchasing (ordnance acquisition), staff training and deployment (exercising/tactics/strategy) will also dominate in the final analysis. When left with no competitive product to sell, the grocer has to improvise to make a living; likewise the "freedom fighter", terrorist or aggressive radical.

Mine clearance using a robot with manipulator arm to traverse gravel, sand and water pits. © *US Navy*

Deprived of conventional weaponry, the non-aligned fighter turns to improvising ordnance from whatever is available as to explosives and delivery systems. Intelligence on either of these may be obtained from the www or by direct/indirect contact and information sharing with like-minded radicals. Dealing with these adhoc devices is unlike normal EOD where "render safe" procedures are normally laid down at the point of manufacture and taught at the many military establishments specialising in the training of "ATOs" and the like.

The need for intelligence on the radical cells, their contacts for training, and an awareness of the stocks available to them for the manufacture of IEDs is an essential part of planning countermeasures under identifiable circumstances. Feedback and analysis of information from locals, both anecdotal and practical, provide the basis of developing the applicable modus operandi to combat the IED attack. But predicting who, when and how is, at best, extremely difficult and in fact close to impossible although there are an increasing number of "plots" that are nipped in the bud by improved intelligence gathering, analysis and decision making. Counter-IED measures are incident driven; the only measure that can confound a planned attack is knowledge of at least who and when. The how then becomes less important. The only safe prediction with regard to the use and development of IEDs is to predict the unpredictable.

US Navy EOD robot with built-in camera. © *HMS*

John Bright has worked on the periphery of the EOD/IEDD community for more then 20 years organising seminars and producing many papers and articles on the wider EOD topic. During that period he has seen many changes and developments to threats and resolutions. Current non-aligned group tactics have brought him and Chris Hunter QGM together to provide specialist training seminars.

In our next issue we will continue on the theme of Countermeasures against IEDs with an examination of the current technologies in use in counter-insurgency theatres, and an investigation into technology transfer between terrorist groups.

Weapons intelligence training being conducted on a car. Even destroyed vehicles provide valuable forensic evidence. © *US Navy*

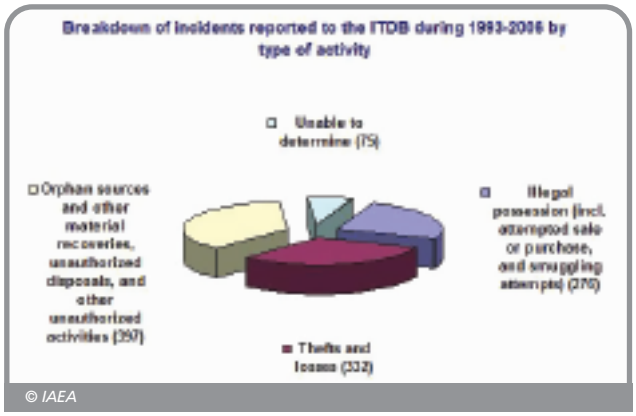
Radiological dispersal weapons: IS there a threat?

For many years I have been writing, advising and lecturing on the radiological threat. First, back in the Cold War, on the nuclear stand-off between the US and the Soviets; later, on proliferation of nuclear weapons to other countries; and more recently, particularly since 9/11, on those things which have come to be called 'dirty bombs' – radiological dispersal devices (RDDs).

On Monday, I think there is a RDD threat. On Tuesday, I don't. And so on. This is one of those conundrums in the pantheon of CBRN analysis that poses seemingly endless challenges, and reflects the difficulties in predicting or assessing such threats – because we, thankfully, have little or no precedent of a RDD attack. Nevertheless, measures for readiness to respond to such an event are in train in many countries, where military units and first-responder services are being equipped and trained to respond to RDDs.

