The threat of asymmetric attack methods
June 2016
The threat of asymmetric attack methods

June 2016

Overview 4

Attack Methods & Order of Threat
Chemical 6
Radiological 9
Biological 12
Nuclear 14

Conclusions 16
## Costs of 9/11 to the US

<table>
<thead>
<tr>
<th>Cost Description</th>
<th>USD billions</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 civilian aircraft destroyed</td>
<td>0.4 bn</td>
</tr>
<tr>
<td>World Trade Centre (replacement costs)</td>
<td>3—4.5 bn</td>
</tr>
<tr>
<td>Damage to the Pentagon, up to</td>
<td>1 bn</td>
</tr>
<tr>
<td>Clean-up costs</td>
<td>1.3 bn</td>
</tr>
<tr>
<td>Property and infrastructure damage</td>
<td>10—13 bn</td>
</tr>
<tr>
<td>Federal emergency funds</td>
<td>40 bn</td>
</tr>
<tr>
<td>Heightened airport security, sky marshals, government takeover of airport security, new in-aircraft security measures, cost of operations in Afghanistan</td>
<td></td>
</tr>
<tr>
<td>Direct job losses: 83,000. Lost wages</td>
<td>17 bn</td>
</tr>
<tr>
<td>Level of damaged or unrecoverable property</td>
<td>21.8 bn</td>
</tr>
<tr>
<td>Losses to NYC</td>
<td>95 bn</td>
</tr>
<tr>
<td>Lost jobs, taxes, damage to infrastructure, cleaning</td>
<td></td>
</tr>
<tr>
<td>Losses to the insurance industry</td>
<td>40 bn</td>
</tr>
<tr>
<td>Loss of air traffic revenue</td>
<td>10 bn</td>
</tr>
<tr>
<td>Fall of global markets</td>
<td>incalculable</td>
</tr>
</tbody>
</table>

Source: Institute for the Analysis of Global Security
The difficulty of predicting the future is no warrant to ignore it.  

The cost of 9/11 demonstrates the scale of damage that can be inflicted by asymmetric attack methods. No one predicted the nature of the attack, or even the intent of Islamic militant groups to fly tonnes of aviation fuel into the heart of the US financial and military establishment. Such attacks, involving mass causalities and unconventional methods of delivery, are clearly rare and catastrophic events due to the difficulties in planning and execution, as well as significant improvements in law enforcement and intelligence practices. However, today’s threat actors undoubtedly aspire to emulate these types of mass-causality events.

The challenge now is to try and predict the next catastrophic terrorist event and not merely react to it. Although a high degree of accuracy is hard to achieve with events shaped by human behaviour, there is a significant body of intelligence which suggests that the next catastrophic terrorist event could quite possibly involve a chemical, biological, radiological or even nuclear (“CBRN”) component. The evidence for this is clear, present and dangerous: the continued use of chemical IEDs in Syria, Iraq and Jakarta; Daesh websites and social media chatter declaring their intent to develop a radiological capability; the FBI Moldovan sting operation that prevented the sale of radiological material to Islamic militant groups; and the recent unconfirmed reports of a Daesh-affiliated anthrax plot in Kenya (May 2016). The perpetrators of the Brussels attacks were also reported to have been conducting surveillance on a senior official in Belgium’s nuclear research and development programme.

As pressure on Daesh intensifies, the possibility of more fighters returning back to their home countries increases the threat of a transfer of technology, operational tactics and weapons used in the Middle East to a wider global setting. Asymmetric uses of CBRN devices provide shock, awe and mass casualties, a lure that Daesh would be unlikely to ignore as their territorial hold in Iraq and Syria shrinks. ▶
It should be stressed that conventional CBRN weapon systems represent a highly advanced capability, with significant barriers to acquisition, production, weaponisation and delivery. Current intelligence assessments conclude that Daesh’s aspirations exceed their capability to unleash a chemical or radiological device against a Western target, but they are investing significant resources into enhancing this capability. In spite of the many technological barriers, it is usually the psychological impact of these weapon systems that has the potential to cause widespread panic and significant economic losses, irrespective of the success of an attack.

