LLOYD'S

Emerging Risk Report – 2016
Innovation Series

SOCIETY & SECURITY

Use of Chemical, Biological, Radiological and Nuclear Weapons by Non-State Actors

Emerging trends and risk factors

CHATHAM HOUSE
The Royal Institute of International Affairs

About Lloyd's

Lloyd's is the world's only specialist insurance and reinsurance market, and offers a unique concentration of expertise and talent, backed by strong financial ratings and international licences. It is often the first to insure new, unusual or complex risks, providing innovative insurance solutions for local, cross-border and global risks. Its strength lies in the diversity and expertise of the brokers and managing agents working at Lloyd's, supported by capital from across the world. In 2016, more than 90 syndicates are underwriting insurance and reinsurance at Lloyd's, covering all lines of business from more than 200 countries and territories worldwide. Lloyd's is regulated by the Prudential Regulatory Authority and the Financial Conduct Authority.

Key contacts

Trevor Maynard
Head, Exposure Management & Reinsurance
trevor.maynard@lloyds.com

Nick Beecroft
Manager, Emerging Risks & Research
nick.beecroft@lloyds.com

Charlotte Searle
Executive, Emerging Risks & Research
charlotte.searle@lloyds.com

About the authors

Dr Beyza Unal is a research fellow with the International Security Department at Chatham House. She specialises in nuclear weapons policies and her current research explores the humanitarian impacts of nuclear weapons testing. She is interested in NATO's defence and security policy as well as security in the Middle East. Dr Unal formerly worked in the Strategic Analysis Branch at NATO Allied Command Transformation, taught international relations, transcribed interviews on Turkish political history, and served as an international election observer during the 2010 Iraqi parliamentary elections. She has been given various fellowships for her achievements – foremost, she is a J. William Fulbright alumna. She has received funding from the US Department of Energy to participate in workshops at the Brookhaven National Laboratory and the James Martin Center for Nonproliferation Studies.

Sasan Aghlani is a research assistant in the International Security Department at Chatham House, and is co-author of the 2014 Chatham House report, ***Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy***. He is currently pursuing a PhD at the School of Oriental and African Studies (SOAS), University of London, in the Department of Politics and International Studies. He holds a BA in Politics from Goldsmiths, University of London, and an MSc in International Relations from the London School of Economics and Political Science (LSE).

Acknowledgements

The authors would like to thank reviewers Steven Johnson and Stephen Donnelly for their advice and comments on the report. They would like to acknowledge, with much appreciation, the crucial guidance and feedback of Dr Patricia Lewis, and Richard Woolgar-James and Clare Henley for their assistance in preparation of this report.

Disclaimer

This report has been produced for Lloyd's by Chatham House for general information purposes only. While care has been taken in gathering the data and preparing the report, Lloyd's does not make any representations or warranties as to its accuracy or completeness and expressly excludes to the maximum extent permitted by law all those that might otherwise be implied.

Lloyd's accepts no responsibility or liability for any loss or damage of any nature occasioned to any person as a result of acting or refraining from acting as a result of, or in reliance on, any statement, fact, figure or expression of opinion or belief contained in this report. This report does not constitute advice of any kind.

© Lloyd's 2016 All rights reserved

Date of publication: January 2016

Contents

Executive summary	02
Introduction	03
What are chemical, biological, radiological and nuclear weapons?	05
Strategic trends in the CBRN threat	07
CBRN threat matrix	09
CBRN threats: capability and intent	10
Chemical weapons	10
Biological weapons	12
Radiological weapons	14
Nuclear weapons	16
Emerging technologies: threats and opportunities	18
Nanotechnology	18
Synthetic biology and chemicals	18
Cyber technology	19
Drone technology	19
New detection technologies	19
3D printing	19
Risk management and resilience	20
Increasing security	20
Ensuring laboratory security, safety and safeguards and psychological evaluations	20
Introducing alternatives to radioactive material	20
CBRN weapons use scenarios	21
Chemical: explosion of sodium cyanide containers in a port	21
Biological: ricin poisoning at a music festival	22
Radiological: detonation of an RDD in a busy city centre	23
Nuclear: detonation of an improvised nuclear device in a heavily populated city	24
Conclusion	25
References	27

Executive summary

Lloyd's commissioned Chatham House to investigate the potential for chemical, biological, radiological and nuclear (CBRN) weapons use by non-state actors, in order to improve understanding of the nature of this threat. Lloyd's believes that greater understanding of these issues can be important for developing robust exposure management and underwriting strategies.

CBRN weapons are some of the most indiscriminate and deadly weapons in existence today. Given the potential deadliness and costliness of even a single CBRN attack, and the relative ease with which malicious actors could obtain many of the materials and know-how required to build CBRN weapons, it is important to assess the current global threat of use of these weapons in light of society's resilience and vulnerabilities, and emerging technologies.

This report, produced for Lloyd's by Chatham House – an independent policy institute based in London – explores some of the key factors driving the global threat of CBRN attacks as an act of terrorism or sabotage. The report also presents a set of plausible but extreme scenarios for each form of attack. These are devised to be illustrative of the types of events that insurers may want to consider in their exposure management and underwriting strategies. The scenarios are not predictions, but they could provide a useful tool to assist insurers in thinking about CBRN weapons use.

The report indicates that the global threat of CBRN weapons use is evolving, driven by three strategic trends:

1. **Potential perpetrators** – CBRN weapons could be used by terrorist organisations, saboteurs or lone actors, and there is growing evidence suggesting that terrorist groups have the intention of acquiring such weapons.

2. **Technological and scientific capabilities** – cyber techniques with the capacity to sabotage or severely damage chemical or nuclear facilities are becoming more refined, while scientific advances are increasing capabilities to synthesise deadly viruses.

3. **Dual-use materials** – a wide range of materials with the potential to be used in CBRN weapons can also be used for civilian purposes, with many easily purchased online or from high street retailers.