Dirty bombs are not nuclear weapons, as most know – they are conventional explosive devices with a radioactive component. So far, according to the meticulous database maintained by the International Atomic Energy Agency (IAEA) and whatever intelligence services care to publish or announce, there has not been an incident in which a– dirty bomb – has exploded. Lack of precedent is a big problem in planning response and readiness.

Statements by terrorist groups of intent are insufficient in any assessment of capability, expertise or weapons acquisition, despite the constant outpourings of jihadi propaganda about the intended use of nuclear and other non-conventional weapons. Only one RDD instance is known – a dynamite bomb laced with cesium-137, a radioisotope used widely in medicine and industry, planted by Chechen separatists in a Moscow Park in December 1995. It was discovered before it could go off. The Chechens have made four other attempts at RDD deployment and nuclear power plant attack which are not well documented, but are known to the EOD (explosives ordnance disposal) community. There may well be others, especially where insurgency is ongoing.



© IAEA

Although a non-explosive radioactive dispersal event (RDE), the poisoning of Alexander Litvinenko by the rare radioisotope polonium-210 in London in November 2006 provided a rare precedent of an incident other than a nuclear disaster or accidental release. Although apparently intended just for one victim (although some believe the Russians intended it to spread to show what they could do against dissidents), the material used for Litvinenko's assassination spread beyond its original target. It is said that, because Litvinenko talked so much instead of drinking up all of the polonium-laced tea in the alleged teapot containing it, his agonising death took longer - during which time he had 'spread' the contamination to others.

The other, more controversial, example of radiological weapons is the use by armed forces of tank-penetrating shells containing depleted uranium (DU). The jury is still out on whether the particulates from explosions cause Gulf War Syndrome (GWS) and other health problems being endured by army veterans who have seen service in Iraq and other theatres – and by civilians, whose medical records are far harder to acquire for such research. Many official reports have been published on this topic and are mainly inconclusive. Independent researchers have produced detailed accounts attempting to link GWS and other problems with DU, but their research results and methodologies, while sound, have still to be taken seriously.

Factors for assessment

So, how do we assess the threat of an RDD? Many risk reports are based on the incidence and prevalence of radioactive materials smuggling. Figures for arrests, thefts, including 'sting' operations to trap smugglers and other interdictions of smuggling, and losses are recorded by the IAEA. According to the IAEA, from 1993 to 2004 there were more than 400 confirmed incidents of trafficking materials that could only be used to produce a RDD. Most cases involved very small – in grams, not kilos – amounts of nuclear materials. Some materials were weapons-grade or near-weapons grade while others were of civilian-use isotopes, which would in theory have been useful not in a fission weapon, but in a RDD. But it is difficult to trace where the smuggled radioisotopes end up, whether the recipients have any idea what to do with it, or whether they even know it's radioactive.

Risk levels may also be indirectly set by measuring the effectiveness of border and other monitoring authorities and by testing the equipment installed in airports, ports and other locations to detect radiation. Drills and fake smuggling exercises can test awareness and response. For example, a Congressional report in 2007 described how investigators from the US government watchdog, the Government Accountability Office (GAO) in December 2005 smuggled into the US enough cesium-137 to make two RDDs. The material was smuggled in rented cars and driven through two state border checkpoints. Although the cesium triggered detector alarms, the 'smugglers' were able to persuade US Border officials to let them through with it – with false documents. And this was in the US, not a country in a state of war or insurgency.

Civilian sites such as hospitals and research labs which use radioisotopes are not guarded like nuclear weapons facilities or heavily shielded like nuclear power plants, and therefore pose a risk of theft or abandonment of materials. This may be possible with the assistance of insiders or infiltrators. This danger has been highlighted in statements by the British intelligence service, MI5, since the attempted London car bomb and Glasgow airport attacks, for which a National Health Service employee was convicted in December 2008.

How do we know it's an RDD?