The concern is not that terrorist groups are on the brink of acquiring a fully-operational CBRN capability — the technical barriers, particularly in the case of nuclear and biological weapons, entail that these weapon systems generally only reach their destructive potential at the hands of nation states. Rather, there is a justified concern about the psychological and economic impacts of chemical and radiological weapons deployed in an unconventional setting. What would the effects of a partially successful chemical or radiological device be? The kinetic effects may be limited — the device may not fully function, the chemical or radiological payload may be consumed in the explosion — but how would the public react and what would the levels of interruption to business be? These are important questions for the (re)insurance industry. As the principal terrorism reinsurer of commercial property in the UK there is a need for Pool Re to monitor the threat landscape to identify changes and developments in terrorists’ tactics and capability.

**Pool Re and CBRN**

Since 2003, Pool Re has provided cover for acts of terrorism involving CBRN attack methods to their full insured value. In recognition of changing threat landscape, and increase in threat actors with the intent to deploy CBRN-enabled devices, Pool Re is currently working with Cranfield University, in association with Guy Carpenter, to enhance our understanding of the possible effects of such attacks on the UK. The research will ultimately produce a detailed loss estimation model for CBRN attacks that could affect Pool Re’s exposure across the UK. The model, designed to deal with a number of CBRN attacks and scenarios, is set to be the first of its kind to quantify this peril to the level of detail required. It will involve the use of sophisticated computational fluid dynamics to accurately assess how such agents would behave in an urban environment, such as London. It is assessed that the model will provide a valuable risk mitigation tool and have research applications beyond the (re)insurance market.
IEDs with a chemical payload have seen significant use in Iraq and Syria.

The head of the Organisation for the Prohibition of Chemical Weapons (OPCW) reported that they believe that Daesh are beginning to acquire the capability to manufacture their own chemical weapons. In February 2016, John Brennan, the Director of the CIA, also stated that Daesh has the capability to make small quantities of chlorine and mustard agents. More recent reports suggest that the group has conducted experiments on prisoners to refine their devices and have set-up a dedicated research arm based in Mosul, comprised of foreign experts and scientists who worked on Saddam Hussein’s chemical weapons programmes in the 1980s and 1990s. Furthermore, discussions held with CBRN specialists, recently returned from the region, indicate that Daesh are also experimenting with radiological dispersion devices (‘dirty bombs’). Our sources reported that these devices would not be suitable for the group’s strategy in Syria and Iraq, but would clearly have application to asymmetrical attacks against Western targets.

One of the significant differences between chemical, and to a large extent radiological devices, as opposed to the nuclear and biological ones, is the materials used to manufacture chemical or radiological weapons have dual uses — they have an industrial and commercial use, making them more widely available, as well as an offensive use. Although deadly biological pathogens and toxins are used in medical research, the quantities available, complex storage requirements and number of institutions holding them is severely limited. By contrast, certain chemicals and radioactive isotopes have almost every-day applications and are more freely available.

In the case of chemical devices, there is the added dimension of stockpiles acquired in conflict zones. It is no secret that there are significant stockpiles of chemical agents that have fallen into the hands of Islamic militant groups, particularly Daesh, in Syria and Iraq. Consultations held with CBRN specialists working in Iraq and Syria have identified the following events as evidence for Daesh’s increasing use of chemical weapons:

2. ‘Isil manufacturing its own chemical weapons, warns watchdog’, The Telegraph, 4 May 2016

3. ‘John Brennan, CIA director: Islamic State has used, and can make, chemical weapons’, The Washington Times, 12 February 2016

4. ‘Isil manufacturing its own chemical weapons, warns watchdog’, The Telegraph, 4 May 2016
Global reach

There is also the additional threat posed by the increasing ability of the major terrorist groups to communicate securely, through largely open source encrypted messaging services, and pass on operational information and technical knowledge to assist geographically disparate cells. A good example of this is the Mubtakar device, an improvised Cyanide-producing device that has been found in either a physical or digital form in Iraq, Afghanistan, the US and UK.