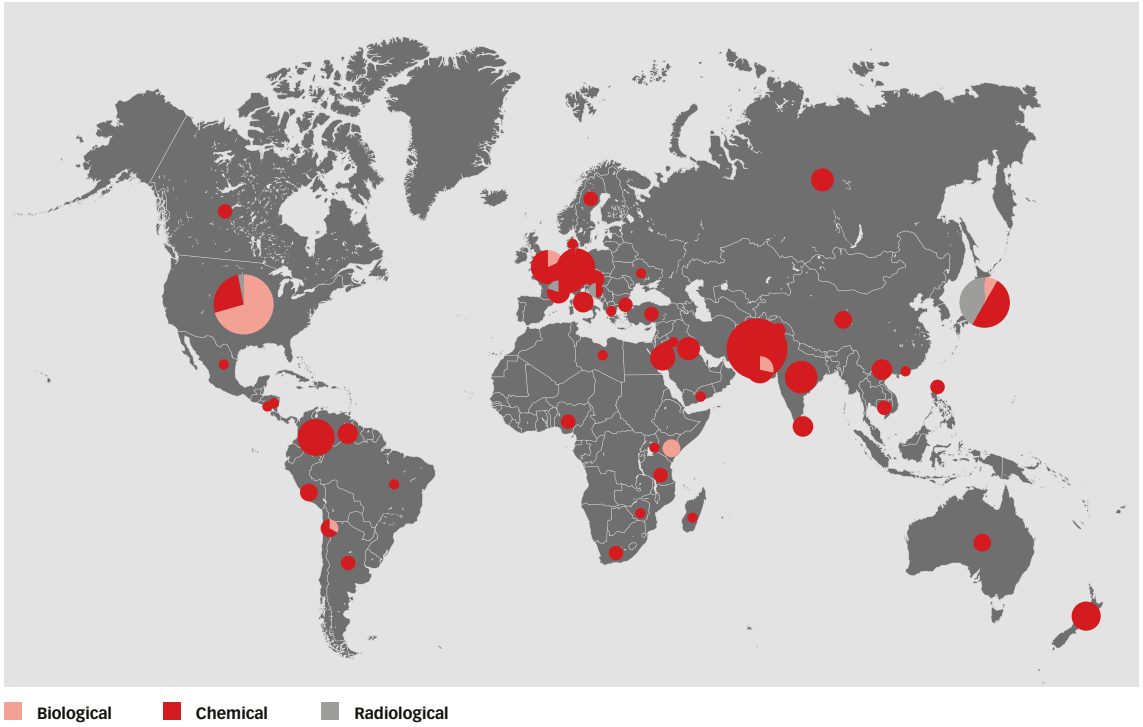
Today's heightened terrorist and saboteur threat, combined with the significant potential for CBRN weapons to cause widespread disruption and fear, could increase the likelihood of these weapons being used by malicious actors. Despite this, there have been relatively few large- or even medium-scale incidents of CBRN terrorism or sabotage in the 20th and 21st centuries. The probability and nature of this threat varies geographically, and is linked to the capabilities, intentions, (dis)incentives for use and the consequences of use for a potential perpetrator.

Emerging technologies are altering the risk landscape for CBRN weapons use in a variety of ways. Technological developments – including those in nanotechnology, synthetic biology and chemicals, cyber technology and 3D printing – could enable hostile actors to develop weapons that are cheaper, more powerful and easier to use. However, these same advances also have the potential to enhance detection, and reduce the destructive and disruptive capacity of CBRN weapons.

Although CBRN attacks are rare, the threat is dynamic, and effective risk management requires co-operation, vigilance and innovation. Governments and industries can increase resilience to attacks by strengthening existing security measures – particularly around chemical facilities and critical infrastructure – ensuring laboratory security, safety and safeguards, and introducing alternatives to radioactive materials in non-military locations such as hospitals.

Introduction

Figure 1: Chemical, biological and radiological attacks across the world from 1970 to 2014



According to the University of Maryland's Global Terrorism Database, there were a total of 143 attacks – 35 biological, 95 chemical, and 13 radiological – using CBRN weapons across the world from 1970 to 2014. This information is captured in figure 1.[a]

Insurance is available to cover some of the effects of the use of chemical, biological, radiological and nuclear (CBRN) weapons by non-state actors. With this in mind, Lloyd's commissioned this study by Chatham House with a view to providing a forward-looking assessment of the global threat relating to the use of these weapons. The report includes scenarios which are designed to be representative of plausible but extreme occurrences for the use of each weapon type. These scenarios were devised by Chatham House to be illustrative of the types of events that insurers may want to consider in their exposure management and underwriting strategies. Lloyd's hopes that, by providing an up-to-date, balanced assessment of the present risk, this report will help inform exposure management and product innovation in the insurance industry.

CBRN weapons are some of the most indiscriminate and deadly weapons in existence today. Besides the physical damage they can inflict, they also have the potential to inspire fear, provoke panic, and cause significant economic and societal disruption.[3] Fortunately, the use of CBRN weapons by states and non-state actors has remained relatively rare to date. Nevertheless, the risk presented by these weapons is not zero, and insurers may benefit from understanding the exposure of their portfolios to plausible but extreme events of their use.

A key incentive for use of CBRN weapons is their capacity to cause significant disruption across sectors, as well as considerable revenue loss for governments. In particular, cleaning up after a CBRN incident could require that people, buildings, infrastructure and the environment undergo a cost intensive and lengthy decontamination process. For instance, the cost of decontamination after the 2001 anthrax attacks in the US, which produced almost 3,000 tonnes of contaminated waste, is estimated to have been around $800m.[4]

[a] The Global Terrorism Database[1] is modified for terrorist organisations, and saboteur groups use of chemical, biological and radiological weapons. This dataset includes attempted CBRN attacks. In addition to this database, the Center for Nonproliferation Studies has WMD Terrorism Databases.[2]

Through a series of multilateral treaties and compliance measures, almost all states worldwide have prohibited the use and possession of chemical[b] and biological[c] weapons. There also exist treaties and other legal instruments, monitoring organisations, and verification and safeguarding procedures aimed at preventing the transfer, loss or theft of nuclear weapons, materials and technologies. These measures also cover radiological materials which could be used in a 'dirty bomb'. The Chemical Weapons Convention (CWC) incorporates a general clause prohibiting the weaponisation of all chemicals, and the Biological Weapons Convention (BWC) similarly bestows a prohibition on the weaponisation of biological pathogens and agents. Regardless of the international treaties and norms established around non-use, CBRN materials still pose a significant threat to safety and security.

Many of the chemicals that can be used as a weapon are dual-use, meaning that they can be used for both civilian and military purposes. Similarly, many biological agents and toxins that could potentially be weaponised are accessible for both civilian and military research. Given their relative availability, it is highly unlikely that societies could ever completely eliminate vulnerability to these agents.[5] The BWC does not have a verification mechanism for monitoring global sources of dangerous pathogens,[6] but focuses its efforts instead on voluntary confidence-building measures. To date, the destruction of bioweapon stocks has been undertaken unilaterally by states rather than under the auspices of the BWC. In spite of security and safety measures, loss and theft of radioactive materials remains a threat.[7]

Given the potential deadliness and costliness of even a single CBRN attack, and the relative ease with which malicious actors could obtain many of the materials and know-how required to build CBRN weapons, valuable insights can be gained by assessing the current global threat of use of these weapons in light of society's resilience and vulnerabilities, and emerging technologies.

This report explores some of the key factors driving the global threat of CBRN attacks as an act of terrorism or sabotage, and presents a set of plausible but extreme scenarios for specific forms of attack. In order to assess the global threat of CBRN attacks, this report presents actual cases that have been detailed in open sources and the University of Maryland's Global Terrorism Database.[1]

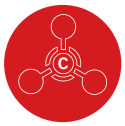
The likelihood of CBRN use is defined according to the extent to which terrorist organisations and saboteur groups may be able to obtain these materials, as well as the financial costs of researching, producing, buying or sustaining these materials as weapons. The CBRN threat from terrorist and saboteur groups is bound to several factors: capabilities, intentions, incentives and disincentives for acquisition, and consequences and impact of use of unconventional means in an attack.

This report does not cover the threat of CBRN weapons use among or between states, despite the fact that – at least in the case of nuclear weapons – such risks may be far greater.

[b] *As of 11 August 2015, Israel has signed but not ratified and the CWC. As of February 2015, Angola, Egypt, North Korea and South Sudan have neither signed nor ratified the CWC.*

[c] *Angola, Egypt, North Korea and South Sudan neither signed nor ratified the BWC. Central African Republic, Côte d'Ivoire, Egypt, Haiti, Liberia, Nepal, Somalia, Syrian Arab Republic, and the United Republic of Tanzania have signed but not ratified the BWC.*

What are chemical, biological, radiological and nuclear weapons?