Cesium and other gamma emitters are relatively easy to detect. Weapons-grade materials – uranium enriched to 80% and plutonium-239 – and other alpha emitters, most notably the aforementioned polonium-210 – are harder. But only if detectors are taken to every explosive incident (and warfare incidents), and reported thereafter, will anyone know if radiation of any kind is involved.

Radiological dispersal weapons: IS there a threat? continued...

For example, a bomb goes off in a major city. The emergency services are primarily concerned with saving lives and getting people out of harm's way. The media are concerned with reporting the effects of the explosion. They will be the first to ask the authorities and experts if chemicals or other non-conventional means have been used. The first-responder services would also have to be concerned with this, as they would have to assess the area immediately for radiation – or else the explosion will be judged like any other, that is, until victims start showing up in hospital emergency departments with symptoms of acute radiation syndrome or, weeks, months or even years later, cancer. By then, their illnesses – among the commonest worldwide - would likely not be linked to the RDE they were caught up in unless medical practitioners ask the right questions and make a full assessment of the cause of these, and other patients' morbidity and mortality patterns.

Equipment used to survey and remediate premises affected by the Litvinenko radioactive poisoning incident in London in November 2006 © *GDS*

Making RDDs – is it that simple?

Many accounts of RDD threats appear to make their construction and deployment sound simple. Handling unshielded or powdered gamma-emitting materials such as cesium-137, cobalt-60, and other gamma-emitting isotopes in common civilian use is lethal. The dirty-bomber would also have to hide it for long enough and get it into place with a workable detonator and possibly timer to ensure it goes off exactly when and where they want, or simply, as is now terrifyingly common, blow themselves and everyone else up in the vicinity. Original material in an RDD may have to be chemically or physically altered to enhance dispersal. For example, strontium fluoride in some sealed sources is sintered making it essentially insoluble and not useful for effective radiological dispersal. Even suicide terrorists want a cheap and easy means of causing destruction, and usually instant results. The chosen means of causing mayhem is the almost daily use of IEDs in Afghanistan and elsewhere. The attacks in the Indian city of Mumbai in November 2008 involved simple weapons, but a sophisticated level of planning.

Effects – hotly debated

And how dangerous would the radiological component in a device be in terms of effects on victims who survived an explosion? There are varying opinions on this. We now know that radioactive contamination, even if low-level, would necessitate remediation of the properties and area affected by particulate emission from a dirty bomb. That this would be inordinately expensive, economically damaging, and psychologically frightening (due mainly to the public's understandable fear of radiation). The tiny amount of polonium-210 that contaminated as many as 20 premises in London in the Litvinenko incident has meant full decontamination of whole rooms in hotels, while other premises have been left to 'soak' until normal background radiation levels are reached. The RDE in Goiania, Brazil, in 1987, when a medical radiotherapy machine was pillaged and the cesium chloride in it spread by those handling it, necessitated the demolition of many homes and thousands of people to be monitored for months after the stolen material was traced.

Major nuclear events such as the atomic bombings and the Chernobyl disaster, which affected whole populations, are well documented and provide evidence about radiation effects on people, property and land, both short-and long-term. On a far smaller scale, those affected by the Litvinenko incident – that is, those who can be monitored – will provide another set of reference results. Po-210 kills once inhaled or ingested, and of 1,500 possible contacts, some 17 people are known to have been contaminated to above-average levels of radioactivity.

It is hard to conclude how high the threat is of a radiological incident occurring, and being recognised as such, anywhere in the world. The nature, timing, and extent of any CBRN event is impossible to predict. Many scenarios are envisaged for RDD attack and effects and drills to test first response are conducted regularly, particularly in the US. But no exercise can totally imitate the effects of radiation, which is unpredictable, uneven, and dependent on climatic variation, amount and type of radioisotope, positioning of the device, site of the explosion and many other variables. Many experts believe that nuclear accidents are more likely than terrorist acts, while others opine that an RDD attack is just around the corner. As Al Qaeda appear to be in for the long haul, such an event can never be ruled out – but has to be taken in context with other, more prevalent, threats.