Sources close to Aimen Dean, a former Al-Qaeda operative who worked as an MI6 source for 12 years, reported that Dean witnessed the development of this programme and confirmed its viability. Conversations held with medical staff based in Aleppo also indicate that a Daesh suicide bomber used Cyanide to kill up to 50 members of a rival Islamist group, Ahrar al-Sham, in October 2014.

The most concerning example of Daesh’s ability to collate and disseminate tactical information globally came in January 2014, when a Daesh laptop was captured in Idlib province Syria. The laptop contained 19 pages of Arabic text on how to make biological weapons from animals infected by bubonic plague, as well as large amounts of data on conventional IED construction and other attack methods.

This rapid knowledge transfer, coupled with the declared desire for “spectacular” style attacks, increases the risk that formally isolated terrorist cells will successfully prosecute an attack with significant consequences.
Daesh have also been on the receiving end of Syrian Regime chlorine barrel bombs on a number of occasions around the contested city of Deir Ezzor, which the group has been trying to take for the last 18 months. A number of analysts have suggested that the Regime’s chemical attacks are preventing this and the effectiveness of chemical weapons, which Daesh have witnessed in Deir Ezzor, is a key reason they are now using these weapons with increasing frequency.

As with all CBRN weapon systems, the effectiveness of a chemical strike may be limited — the wind may blow in the wrong direction, the explosive dispersion method may consume much of the chemical agent — but the psychological effects and the wider loss in public confidence have the potential to cause substantial economic losses. In the above example of the attack on Taza in Iraq, in spite of minimal causalities, compared to losses suffered in conventional operations — the recapture of Ramadi, for example — Hussein Abbas, the major of Taza, reported that 25,000 people left the surrounding area in fear of another attack. Were a similar event to take place in the UK the effects to public order could be catastrophic.

In line with chemical devices, due to the availability of radiological isotopes, a radiological device presents a greater threat to the UK than alternative, and inherently more complex, biological and nuclear weapon systems.

It should be stressed that a radiological dispersal device (RDD) is not a nuclear weapon, or even an Improvised Nuclear Device ‘IND’ (a less sophisticated version, still involving fissile material in an explosive chain reaction). An RDD (‘dirty bomb’) could be as simple as a small amount of radioactive material strapped to a conventional explosive device. The purpose is not to engineer a chain reaction involving nuclear fission, as is the case in a nuclear device or IND, but to contaminate an area, causing death and damage to property as a result of the conventional blast effects of the device and radiological contamination.

The threat from an RDD comes from the availability of radiological sources and their suitability as an asymmetrical weapons system. The table below details radioactive sources that can be found in a commercial setting.⁹

### Examples of Radiological Isotopes And Their Common Use

<table>
<thead>
<tr>
<th>Radionuclide and Emission</th>
<th>Half-Life</th>
<th>Chemical Form (typical)</th>
<th>Typical Use and Activity</th>
<th>Common Radiation Uses</th>
<th>Typical Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cobalt-60</td>
<td>5.3 yrs</td>
<td>Hard Metal</td>
<td>Teledthrapy (1,000s Ci)</td>
<td>Used to treat cancer tumours</td>
<td>Hospitals / Medical Research Facilities</td>
</tr>
<tr>
<td>Caesium-137</td>
<td>30.1 yrs</td>
<td>Salt Powder</td>
<td>Irradiators (1,000s Ci)</td>
<td>Used to irradiate blood prior to transfusion</td>
<td>Hospitals / Medical Research Facilities</td>
</tr>
<tr>
<td>Iridium-192</td>
<td>74 days</td>
<td>Hard Metal</td>
<td>Radiography (~100 Ci)</td>
<td>Used to determine the quality of a particular material and detects areas of varying density and composition.</td>
<td>Extractive Industries / Academic Research Facilities</td>
</tr>
<tr>
<td>Americium-124/ Beryllium</td>
<td>432 yrs</td>
<td>Mixture of Oxide / Metal</td>
<td>Well Logging (~10Ci)</td>
<td>Radiation is used to measure properties of the geologic strata through which a well has been or is being drilled to examine earth formations.</td>
<td>Extractive Industries</td>
</tr>
</tbody>
</table>