Chemical weapons

The Organisation for the Prohibition of Chemical Weapons (OPCW) defines chemical weapons as any toxic chemical or its precursor that can cause death, injury, temporary incapacitation or sensory irritation through its chemical action, and includes related munitions and delivery systems.[8] Chemical agents are more broadly categorised according to their effects on the human body. Some of the most well-known categories are: nerve agents, such as sarin and VX; blood agents, such as hydrogen cyanide; blister agents, such as sulphur mustard and other mustard agents; choking agents, such as phosgene; and irritants, such as tear gas. Skin exposure to some agents may cause blistering, while other agents will cause lung damage if inhaled. Others will maim and kill in significant doses. Chlorine, mustard gas and sarin are among the most well-known and regularly used weaponised chemicals.[9]



Biological weapons

Biological weapons, also referred to as bioweapons, are deadly pathogens – bacteria, microorganisms or viruses – or toxins which can be deliberately released in order to inflict harm.[10] Biological weapons can be disseminated through inhalation, ingestion or skin absorption. Unlike chemical agents, biological agents can be grown from a tiny initial supply.[5] The suitability of different pathogens and toxins for use as bioweapons depends on the motivation of the user; some biological agents might be better suited to affecting large numbers of people, such as the highly contagious severe acute respiratory syndrome (SARS) virus, while others, such as Ebola, might be less contagious but more deadly for those they affect.



Radiological weapons

Radiological weapons disperse radioactive material using conventional methods, which may include an improvised explosive device. This is called a radiological dispersal device (RDD) – more commonly known as a 'dirty bomb'. While the majority of immediate fatalities in such an attack would be likely to be caused by the explosion itself rather than the levels of radiation, the exposure of people and the environment to radioactive contamination would cause massive disruption and have a severe psychological impact on those affected. Another radiological threat relates to the vulnerability of nuclear power plants to acts of sabotage or terrorist attacks.[d]



Nuclear weapons

Nuclear weapons rely on nuclear energy produced by either fission or a combination of fission and fusion of atomic nuclei. Nuclear weapons have not been detonated in armed conflict since 1945, and most concerns today tend to centre on states selling a nuclear weapon to terrorist organisations, or the security of highly radioactive nuclear material (uranium and plutonium) that could be stolen for use in an improvised nuclear device (IND).

[d] A nuclear military complex in Pakistan has suffered three separate attacks by militants, including suicide bombings.[11]

Strategic trends in the CBRN threat

CBRN capabilities encompass factors relating to the accessibility of agents, substances and materials needed for CBRN weapons, and the ability to deploy and use these weapons effectively. Easy access to these resources increases the likelihood of threat. Industrial and agricultural toxic chemicals can be purchased relatively cheaply and easily in most parts of the world. Chlorine, for instance, has a multitude of industrial uses, and can be easier to acquire than other weapons.[12] Other materials and agents can be accessed on the black market, and increasingly on the so-called 'dark web'.[e]

How real is the CBRN threat?

The impact of CBRN weapons can be enormous, involving not just the loss of human life but also considerable economic losses and longer-term psychological effects on the individuals and populations involved. As knowledge diffuses rapidly to different parts of the world through the globalisation of information and communications technology, a growing concern is that CBRN weapons could be used even more easily by terrorist organisations and saboteurs in the future. Increasing mobility of people has added to this complexity. The fact that CBRN weapons have been used in the past in almost all parts of the world is indicative of a real threat. States with scientists and engineers with practical knowledge of CBRN materials or states experiencing domestic or international turmoil are considered to pose the greatest security threat. In such conditions, hazardous materials could fall into the hands of terrorist groups or saboteurs for use in urban areas or near critical infrastructure, which could impair and impact global economy and security.

There are three key strategic trends affecting the global threat of CBRN weapons use: potential perpetrators, technological and scientific capabilities, and dual-use materials.

1. **Potential Perpetrators**
Terrorist organisations, saboteur groups or lone actors could use CBRN weapons, and some evidence suggests that terrorist groups have the intention to acquire them. In September 2006, the leader of al-Qaeda in Iraq released a statement inviting followers to gain knowledge of "unconventional bombs – especially the so-called germ or dirty variety".[15] There are also allegations that Islamic State (IS) has already used chemical weapons, including mustard gas, against civilians in Iraq and Syria.[16,17] This presents a further challenge, in that so-called 'foreign fighters'[f] engaged in conflict zones may bring this type of knowledge and experience from the battlefield to the streets of North American and Western European capitals. UK Prime Minister David Cameron has already expressed concern that British-born fighters in Syria could return to the UK and carry out terrorist attacks.[19] Experts applying quantitative analysis have found that organisations embedded in alliance structures and in authoritarian countries with strong links to a globalised world are more likely to seek to develop or acquire CBRN materials.[20]

With regard to sabotage or lone actors, the possibility of 'insiders' using their position, expertise and knowledge of biological and chemical agents, or even of the security of nuclear facilities, should not be understated in a CBRN threat assessment. This is particularly highlighted in light of Able Seaman William McNeilly's recent disclosures regarding the flaws in the safety and security systems in UK Trident submarines.[21] The European Commission has acknowledged the lack of measures to mitigate the 'insider' threat, and proposed that efforts should be made to improve the security vetting of personnel by examining the best practices of background checks.[22]

[e] In 2014, Kuntal Patel was convicted of purchasing abrin on the 'dark web' from a US-based dealer under section 1 of the UK Biological Weapons Act 1974.[13] In July 2015, a man was convicted of attempting to purchase 500mg of ricin – a bio-toxin derived from castor beans – online from an undercover FBI agent posing as a retailer.[14]

[f] Foreign fighters are individuals who fight in conflicts outside their home country.[18]