Truck being scanned for radioactive materials at checkpoint © *IAEA*

Weapons of Hamas Destruction?

Only days into the Israeli Defence Force (IDF) offensive into Gaza which commenced at the end of 2008, the Israeli defense establishment expressed growing concerns that Hamas missiles would pose a threat to its top-secret nuclear facility at Dimona in the Negev Desert.

The plutonium separation unit at the Dimona nuclear facility in Israel. One of the photos taken by the whistleblower Mordechai Vanunu.

The fear is the dozens of Iranian-made Fajr-3 missiles – range 40 km – Hamas has acquired will bring the nuclear installation 10 km of the town of Dimona, over 30 km (20 miles) east of Beersheba, within its rocket range. The cities of Ashdod and Beersheba – 28 km (18 miles) and 40 km (25 miles) away from the Gaza Strip – are already regularly targeted. During the first 11 days of fighting Hamas launched more than 300 rockets into Israel, hitting targets 40 km into the occupied lands. As well as B-20 and home-made Shewath devices it was estimated, before the Gaza offensive, to possess 6,000 rockets. Many are home-made, using ammonium nitrate and sugar as the explosive charge.

Dimona was exposed as being a nuclear weapons factory by the Israeli whistleblower Mordechai Vanunu, whose photographs of plutonium-core manufacture and other extensive weapons-related activities were published in The Sunday Times in 1986. Successive Israeli governents have refused to confirm or deny this publicly, following a policy of "nuclear ambiguity".

Just how vulnerable is the Dimona plant to rocket attacks? It will be among the most hardened facilities of its kind in the world and is defended from aerial attack by a battery of Hawk anti-aircraft missiles. A complex possibly associated with such defences is evident in IKONOS satellite imagery acquired in July 2000. A Patriot or Arrow anti-missile battery was observed by satellite, believed to have been constructed sometime between 1986 and 2000 – four Scud-derived missiles having been fired close to Dimona by Iraq during the 1991 Gulf War. A site regarded as a probable nuclear waste disposal area is also visible about a kilometre from the main facility which, if attacked (let alone the main plant) would produce a radioactive accident comparable with Chernobyl.

In October 2008 it was reported in the Israeli press that Israel is to install two massive radar antennae near the Dimona nuclear plant to bolster defence against Iran (the main supplier of rockets to both Hamas and Hizbollah groups, and arguably the biggest potential threat to the Jewish state).
A previous attack in the town of Dimona, by a Gaza-based suicide bomber claimed by the "Army of Palestine" wing of Al-Aqsa along with the Popular Front for the Liberation of Palestine (PFLP), killed a woman and wounded 11 others. In 2006 an Israeli District Court charged a member of a breakaway band of the Al Aqsa Martyrs' Brigade with planning a wave of "strategic" attacks in Israel, including simultaneous suicide bombings in various cities, as well as an attack on the Dimona reactor.

It remains to be seen how far the Israelis will eliminate the Hamas rocket threat. The land offensive and intelligence successes are making inroads: Information has been gleaned from Palestinian Authority infiltrators about Hamas militants, their headquarters, shelters and tunnel network beneath Gaza City. As of the first week in January some 370 rockets and mortar rounds had either failed or been intercepted by the IDF. While Hamas has obtained higher grade 122mm Grad artillery rockets manufactured in more than 50 countries and widely available on the black market, the real capability of Hamas to conduct an effective battlefield strategy of surprise and ambush is in doubt, according to the IDF. The longer-range Iranian Fajr-3s fall short of the 50-mile distance to the major cities of Tel Aviv, Jerusalem and – of prime importance – Dimona. Nevertheless, throughout the ground battle Hamas continues to launch rockets at Israel. While these rockets have created havoc and caused misery and injury to their Israeli victims, it could be said they are true terror weapons rather than being of substantial military value, sufficient to take out a large hardened structure such as a nuclear reactor. But this may change: Israeli security experts claim that if Hamas is not curtailed, it will acquire the Iranian Fajr-5, which would put Tel Aviv and Jerusalem – and Dimona – within rocket range.