Source: Nuclear Threat Initiative

⁹. Argonne National Laboratory, a research facility for the US Department of Energy, has identified an additional five radiological isotopes that would be usable in a RDD. They include Radium-226, Plutonium-238, Californium 252, Polonium-210 and Strontium-90.
The potential length of the decontamination process, as witnessed by the half-life of some of these commercially available isotopes, represents the principal concern. Denial of access to commercial property and the containment issues surrounding the dispersal of radioactive material have the potential to cause large costs to (re) insurers and the wider economy.

**Ease of weaponisation and delivery**

As highlighted above, an RDD is not necessarily a sophisticated weapon. Terrorist groups certainly have the capability to create a wide variety of explosive devices at varying levels of sophistication. Given the relative availability of radiological sources, what are the formal barriers to weaponisation and delivery of a radiological device in the UK?

Radiological isotopes cannot be manufactured with the ease of chemical sources — a nuclear reactor or a mining and enrichment process are required. Theft or state sponsorship are therefore the only methods for acquisition.

The IAEA track and record all radiological isotopes and log the loss of any material classified as Special Nuclear Material. The chart below details the incidents reported to the IAEA involving unauthorised possession and related criminal activities of radiological material.

---

**Radiological incidents**

Confirmed incidents involving unauthorised possession and related criminal activities, 1993 — 2015

- **1993**: 12 incidents
- **1994**: 32 incidents
- **1995**: 48 incidents
- **1996**: 32 incidents
- **1997**: 12 incidents
- **1998**: 0 incidents
- **1999**: 0 incidents
- **2000**: 0 incidents
- **2001**: 0 incidents
- **2002**: 0 incidents
- **2003**: 0 incidents
- **2004**: 0 incidents
- **2005**: 0 incidents
- **2006**: 0 incidents
- **2007**: 0 incidents
- **2008**: 0 incidents
- **2009**: 0 incidents
- **2010**: 0 incidents
- **2011**: 0 incidents
- **2012**: 0 incidents
- **2013**: 0 incidents
- **2014**: 0 incidents
- **2015**: 0 incidents
- **2016**: 0 incidents

*Source: IAEA Incident and Trafficking Database*
In addition to international monitoring by the IAEA, the UK has an effective detection system for radiological sources. Programme Cyclamen is a joint initiative between the UK Border Force and Home Office that monitors any potential trafficking of radiological isotopes at points of entry throughout the UK. This detection capability is supplemented by Mobile Radiation Detection Units (MRDUs) that are deployed at high profile events and key locations (including ports), informed by the latest intelligence assessments and risk profiles.

These preventative measures provide a significant defence to the UK against radiological devices. However, as the targeted assassination of Alexander Litvinenko with a small amount of Polonium 210 at a Mayfair hotel in 2006 suggests, small-scale radiological attacks are possible (although it should be noted that Programme Cyclamen did not become fully operational until 2009, and the government continues to improve and invest in these capabilities). In spite of only one fatality, 10 buildings, 2 cars and 4 planes were contaminated; the Millennium Hotel suffered 12 days of business interruption, with some areas estimated to have been off-limits for up to 5 years; additionally, the total clean-up cost exceeded GBP 4.4 million.10

There is a risk that such small-scale radiological attacks could happen again on the UK mainland. This leaves the possibility that devices with limited amounts of radiological material could be effectively employed by terrorist groups, causing significant costs to (re)insurers, in the form of property damage and business interruption, as well as damaging public confidence in the UK’s preventative measures.