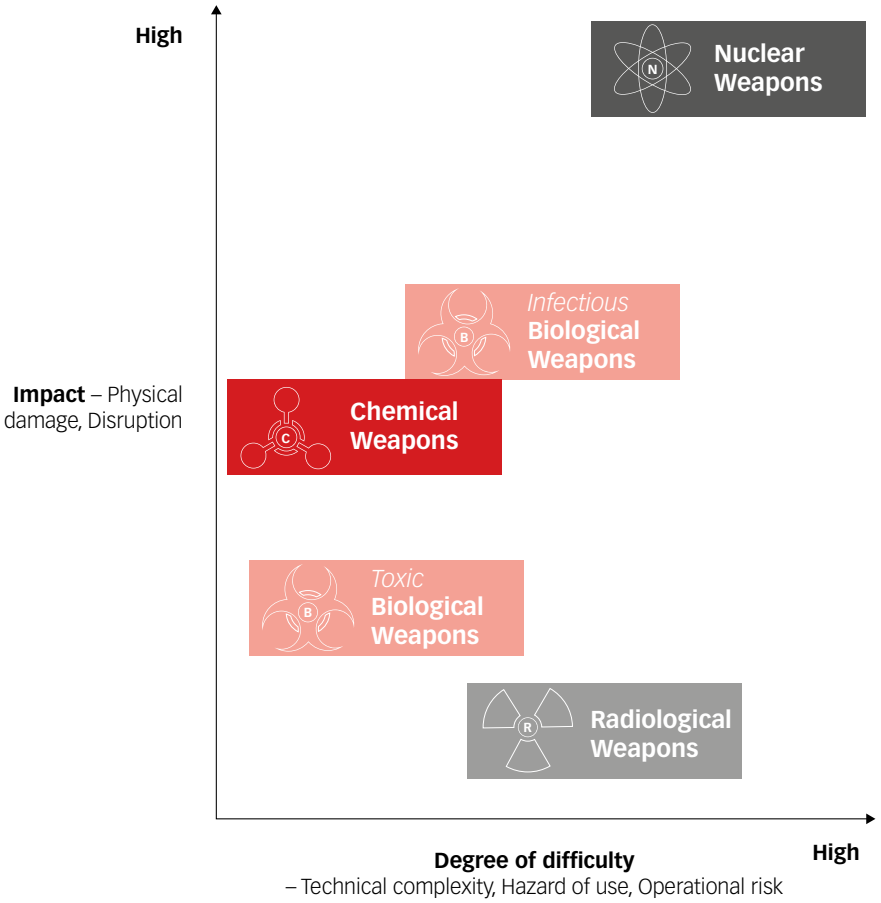
2 **Technological and scientific capabilities**
Certain emerging technologies and scientific advances could also be a cause for concern in the context of CBRN threats. In light of state-sponsored cyber attacks against critical infrastructure – such as the Stuxnet virus, which targeted the Iranian Natanz nuclear research facility in 2010 [g] – it is apparent that cyber techniques with a capacity to sabotage or severely damage chemical or nuclear facilities are becoming more refined. As a result, the likelihood that vulnerabilities at sites such as these could be exploited has escalated. Increasingly sophisticated improvised delivery systems and modified weaponry could also increase the CBRN threat. Advances in scientific knowledge now mean that deadly viruses such as polio and Ebola can be synthesised using public databases and available technology.[24] Nanotechnology, 3D printing and robotics are other areas of concern. As NATO Deputy Assistant Secretary General for Emerging Security Challenges Jamie Shea highlights: "We could live in a future in which anyone could be targeted, anywhere, and at any time." [25]

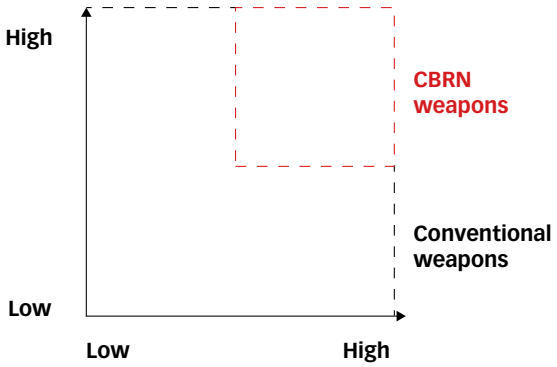
3 **Dual-use materials**
Dual-use agents and materials – those which can be used for civilian as well as military purposes – represent a perennial challenge to those attempting to reduce the likelihood of or build resilience to CBRN attack. Until recently, it was legal in many Western countries to purchase and use certain pesticides containing chemicals that have a similar effect on humans to nerve agents. When procured in sufficiently large quantities, solvents used in ballpoint pen ink can be converted into mustard gas.[26] Many other potentially lethal chemicals can be purchased with relative ease online or from high street retailers. Legal, as opposed to illicit, acquisition of dual-use materials and agents could therefore be a catalyst in CBRN weapons procurement and use.

[g] *Stuxnet is a state plotted computer virus that delayed a fifth of Iran's nuclear centrifuges.*

CBRN threat matrix

There is arguably no such thing as a 'low-impact' CBRN attack. Even one which results in limited casualties and physical damage would arguably generate significant disruption through widespread fear and uncertainty. To introduce the threat attached to each weapon type, the matrix below provides a representation of the incentives for use (scale of achievable impact) and disincentives for use (degree of difficulty for a non-state group) for each weapon type. CBRN occupies the upper-right quadrant of impact and difficulty when compared with conventional weapons used by non-state actors – principally firearms and explosives. The threat profile for each type of weapon is described in more detail in the following section.

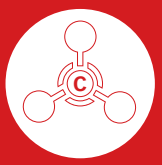




CBRN threats: capability and intent

The scale of impact that can be achieved through the use of CBRN weapons is likely to make them appealing to non-state actors seeking to achieve strategic effect. This has prompted experts to ask why there have been relatively few large- or even medium-scale incidents of CBRN terrorism or sabotage in the 20th and 21st centuries.

This section examines why this may be the case, assessing the incentives and disincentives for CBRN weapons acquisition and use, and the factors affecting the probability of their use by terrorists or saboteurs.



Chemical weapons

1A

One of the most devastating and well-known chemical attacks committed by non-state actors occurred on 20 March 1995 in Tokyo, Japan, when members of the Aum Shinrikyo cult punctured plastic bags containing sarin with an umbrella on the city's busy subway.[27] The attack killed 12 people and injured 3,800 others.[28] From 1990 to 1995, Aum Shinrikyo was also responsible for 17 known attacks with chemical and biological weapons (including botulinum toxin and anthrax)[29] as it attempted assassinations and mass murder.[30]

1B[31]

Nerve Agents
- Highly lethal and fast acting
- Pre- and post-countermeasures exist; post-countermeasures must be taken almost immediately upon exposure
- Challenging to synthesise outside equipped laboratories

Blister agents
- Less lethal unless mixed with systemic poisons such as an arsenic
- Symptoms may not develop immediately
- Only supportive and symptom treatment is possible

Choking agents
- Moderately lethal, highly dependent on concentration
- Some countermeasures available but in some cases treatment is just respiratory support
- Quite simple chemicals, often industrially available

Poisons
- Some chemicals with a relatively low toxicity threshold are publicly available, such as agricultural pesticides
- Generally require consumption or injection to be effective, therefore difficult to use to generate mass casualty effect
- Usually handled well by national poison centres

Riot control agents[32]
- Designed to incapacitate, but may cause death under certain circumstances
- Availability varies by country; sometimes carried as a personal security device
- Effects can be confused with those of more lethal chemicals

Chemical weapons were used or attempts were made to use them a recorded total of 217 times worldwide between 1970 and 2014.[1] The frequency of chemical weapons use has varied throughout history, but global chemical weapons use by non-state actors has been on the rise since 2012.[1]

Even as the CWC halted chemical weapons programmes when it came into force in 1997, scientists and technicians from countries that have had chemical weapons programmes could potentially be hired, coerced or duped into lending their expertise to a terrorist organisation.[33] Many chemical agents with a potential for weaponisation are currently produced at commercial facilities, and are therefore dual-use. Furthermore, although chemicals specified in the CWC are strictly monitored, many states possess the precursor agents. Open source information which details the process of weaponising deadly chemicals is also freely available online.

Terrorist and saboteur threats
The heightened terrorist and saboteur threat in the world today arguably increases the likelihood of chemical weapons use by malicious actors. Countries experiencing political or social instability, and which possess chemical weapons programmes (such as Syria) or have in the past (such as Iraq), run the risk of hazardous precursor agents or chemical weapons themselves falling into the wrong hands.[h] There are a number of instances online of lone actors discussing easy ways to make chemical explosives using only over-the-counter chemicals, explaining in detail the processes to compose chemical agents and even make fertilisers at home.[35] Additionally, an orchestrated explosion or act of sabotage at facilities producing toxic chemicals in large quantities could potentially cause significant damage to both human life and the environment.