MI5 threat levels: what are they good for?

In the second week of January Jonathan Evans, head of the British domestic intelligence service MI5, said that the Israeli offensive gave extremists the ammunition they need to gather support – while also stating that the threat of an immediate attack in Britain by Al-Qaeda had diminished. The recent prosecutions of 80-plus suspected terrorists have had a 'chilling' effect on would-be attackers. Nevertheless, the threat level remains 'severe'. While it is understood that various factors, some of them contradictory, define the threat levels, does it help us, the public, to know about this? And what purpose do they serve anyone other than the authorities and services who would be involved in responding to an attack?

It is of course vital we know what is going on, and a reduction of secrecy among intelligence services about this information is welcome. But there may be disagreement among officials and the government about defining the threat level. Evans does not concur with Whitehall officials who in recent months suggested it was close to being raised to 'critical' – the highest. And how consistent and accurate are these warnings? In the 24 hours before the 7 July 2005 suicide bombings in London senior MPs were reassured by the then head of MI5, Dame Eliza Manningham-Buller, that there was no imminent terrorist threat to London or the rest of the country. In this case, the disclosure that MI5 had been so completely taken by surprise on 7 July will fuel calls for a public or independent inquiry into the events leading up to the suicide bomb attacks that claimed 52 lives and injured 700.

Evans also said that Irish dissident groups in Northern Ireland still posed a threat as they continue to target police officers in the province. Those familiar with the Provisional IRA's long campaign were not graced with constant threat level reminders. We also did not witness too many disagreements about the IRA threat level, which was not only constant but, the 1998 Omagh bombing aside, dwarfed anything the dissident groups are able to throw at us. Of course, this may change – they are acquiring enhanced expertise in roadside bomb deployment – but need to be treated separately from the jihadist threat.

The many trials that have concluded in the UK and more still to come are indeed an indicator of successful intelligence operations and interception of terrorists' plans before they come to fruition – hence, no attack. But the threat level will also reflect the extent of terrorist recruitment, community support, economic conditions, and weapons acquisition. According to Evans, Al-Qaeda leaders still intend to mount an attack in Britain and that there are individuals in Britain able to do so (thousands, according to his previous statement in November 2007). This is the real chilling effect – on the public, not so much the would-be terrorists – and may be summed up in the words of the IRA following the 1984 bombing of the Brighton Grand Hotel: "we only have to be lucky once. You have to be lucky always".

Russian roulette

With the inauguration of a new US President imminent, Russian leaders are prepared to take an even tougher stand on US missile defence activities in order to 'test the mettle' of President-elect Barack Obama.

Before taking office Obama had not confirmed his planned policy on pursuing Bush's European missile defence programme, but has indicated that the technology must be proved to function before deployment. This is a marked departure from his predecessors, who chose to install new systems and test them – often with mixed results – only after embarking on a ballistic missile defence programme.

As in the Cold War Russia is objecting to the US ballistic missile defence programme, particularly interceptors and radars to be stationed in Europe. *© TNO Defence and Safety*

Moscow has repeatedly made its objections clear with the Bush administration's plan to install Star Wars Mark III – that is, to deploy 10 missile interceptors in Poland and a radar site in the Czech Republic to counter potential threats from Iran or other rogue nations. Iran in particular is estimated as needing no less than six years to produce missiles capable of hitting targets in Europe or the United States. Russia's response has been to threaten deployment of short-range Iskander missiles in Belarus and its western enclave of Kaliningrad on Poland's northeastern border against what it regards as a threat to its strategic security and to demand access by Russian personnel to the European BMD facilities.