The Moldovan Sting
Between 2010 and 2015 Moldovan authorities and the FBI intercepted four attempts by Russian-linked gangs to sell radioactive material to terrorist groups. In the most recent case (February 2015) Caesium-137 was offered to undercover agents with the express purpose of supplying Islamic extremists.

Biological weapons require a high level of expertise not only to acquire the raw materials but to effectively weaponise them.

Examples of significant biological incidents also provide inconclusive evidence as to the conventional effectiveness of biological weapons. In line with this, the incubation period for most biological weapons represents a disadvantage for terrorist groups seeking propaganda from attacks, as such pathogens or toxins are not generally fast acting and can go unnoticed if they are not ingested.

The cultivation of anthrax, or any deadly pathogen or toxin, not only requires high levels of expertise but is extremely hazardous even to well-equipped specialists working in a secure bio lab. The realities of a terrorist ‘bio cell’ cultivating anthrax, or something similar, behind closed doors would most probably result in failure, and quite possibly the deaths of those involved. Even stealing a pathogen or toxin from a secure laboratory setting would yield small quantities and still require ‘scaling up’ to produce amounts that would result in significant causalities.

It should be noted that the risk of theft has increased with the rise in medical research Biosafety Level (BSL) 3 and 4 Laboratories. BSL 4 laboratories have the authority to carry the most dangerous biological agents, such as haemorrhagic fevers (Ebola and Marburg) as well as smallpox and anthrax; BSL 3 facilities contain less dangerous but still lethal pathogens such as bubonic plague, SARs and yellow fever. There are currently 59 declared BSL 4 laboratories globally, 9 of which are UK-based. Additionally, there are an estimated 600 BSL 3 laboratories within the UK which represents a significant increase from 347 in 2007.  

In 1979, dried *anthrax* spores were released through an exposed ventilation system at a Soviet military instillation. 65,000 people were exposed to the pathogen. Only 70 were reported to have been infected, with 68 deaths. The incident is often referred to as the ‘bio Chernobyl’, but raises questions around anthrax as a suitable weapon, given the high exposure and low infection rate.

National Security Archive

11. Pool Re Threat Study, produced by Avon Protection
Although there is a greater availability of potential biological sources, effective weaponisation is highly problematic. Many delivery systems have been tested over the years, most notoriously by Saddam Hussein during the 1990s. They can range from conventional military delivery methods — missile delivery systems, aerial bombs, aircraft-borne spray systems, drones, landmines, artillery shells, — to low-tech solutions such as a ‘cold bomb’ — dry ice in a drinks bottle. Regardless of the method of delivery, biological weapons are a complex affair, requiring the effective fusion of a number of scientific fields: microbiology, pathology, aerosol physics, aerobiology and meteorology, to name a few.

In spite of the technical barriers, a persistent theme with CBRN capabilities is the psychological hold they have over us — irrespective of the realities of prosecuting a fully-scaled attack. This increases the threat that asymmetric uses of biological weapons pose as even a series of credible hoaxes can be highly disruptive to business activity. Events such as the US anthrax attacks demonstrate that a partially successful biological attack would still involve heavy costs to the (re)insurance industry, in terms of business interruption and decontamination.

US Anthrax Attacks

Following 9/11, anonymous letters containing dried anthrax spores were sent to US senators and several media offices.

In spite of minimal causality numbers — 5 deaths and 17 non-fatal injuries — and damage to property, the clean-up operation, and other associated costs, was estimated by the FBI to exceed USD 1 billion.

In terms of business interruption, the Brentwood postal facility was closed for 26 months and cost USD 130 million to decontaminate.

The New Jersey postal facility was closed until March 2005 and cost USD 65 million.

The US Environmental Protection Agency spent USD 41.7 million on the decontamination of a number of government buildings in Washington D.C.
A conventional nuclear attack appears the least likely attack method for a terrorist group.

The probability of any terrorist group acquiring a fully operational nuclear device, let alone managing to smuggle it into the heart of a Western capital, is likely to be exceedingly small.