Probability of use
Chemical weapons, characterised as the 'poor man's atomic bomb',[36] are cheap and relatively easy to acquire. Around the world, chemical agents continue to be used on a regular basis in the form of acid attacks, which permanently disfigure or blind between 1,000 and 1,500 people (predominantly women and children) each year.[37,38] Extremists in the US have already been convicted of stockpiling deadly chemical agents.[i]

In terms of potential terrorist use, VX and other nerve agents are low-probability but high-impact agents, meaning that while there is difficulty in obtaining the chemicals, their use could potentially be catastrophic. Side effects depend on the level of toxicity of agents. Conversely, chlorine has a high probability of use but is considered a low-impact agent, meaning that although it is easy to obtain it is not as deadly as other agents. The duration and location of exposure is fundamental for examining impact. In Syria, although the use of chlorine as a chemical weapon has been confirmed, conventional explosives and improvised explosive devices such as barrel bombs have caused far more devastation. Nevertheless, the green smoke emitted by chlorine does have its own psychological impact and chemical weapons use helps to mobilise the international community into action.

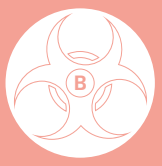
(Dis)incentives for acquisition and use
Incentives to acquire or use chemical weapons rest on the motivation of the actors involved. One incentive for acquisition is that often only a small amount of a chemical agent is needed to inflict considerable harm. Some chemical agents, such as sarin or VX, are certainly highly lethal even in small concentrations when weaponised. Additionally, most agents do not have to be stored in the form of a weapon, and can therefore also be handled relatively safely. The relative benefit of using chemical weapons to cause massive disruption, as opposed to inflicting large numbers of casualties, could also provide an incentive to those wanting to commit economic disruption or create a climate of fear.

Much depends on how and where chemical weapons are released: most chemical agents tend to diffuse rapidly in open areas, and their effectiveness therefore diminishes reasonably quickly after release. Gaseous chemical weapons are far more lethal if released into sealed enclosed spaces from which there is restricted or no escape, such as homes and schools.

Geographical locations
Recent incidents of non-state armed groups using chemical weapons, in addition to state use, indicate there is high risk of use in conflict-prone areas in the world, such as Syria and Iraq. Especially in light of the coordinated terrorist attacks carried out in Paris in November 2015, Europe is now considered vulnerable to terrorist attacks. Analysts have argued that there is a very real risk of IS using chemical weapons in Europe and beyond.[40]

[h] In February 2015, Indonesian police linked militants returning from Syria to a failed attempt at detonating a chlorine bomb in a Jakarta shopping centre.[34]

[i] In 2004, Texan authorities raided storage units rented by William Krar and Judith Bruey, and found –among white-supremacist literature, 500,000 rounds of ammunition, and dozens of guns, bombs and silencers – almost 1kg of deadly chemicals (including a cyanide compound).[39]



Biological weapons

2A

Seven days after the attacks on the World Trade Center in September 2001, anonymous letters laced with deadly anthrax spores were sent to the offices of several news media companies and two Democratic US Senators. Over the following months, five people were killed and 17 others infected as a result of inhaling the pathogen. An investigation into the attack by the FBI spanned eight years, eventually identifying a lone army scientist as the likely perpetrator.[41,42]

2B[43]

Toxic biological weapons

- Potentially available in the environment but extraction can be difficult
- May not be environmentally stable – may have low persistency and be difficult to disseminate effectively
- Most effective when administered like a poison
- Toxicity varies by agent, but some are among the most lethal substances
- Only supportive care is available in most cases

Examples: ricin, SEB (staphylococcal enterotoxin B), botulinum, trichothecene

Infectious biological weapons

- Potentially available in the environment but selection, culturing and weaponisation are challenging
- Difficult to control spread and ensure infectivity
- Infectivity and morbidity vary widely
- Some vaccines and treatments are available

Examples: E. Coli, monkeypox, brucellosis

Most common example: anthrax[44]

- Low infectivity
- Can be spread by close contact (rare), or through ingestion or injection (quite common)
- Can be encouraged to form a spore which makes it very stable and suitable for dispersion and infection by inhalation
- Disease may take time to develop as the spore remains dormant; exposed population may therefore require extensive antibiotic treatment (90 days or more)
- Vaccines and post-exposure treatments are available
- Untreated inhalational exposure is highly lethal

Countries without adequate health services are most vulnerable to the impacts of biological weapons due to the difficulty of administering effective treatments such as antibiotics early, and putting effective preventative measures such as vaccines into place. Depending on the resilience of the bio-agent, cleaning up an affected area can take more than a year and is likely to be extremely costly. Biosafety programmes, such as BSL-4 facilities, are also vulnerable to intrusion, and there is no formal verification and compliance system established within the BWC to prevent states selling bio-agents to terrorist groups.[45]

Terrorist and saboteur threats
During the Cold War, scientists in the Soviet Union and the US had converted at least eight extremely high-risk bio-agents into 'military grade weapons' as part of their former bioweapons programmes. Many of the scientists and researchers previously employed in these military labs could be coerced, duped or convinced to use their expertise to develop a bioweapon to be used in an act of terrorism or sabotage, or could do so as part of a lone actor attack.[j]

Terrorist groups have previously shown interest in acquiring biological weapons. For instance, al-Qaeda has attempted to recruit members holding PhDs in biological fields possibly in order to achieve this goal. In the late 1990s, one such recruit wrote to Ayman al-Zawahiri – now the group's leader – about a visit he had made to a biosafety level 3 (BSL-3) laboratory in the UK, demonstrating in the letter an eagerness to obtain pathogens and anthrax vaccines on behalf of al-Qaeda.[47]

Probability of use
The relative ease with which biological weapons can be acquired and disseminated, as well as the resilience of specific pathogens to medical treatments (including vaccines), and ultimately the capacity of these pathogens to cause widespread death and disruption, are all factors which determine the probability of biological weapons use. Multiple pathways exist for those attempting to acquire pathogens that can be used as biological weapons, such as theft from laboratories and culture banks, and even natural sources. Identification of these sources is also becoming easier, as locations of both outbreaks and laboratory sources for pathogens are freely available on the internet.[48]

(Dis)incentives for acquisition and use
As with chemical weapons, terrorists or saboteurs could be drawn to use bioweapons because of their potential to cause mass disruption and anxiety, as well as their more distinctive 'shock effect'.[35] Bioweapons use could be made to resemble natural pandemics[49] or – as part of a coordinated attack – be used to engineer a global crisis. Developing a small-scale bioweapon facility could be achieved at relatively low cost; one estimate has placed this cost at between $10,000 and $100,000.[50] Even a small-scale facility could allow large-scale production.[51]

Most biological agents have an incubation period, which allows perpetrators to conduct simultaneous deliberate attacks without alarming officials. It is also difficult to differentiate between naturally occurring pandemics and those resulting from biological weapons use. This could provide an incentive for non-terrorist actors and lone actors, unconcerned with political goals or notoriety, to use certain biological weapons as a way of committing mass murder or inflicting considerable economic damage while reducing the chance of being caught.