Despite the economic recession Moscow can better afford to match the USA's plans in contrast to the 1980s, when President Reagan hatched the first stages of the Strategic Defense Initiative, which proved inordinately expensive for the Soviet Union to counter. 21st-century Russia – a far richer country with gas reserves as its economic trump card – has already begun an extensive modernisation of its nuclear missile arsenal. Some 70 Russian strategic nuclear missiles are to be commissioned over the next three years, with 50 Topol-M ICBMs planned for installation in the next ten years, some of which may also be deployed in Belarus to counter the US plans for BMD in Europe. The RS-24 tactical nuclear missile could be equipped with multiple nuclear warheads when deployed in 2009. In December, head of the Russian General Staff Gen. Nikolai Makarov stated that his country would keep non-strategic nuclear forces "as long as Europe is unstable and packed with armaments. That is a guarantee of our security." The Russians claim that the RS-24 does not represent a violation of the treaty's ban on adding warheads to single-warhead missiles.

Added to which the most recent treaty signed by the US and Russia setting limits on deployment of nuclear weapons and delivery vehicles, the Strategic Arms Reduction Treaty, will expire at end 2009. Russia is seeking a replacement pact that would also address long-range bombers and other conventional weapons, while the Bush administration believes the focus should remain nuclear.

Makarov also said Russia plans by 2020 to deploy new nuclear-capable missiles capable of penetrating a planned European missile shield – including new complete missile systems "with improved combat characteristics capable of carrying out any tasks, including in conditions where an enemy uses antimissile defence measures" – that is, nuclear artillery shells: non-strategic, short-range, atomic weapons. These plans will coincide with continued funding for Russia's strategic nuclear arsenal, with 13 test launches planned for 2009: five test launches of new missiles, three launches to confirm the extension of missiles' service lives, and five launches of converted SS-18 Satan ICBMs to orbit various satellites, bringing echoes of the 1980s stand-off– when Europe and the UK bristled with deployed short- and medium-range nuclear weapon delivery systems. The Russians have suggested a halt to its further strategic missile deployment if the US backs down over BMD, which the new US President and a Democratic-controlled Congress – having already showed signs of a BMD policy change – may be prepared to do.

When subs collide

Reports in February of a collision deep in the Atlantic Ocean of two nuclear-armed submarines, France's Le Triomphant and Britain's HMS Vanguard, two weeks after the incident occurred have led to the obvious questions: how often have such collisions happened before, and what would happen if the missile tubes – and their city-destroying contents – are breached?

Submarines carrying ballistic missiles with nuclear warheads are not supposed to be heard, and because they are quiet and constantly moving, they are essentially invulnerable to pre-emptive attack – making the sea the prime leg of the nuclear deployment triad for several nuclear weapons states (NWS). The sonar and radar on the subs are intended not only to try to suss out other submarines but also to avoid collisions. But one official appeared to contradict this by saying "They can't see each other in the water" – raising questions about the submarines' sonar and why they did not detect one another. It is believed their respective anti-sonar devices, which aid the stealth activities of the subs, were too effective in concealing them. The American, British, French and Russian nuclear-armed navies which cruise the Atlantic refuse to disclose any information about the whereabouts of missile submarine operations. According to the UK Navy, however, the UK submarine service – like the nuclear industry, both weapons and civil – has been badly undermanned for some time with a shortage of highly skilled technicians.
A more likely explanation is that as France is not part of NATO's military command structure, it does not provide information on the location of its mobile nuclear arms to that system. Another is that environmental factors – the ocean temperature being different at each submarine location – mean that sound cannot penetrate adequately for each submarine to hear the other in time and avoid collision.

Whatever the causes, the possible results of a repeat of such an incident have invited speculation about the likely consequences. According to the French military, damage to the submarines was reportedly minor, restricted to the sonar dome on the front of the submarine. HMS Vanguard, was said to have visible dents on its hull as it was towed home. The warheads were not compromised. Repairs will cost up to £50 million.