In the unlikely event of a terrorist group obtaining such a capability it would probably come in the form of a manufactured Improvised Nuclear Device (IND). This is due to the fact that only nuclear-equipped nation states hold modern nuclear weapons and the sale or sponsorship of such a capability would not be in the foreseeable interests of any nation state. An IND could, however, be manufactured from a stolen, or otherwise acquired, source of weapons-grade nuclear material. Such a device would be similar in design to the first atomic weapon – Little Boy – which used a gun-type design, pictured in Fig.2, that fired one amount of U-235 at another to combine the two masses. The effect of this sudden combination of the two masses creates a critical mass that has the ability to initiate an explosive chain reaction involving nuclear fission (the splitting of the atomic nuclei) and cause detonation. However, this is very difficult to achieve as the speed at which the two masses combine is the determining factor in creating the chain reaction. It is far more likely that such a device would result in the dispersal of radioactive material, similar to an RDD, through the conventional explosive within the device, rather than producing a nuclear chain reaction.

Fig 2, Improvised Nuclear Device
Often referred to as a Gun Gadget Device

During the Cold War, a small group of countries holding nuclear weapons (primarily the USA, USSR and France) did develop limited-yield tactical nuclear weapons in the form of artillery and special atomic demolitions (man-portable nuclear weapons designed for the destruction of critical national infrastructure). There is a remote possibility that such legacy devices would present an additional source for terrorist groups seeking to acquire a nuclear device.
Independently of the exacting technological standards required to produce an IND, there is general agreement that the acquisition, or production, of a nuclear device would require significant input and assistance from a nation state.

In such an instance, where a nuclear-equipped nation state does enable a terrorist group to prosecute such an attack against the UK, not only would the damage be of a scale as to eclipse any recovery efforts by the (re)insurance industry, but it could quite possibly count as an act of war, and therefore be excluded not only by the Pool Re Scheme, but the (re)insurance market generally. The realities of a terrorist group detonating a nuclear weapon or device on the UK mainland would cause levels of damage on such a scale as to make the Government the principal contributor to disaster recovery. Whilst we do not dismiss the gravity of such an attack, our role in recovery assistance is inherently limited by the scale of devastation.
Conclusions

There is a reoccurring theme with all CBRN weapon systems that the emotional and psychological impact has the potential to cause far greater losses than the physical effects of an attack.¹³

This appears to tip the balance in favour of the perpetrator over those charged to prevent such an event. Without well-considered mitigation measures and sound planning, our natural reaction to such an event could easily cause self-inflicted damages quite independently of the physical outcome of an attack.

The significant technical barriers to acquiring an effective CBRN capability are likely to hinder a terrorist group prosecuting a successful attack. Success, however, in the sphere of asymmetric threats is not necessarily measured in terms of lives lost or buildings destroyed — the fear and panic alone would cause a widespread loss in confidence in the UK’s protective measures. This in turn would have severe economic consequences in the form of business interruption and wider costs to GDP. How many employees would travel into work, or make use of the country’s city centres and transport infrastructure even after a series of credible hoaxes, let alone a small-scale chemical or radiological attack? The ‘hard effects’ of these weapon systems may be currently limited in the hands of terrorist groups but the less tangible effects have the capacity to cause high levels of losses to the UK economy.

Like any threat, there are mitigation protocols, operating procedures, training and equipment which, if appropriately sourced and delivered, can minimise the physical and psychological damage, as well as the potential liability which could emanate from a CBRN terrorist attack. Pool Re will be developing these procedures, in conjunction with our expert partners, to provide effective mitigation advice to the wider (re)insurance market.

As well as developing mitigation protocols, Pool Re are continually monitoring the threat landscape through investment in our internal research capability, as well as commissioning research with centres of expertise, such as Cranfield, to enhance our modelling and understanding of the threat. We aim to inform our Members and the wider business community of any findings that may affect industry risk profiling. ●

¹³ This is obviously not the case with a nuclear device, but we do not consider it a likely attack method for a terrorist group.