Nevertheless, there are numerous disincentives for the acquisition and use of biological weapons. Unless they are able to source biological agents from high-security research facilities, saboteurs or terrorist groups would require a scientist or at least an expert with the scientific knowledge and laboratory access necessary to create a virus or bacteria that could be successfully weaponised. Finding an effective means of dissemination could also be problematic.

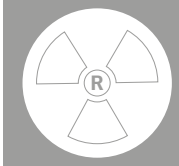
Most biological agents cannot survive at extreme temperatures or levels of humidity, and the decontamination process is straightforward in many cases.[k] Even if the difficult task of cultivating resilient deadly pathogens is overcome, producing them in a manner so as to harm large numbers of people would be technically more difficult.[10] Biological agents are indiscriminate, and cannot be easily contained once released. Terrorists who intend to maim or kill in order to achieve specific political goals are unlikely to use these weapons due to the difficulty of deploying them against specific targets without putting themselves at risk. While there is a possibility that pathogens could be synthesised in order to target only specific people – based on chromosomal gender, for example – the technical capacity to do so in the foreseeable future is very low, especially outside advanced laboratories under government control.

Geographical locations
Distinguishing between a biological weapon attack and a naturally occurring pandemic could be difficult unless it is established early on that the pathogen is alien to the outbreak location. Tropical virus outbreaks in a moderate climate, for instance, would likely be more straightforward to identify, whereas a carefully timed flu pandemic – adhering to established pandemic cycles – could go undetected for a considerable time. The geography of an outbreak is therefore crucial for identifying deliberate use.

Laboratories with a biological safety level of 4 (BSL-4) that deal with exotic and dangerous agents (such as Ebola, Marburg and others) exist in over 20 countries.[52] These facilities are used predominantly for researching virus species, tracing transmission routes and developing vaccines.[53] It is feasible that such laboratories in countries experiencing upheaval could change their focus to weaponisation in a short time frame.

[j] The FBI suspected that the 2001 anthrax attacks in the US (see box 2A) were perpetrated by a senior researcher at the United States Army Medical Research Institute of Infectious Diseases (USAMRIID).[46]

[k] One exception to all is anthrax.



Radiological weapons

3A

In April 2015, a truck carrying a container of iridium-192 – a highly radioactive material used in industrial radiography – was stolen in Tabasco, Mexico (although subsequently found).[54] Only one month earlier, 22 canisters of cobalt-60 – a chemical capable of causing burns and death in large enough quantities – each weighing between 45kg and 70kg were stolen from a warehouse in Poland and remain missing.[55]

3B[56]

- Some isotopes are accessible but are generally controlled
- Difficult to cause death without high exposure or ingestion
- Can injure through either external or internal irradiation of subject
- Non-lethal exposure may increase lifetime risk of cancer
- Some treatments to handle systemic poisoning and speed up biological half-life are available

Examples: radiological dispersal device; inhalation, ingestion and exposure attacks

One tangible source of risk today relates to the theft or illicit trafficking of radioactive materials and substances. From 1993 to 2013, the International Atomic Energy Agency's (IAEA) Incident and Trafficking Database (ITDB) documents that a total of 2,477 incidents – illicit trafficking and other unauthorised activities and events involving nuclear and radioactive materials outside regulatory control – were reported to it.[57] Sixteen of these activities involved radioactive materials: highly enriched uranium (HEU) or plutonium.

Terrorist and saboteur threats
Terrorist groups have shown interest in radiological materials. Former al-Qaeda operative Jamal Ahmed al-Fadl claimed during his 2001 trial for the 1998 bombings of US embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, that the group tasked him with purchasing uranium from a contact in Sudan, in 1993, for the sum of $1.5m.[58]

Probability of use
Many potentially dangerous radioactive materials are dual-use and as such may not have adequate safety and security measures in place to protect them from theft or accidental loss. These radioactive materials are used both for civilian purposes – notably in hospitals, such as radiotherapy and radiography units – and in industry, such as oil exploration.[56] As such, there is a range of sources from which terrorist groups could acquire radioactive material due to inadequate safety and security measures. Caesium chloride, for instance, is used in hospitals but contains caesium-137, a radioactive isotope of caesium, and is potentially dangerous. High-risk radiation sources such as cobalt-60 or iridium-192 are also used for medical purposes.

From 1993 to 2008, more than 1,500 incidents of unauthorised activities, events, thefts or losses were reported to the IAEA; 65% of the losses were never recovered.[59] Another area of concern is theft through commercial use of radioactive materials, especially in private industries. Radioactive substances have high disposal costs for industries; commercial users may choose to dump radioactive materials instead of safely and securely disposing of them, thus potentially increasing the likelihood of theft. This also highlights that radiological materials are relatively accessible and that there are limits to the safety and security measures currently in place in various countries.

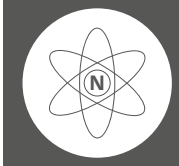
Using materials such as these in an RDD would require limited technical or scientific expertise. Identifying and securing possible theft pathways is an important step towards minimising the risks associated with radioactive materials, and in this context the US Nuclear Regulatory Commission (USNRC) is seeking to replace higher-risk materials with lower-risk ones.[60,61]

(Dis)incentives for acquisition and use
The clearest incentive for groups or individuals to procure radioactive materials for use as a weapon is that they are relatively easy to obtain from hospitals, industrial sources, environmental waste and research facilities. Terrorist groups could be tempted to use an RDD because of the relative ease with which necessary materials can be acquired. In addition, saboteurs could find the prospect of causing a very costly and time-consuming decontamination process appealing.

Radiological substances are also relatively easy to use, as weapons can be detonated using conventional explosives such as TNT, and can be placed at strategic points in a heavily populated city to ensure maximum exposure. Depending on the method of dispersal and conditions, including wind direction, these substances can remain hazardous for long periods of time and can cause significant anxiety as well as economic and political disruption. In this regard, the disruptive capacity of radioactive substances combined with their potential long-term health impacts can outweigh their immediate impact on human life.

Safety comprises a key disincentive for acquiring radioactive materials for use as a weapon – merely handling these materials safely before use in an RDD would be a challenge in itself. Depending on the material used, radiation type (if they are beta or gamma emitters), proximity to the material and length of exposure, these materials and substances could severely affect the health of those handling them, causing radiation sickness and even death.[62]

Geographical locations
There are examples of radioactive materials being smuggled into countries with high levels of corruption and prone to ethnic or regional conflict, such as Georgia and Moldova among many others (see box 4A). Porous borders and a lack of effective border control mechanisms increase the risk of radioactive materials being smuggled and for use in the future. A valuable preventive measure would therefore be to ensure transparency and information sharing among states, civil society organisations and research centres.[63] It is also possible that states do not always report incidents of theft and detection due to concerns about alarming the public.



Nuclear weapons

4A

In March 2010, two Armenians – a businessman and a physicist – pleaded guilty to smuggling HEU into Georgia by train, hiding the material in a lead-lined package.[64] In 2011, six people were arrested in Moldova for smuggling a stash of uranium-235 worth £18m into the country from Russia, with the intention of selling the uranium to a North African country.[65]

4B[66]

- Effective production for a non-state actor extremely difficult
- State weapons generally under secure guard
- Capable of causing significant injury and death, with an extreme and enduring public health impact
- Wide area of impact, with blast, thermal and radiation injuries; fallout may extend for many tens of kilometres

There are currently just under 16,000 nuclear warheads worldwide – this figure includes those deployed, stockpiled and retired.[67,68] Between the US and Russia, thousands of strategic weapons are on high-alert status.