Each sub carries 16 multi-warhead missiles; British and French missiles, like those of the United States, are protected against accidental launch or detonation of their warheads. But a stronger impact could have released the warheads and leakage may have occurred; it could also have sent both subs and their crews to the bottom and possibly dispersed plutonium – mainly from the reactors - into surrounding waters. This would have not only poisoned the crew but would have spread radioactive waste for miles across the Atlantic.

The main well-known precedent for a submarine disaster was the sinking of the Kursk in 2000 with the loss of its entire 118-man crew, and the recent incident is reportedly the first time since the Cold War that two nuclear-armed subs are known to have collided. A UK precedent, two years later, occurred when the nuclear submarine HMS Trafalgar ran aground during a training exercise off the Isle of Skye in Scotland. In 2007, an explosion occurred aboard the HMS Tireless, killing two sailors and injuring another during operations of the vessel's self-contained oxygen generator, a stand-by method of producing oxygen during a power outage.

Products

FiReControl from Bruhn NewTech

Bruhn NewTech, UK is to provide hazard prediction software for FiReControl, a £300-million UK Resilience project set up by the UK Communities and Local Government (CLG) to enhance response to large-scale incidents such as industrial accidents and terrorist attacks. FiReControl is scheduled to be operational before the 2012 Olympics in London to offer greater protection to fire-fighters and the public during first response. In conjunction with the Lead System Integrator, EADS DS, Bruhn NewTech will supply the software to the CLG's nine Regional Control Centres (RCCs) and will take on implementation of software and associated training. The FiReControl system will combine IT-based information management with the practical issues of risk management in the battlespace and equivalent civil emergency operations.

Fire and Rescue from VT GROUP

Defence and support services company VT Group (VT) has begun providing capability management for England's national resilience fleet of emergency vehicles and equipment modules. In a contract with Firebuy Limited, on behalf of the CLG, VT is responsible for making the national capability available for deployment around England in the event of major incidents. The assets are operated by the 46 Fire and Rescue Services throughout England, comprising more than 500 vehicles and specialist modules for dealing with major emergencies such as floods, terrorist attacks and urban search and rescue for collapsed buildings. VT will support the vehicles and equipment modules at locations throughout the country, on an availability basis, and will also provide related services including logistics and communications management. The 16-year programme, with an option for up to four further years, is a primary outsource worth in excess of £100 million and sees VT strengthen its position in the civil resilience sector.

Gore cools off

The GORE® Active Cooling vest

New products in CBRN personal protective equipment (PPE) must be designed for minimum heat stress, which can greatly hamper infantry performance in the field and civilian incident response in cramped, hot and difficult rescue conditions. With this in mind, Gore Associates has launched a one-size-fits-all GORE® Active Cooling vest. A two-layer construction, the vest features a non-burning or melting inner layer. Air is pumped between the layers and passes through the perforated inner to the wearer's torso to enhance the body's natural cooling process. Providing up to 150W cooling power, GORE® Active Cooling vests are wearable with or without body armour. Light, compact blower units fitted in lifting pockets provide over eight hours' operation at full cooling power and up to 17 hours at reduced power without producing additional thermal load under body armour. The suit is claimed to provide all-day cooling with minimum impact on movement, right or left-handed donning and easy emergency removal. It can be integrated with other garments, equipment and operating environment. The blowers are rechargeable in 3.5 hours from flat and come with mains and in-vehicle charging options. The Active Cooling products can also be used with an 'in-vehicle' blower connection option.