Terrorist and saboteur threats
While it would arguably be extremely difficult for terrorists or saboteurs to acquire and successfully launch a nuclear weapon, a low-probability, high-impact event cannot be completely ruled out. Terrorists would also require the necessary hands-on practical information from knowledgeable nuclear technicians and perhaps even weapon scientists.[69] Non-state actors could perhaps obtain a nuclear warhead through theft or through bargaining with a state willing to sell a weapon. Unstable and impoverished states that are not bound by the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) regulations could pose higher risks for the latter category of acquisition.

Probability of use
Terrorists or saboteurs would require either a fully fabricated nuclear warhead or weapons-grade HEU and a fabricated improvised device to conduct a successful attack. A gun-type weapon of this sort is possible but technically very difficult to make. There have already been numerous documented cases of HEU and other highly radioactive material appearing on the black market.[70] For a nuclear explosion, however, uranium needs to be enriched to 80% or more. While it is unlikely that terrorist groups would get access to both the radioactive materials and the delivery mechanisms required for such an attack, it is not impossible. Another material used in nuclear weapons is plutonium. While all plutonium is explosive, whatever the isotope mix, plutonium cannot be used in simple gun-type design.[l] It is therefore considered very unlikely that it could be fabricated for use in an IND.

Possible acquisition pathways for terrorist groups to acquire nuclear materials or 'loose nukes' include theft from facilities, 'gifts' from states with shared ideological principles, or – as is most likely – from states willing to offer the materials for financial gain.

(Dis)incentives for acquisition and use
One clear incentive is that nuclear weapons are capable of causing significant damage to human life, the economy, the environment and society in a way that no other type of weapon can. The effect of nuclear weapons use would be expected to be far more disastrous than the conceivable effects of chemical, biological or radiological attacks.

There are, however, substantial practical barriers to using nuclear weapons. For instance, if a terrorist group were to obtain uranium, it would have to be at weapons-grade level. Unless they had enrichment capabilities to hand, low enriched uranium (LEU) and lower 20–80% HEU would be only useful as a 'dirty bomb'. In addition, the terrorist group would need to secure a means of making a bomb and delivering the explosive effectively. This would likely require scientific and engineering expertise and facilities that cannot be readily sourced, although it is not entirely impossible.

Acquisition from state sponsors also has its difficulties. Regardless of ideological sympathies, the few states that possess nuclear weapons – nine at present – may be unwilling to sell or give these weapons to a terrorist group due to the relative ease with which the attack could be traced back to them.[m]

Geographical locations
Some of the countries possessing HEU are in regions experiencing conflict, including countries such as Iran, Syria and Nigeria, among others.[72] Unstable states not party to the NPT could potentially sell or give some of their nuclear material or knowledge of constructing INDs to terrorist organisations.

[l] The rate of spontaneous fission for plutonium exceeds the assembly time for a gun-type bomb to reach critical mass. Thus, a plutonium bomb built in this manner would not be able to reach critical mass before a stray neutron from spontaneous fission prematurely ignited the plutonium.[71]

[m] Russia, US, France, China, Pakistan, UK, India, Israel and North Korea.[67]

Emerging technologies: threats and opportunities

Given the difficulties in using certain CBRN weapons, emerging technologies could be harnessed by terrorist groups seeking to develop CBRN weapons that are cheaper, more powerful and easier to use. At the same time, efforts are already being made to use these technologies to mitigate the use or effectiveness of CBRN weapons, and there are further opportunities to explore the potential benefits of these developments. These technologies can, for example, help in clean-up and detection, or simply in preserving the health and well-being of first responders. Similarly, technologies that can assist local law enforcement in identifying the nature of an attack and the kinds of chemical or biological agents used, for example, could make responding to an attack easier. In the process, these technologies could decrease the destructive and disruptive capacity of CBRN weapons, thus increasing disincentives for their use.

Nanotechnology

Nanotechnology refers to the creation and/or manipulation of materials at the nanometre (nm) scale,[73] with one nanometre measuring approximately one billionth of a metre.[74] Although this technology is relatively new, there have already been some breakthroughs in developing and improving new techniques in order to detect and mitigate the use of biological or chemical weapons. Decontamination of chemical agents, for instance, requires large volumes of water, and can produce waste which is harmful to both people and the environment.[75] By contrast, nanotechnology could be used in decontamination process even at room temperature, avoiding the need for thermal destruction, and could potentially be utilised to eliminate noxious vapours.[76] Developing better sensors for detecting the dispersal pattern of a chemical attack as it unfolds[77] or for decontamination efforts[78] could also present further opportunities to use nanotechnology to mitigate the effects of CBRN use.

Despite this technology being used for good, nanotechnology nevertheless presents certain longer-term risks. The technology could potentially be used to aid the dispersal and delivery process, or to conceal deadly pathogens. 'Proto-nano-weapons', such as dense inert metal explosives (DIME), have already been designed to make explosives less indiscriminate and more dangerous, miniaturising shrapnel to such an extent that medical professionals find it extremely difficult to treat the wounded.[79]

Synthetic biology and chemicals

Almost all states have the capacity to produce biological toxins that can be used as weapons.[80,81] The development of synthetic biological toxins, and the diffusion of knowledge and technology which would support their development, pose their own associated risks and opportunities.

Many types of pathogen, particularly those that thrive in tropical climates, can survive and propagate only in specific environments or conditions. Furthermore, the effects of many biological weapons can be difficult to contain once disseminated, and this could dissuade politically motivated terrorists from using them. Certain pathogens could in the future be modified so that they are able to thrive in new environments, or become more aggressive, selective or difficult to diagnose and treat.[82] There is a risk that information on the chemical synthesis of viruses such as polio could fall into the wrong hands,[83] and would-be attackers could use this information to tailor pathogens to their specific interests.

The dissemination of information on synthetic biology does theoretically make it easier for would-be terrorists to develop their own biological weapons, or even make existing pathogens deadlier through increasing their resistance to medical treatment. Nevertheless, the assumption that this trend will lead to more people without specialist training developing their own weapons in the short to medium term is considered unfounded at this time.[84,85]

Certain trends also highlight a growing capacity for the use of synthetic biology and chemicals for CBRN threat mitigation. Researchers are in the process of developing compounds capable of quickly neutralising the effects of some chemical agents used as weapons.[86] The development of new vaccinations and inoculations against deadly pathogens also remains a high government priority for countries including the UK;[87] these could be gradually rolled out at a national level in order to protect large populations, or targeted at those working in agencies that would be involved in first response, such as the military, police and fire departments, or health services. There are potential difficulties here, however. Between 2003 and 2008, the UK Armed Forces offered a vaccination against anthrax to its personnel deployed in Iraq. Among 5,302 of these personnel, 28% refused the vaccine for reasons ranging from concerns about it being voluntary, concerns about side effects and insufficient information about the vaccine, to the influence of colleagues and even fear of needles.[88] In this regard, if vaccination programmes were to be used effectively they would have to be made mandatory, or there would need to be improved information campaigns accompanying them. A mandatory programme of this kind could have negative psychological consequences, creating a climate of fear by implying that risks of negative side effects are worth taking due to the imminence of a biological attack.