Secondary nuclear detection for DNDO

When shielded or small amounts of nuclear material in cargo shipments pass through detection systems they may not always sound a reading. Therefore the Department of Homeland Security Domestic Nuclear Detection Office (DNDO) has awarded L-3 Security & Detection Systems has been awarded an $8.5 million contract to develop a secondary inspection system for nuclear material. The system is intended to clear or detect nuclear material in any containers that fail primary inspection. As a portable system, it will be able to identify nuclear isotopes, and distinguish between normal cargo and more sinister packages that are well shielded and well masked. L-3 is currently working with staff at the Massachusetts Institute of Technology (MIT) in using related technology under the Shielded Nuclear Alarm Resolution (SNAR) programme. L-3 also continues to develop the Cargo Advanced Automated Radiography System (CAARS), an initiative also funded by the DHS/DNDO. CAARS uses dual-energy X-rays and is designed to automatically detect shielded special nuclear materials (weapons-grade uranium and plutonium) hidden in trucks and shipping containers.

Fingering Biovein

Easydentic Group, which specialises in biometrics, visual recognition and visual mobility technology for enterprise security, has selected Hitachi's finger vein security finger authentication system for Easydentic's Biovein security control system.

The Finger Vein Authentication System captures images of the vein patterns inside the finger by by passing a near-infrared light through it, allowing an image to be recorded on a CCD camera underneath. The vein patterns, like other biometric data, are unique. But significantly, because they are inside the body, are virtually impossible to replicate while offering a maximum of security.

In operation, light penetrates through the finger using a light-transmission technique to allow the detection of the vein pattern, which is image-processed using a special algorithm resulting in digital data which can be stored in a relevant data repository.

The reading device can be applied to car entry, personal authentication, PC login, door access systems and validation for ATM machines. Intended as a quick, discreet and non-invasive ID system, various applications have been commercialised such as PC login devices, door access systems and validation devices for ATMs in Japan, where 80 per cent of financial institutions have adopted finger vein biometrics.

HazMatID Ranger from Smiths

Smiths HazMatID Ranger

The HazMatID Ranger chemical identifier from Smiths Detection is designed for handheld, backpack or robot portability and ease of use in protective gear. It features touch-to-sample operation and utilises FT-IR technology. Analysis is performed by simply touching a diamond ATR sensor tip directly to a sample. The HazMatID Ranger provides both spectral results and a list of more than 32,000 substances including white powders, chemical warfare agents, explosives, narcotics & drugs precursors, pesticides, common chemicals, and toxic industrial chemicals. This is intended to enhance first-response capability to identify chemicals, as well as components in mixtures – an increasingly vital aspect of detection given the growing threat of novel and improvised chemical and explosive mixes in terrorist weapons acquisition.

DIARY PAGE – Conferences and Exhibitions

March

17-19 March
GSA 2009
Singapore Expo, Singapore
www.globalsecasia.com

April

14-17 April
LAAD 2009
RIOCENTRO, Rio de Janeiro, Brazil
www.laadexpo.com

May

11-14 May
IFSEC
NEC, Birmingham, UK
www.ifsec.co.uk

June

3-4 June
TRANSEC WORLD
RAI Amsterdam, The Netherlands
www.transec.com

6-11 June
UDT EUROPE 2009
Cannes, France
www.udt-europe.com

10 June
NATIONAL RISK 2009 CONFERENCE
City Hall, London, United Kingdom
www.nationalrisk.com

23-29 June
MARITIME ECONOMIC TERRORISM CONFERENCE
London, United Kingdom
www.met09.com

July

21-23 July
UV EUROPE 2009
The Celtic Manor Resort, Newport, Wales & West
Wales Airport, Wales, UK
www.shephard.co.uk

September

8-11 September
DSEi 2009
ExCel, Docklands, London, UK
www.dsei.co.uk

30 September – 1 October
NIGHT-VISION/EOS 2009
Gaylord National Hotel and Convention Center,
201 Waterfront Street, National Harbor,
MD 20745, USA
www.shephard.co.uk

October

28-29 October
SECURE LONDON 2009
The Tower Guoman, London, UK
www.shephard.co.uk

November

17-20 November
MILIPOL PARIS
Paris Expo Porte, Paris, France
www.milipol.com