Cyber technology
Research is already being conducted on the vulnerabilities of civil nuclear critical infrastructure to cyber attacks and attacks using drones.[89,90] Critical infrastructure related to chemical production could be just as vulnerable, such that attackers could potentially turn a chemical plant into a weapon of mass destruction.

The threat of cyber attacks targeting chemical or nuclear facilities is an everyday reality.[91,92] Given that chemical plants are now largely controlled using networked computers, it is possible in some countries that cyber attacks similar to Stuxnet targeting chemical plants by states or non-state actors could cause critical systems failure.[93] By hacking into the computer networks, an adversary could reprogram an industrial control system so that it commands the equipment to operate at unsafe speeds or the valves to open when they should remain closed.[94]

Drone technology
Information-gathering technologies could be used in the future to improve resilience through assisting first response efforts. Miniature unmanned aerial vehicles (UAVs) kitted with gamma probes and chemical sensors have now been specifically developed for use in counter-CBRN missions.[95] The use of swarms of drones in decontamination efforts could also be possible in the future as advances are made in UAV technology and in nanotechnology.[96] Indeed, UAV technology as demonstrated in natural disaster response efforts – together with the intelligence, surveillance and reconnaissance functions of UAVs[97] and other robotic technologies – opens up important avenues for identifying chemicals from a safe distance.[98]

On the other side of the spectrum, the recent flying of a drone with small traces of radiation into the office of Japanese Prime Minister Shinzo Abe[99] raises concerns that drones, even in their present form, could potentially be used in an assassination attempt or terrorist attack.

New detection technologies
The majority of casualties involved in a radiological attack would result from the blast rather than the radioactive material itself.[100] Despite this, most of the damage caused by the attack would be expected to result from the dispersal of radioactive material, which could make the affected area uninhabitable and create a sense of terror. Due to the nature of radiological weapons, many technologies being pursued today concern prevention rather than response. The Defense Threat Reduction Agency at the Pentagon has recently enlisted a technology company to develop new detection techniques that are more efficient and cost-effective than those currently available.[101,102] A more reliable system capable of detecting fissile materials with fewer false alarms was made available on the market at the end of 2014.[103] It was also reported in 2012 that, after research and testing at the Atomic Weapons Establishment,[104] the UK would be introducing systems capable of detecting 'disguised' or 'hidden' nuclear materials at air- and seaports, which would make it more difficult for individuals to smuggle material into the country.

3D printing
As with other developing technologies, the emergence of 3D printing technology brings dangers as well as opportunities to the area of CBRN weapons. 3D printing could be used in the future to help produce the more complex and reliable explosives and detonators needed for an RDD. As digital files can be transferred discreetly via email or flash drives, such digital manufacturing technologies could also make it much harder to detect the transfer of weapons systems. Furthermore, users would not require sophisticated technical expertise to manufacture this equipment; instead, they would potentially only need blueprints and the 3D printing equipment itself.

On a wider scale, states could exploit this technology in order to conduct arms sales more discreetly and engage with non-state actors without physical evidence. However, the cost of these blueprints would likely be expensive, and the risk that they could be caught and sanctioned could deter states from enabling terrorists to use this technology.

Similar to the opportunities provided with other cyber technology, 3D printing could potentially provide solutions for some of the complexities associated with the decontamination process. In the future, unmanned ground vehicles (UGVs) could be produced at a lower cost than at present and with a greater capacity for customisation based on specific challenges.[105] UGVs could ultimately make the task of CBRN decontamination easier and reduce the number of emergency personnel exposed to hazardous material. Forensic investigators could use the technology to trace explosives and ultimately identify the origin of such devices; the FBI has stated its intentions to use it for this purpose.[106]

Risk management and resilience

In addition to harnessing emerging technologies, there are several other ways in which governments and industries can increase resilience to CBRN attacks. An efficient first response unit can be integral to resilience; the remit of such a unit could include vaccination of the public, as well as access to stocks of medication in the event of an incident. Another component of resilience lies in organisational and institutional responsibility to observe the expiration date of prophylaxes. Furthermore, rapid identification of a CBRN agent or material could be expected to improve with the training of national and regional units on CBRN threats. Such training, especially if conducted through an international organisation, could enhance both national and regional capacity to respond to the CBRN threat by heightening awareness of and experience in identification, mitigation and containment procedures. Other resilience areas are a direct outcome of new technologies, and could be effective in their own right.

Increasing security

Strengthening export controls on dual-use materials at borders and ports, decreasing critical infrastructure vulnerability, and coordination and information sharing at regional and international levels through national CBRN teams could help to build a holistic resilience approach. Moreover, given that the potential consequences of a cyber attack on high-risk chemical facilities are so great, increasing cyber security at such facilities is a clear area in which resilience could be improved. For instance, a 2011 report for the US Department of Homeland Security warned against the move in industrial control systems from proprietary to open platforms, the latter being much more vulnerable to cyber attack.[107] Vulnerabilities such as these, which bring with them the danger that large quantities of deadly chemicals could be stolen, released, or even detonated as an act of sabotage or terrorism, support the argument that control systems in chemical facilities should be resilient to cyber attacks.

Ensuring laboratory security, safety and safeguards, and psychological evaluations

There are already safety and security measures in place globally which contribute to preventing accidental or intentional leaks of deadly pathogens from laboratories, but questions remain over how stringently they are adhered to and how to strengthen them. Previous incidents indicate that outbreaks of viruses from these laboratories can and do happen.[o] From 2009 to 2014, more than 100 accidents and 'near-misses' at high-security laboratories were reported to safety regulators in the UK.[109] Incidents of live anthrax being mistakenly sent between laboratories in both the UK and US [110] also highlight that accidents still happen, and can have potentially fatal consequences. A verification system, at least in BSL-4 laboratories, could diminish the risk of terrorist acquisition of biological agents.[111]

With these risks also comes the possibility of deliberate acts of sabotage or terrorism. A lone actor terrorist or even a disgruntled employee could, having worked inside a BSL-4 laboratory and having become acquainted with safety and security procedures, exploit existing vulnerabilities in order to smuggle out deadly pathogens. In the US, beyond standard measures related to personnel management and access control, there are no reasonable or tested and proven technical solutions available to protect biological materials from insider theft or inappropriate use.[112] Capacity-building measures, such as the ability to deploy mobile CBRN analytical laboratories in high-risk geographies such as Africa, could mitigate the risk in cases of a deliberate outbreak.

Introducing alternatives to radioactive material

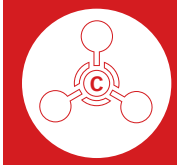
Given the continued risk that radioactive materials stolen from non-military locations with low levels of security (such as hospitals) could be used in a 'dirty bomb', replacing these materials with non-radioactive alternatives could decrease these risks as well as safeguarding the materials at their root source. Experts have suggested that caesium chloride, used in blood irradiation, is especially susceptible to theft by terrorists as it is easy to handle, and recommend that hospitals be given incentives to phase in alternatives.[61]

Nevertheless, some health suppliers and providers in the US have rejected such proposals because of their concerns about the reliability of alternatives and the high financial costs of introducing them.[113] Similar obstacles could be encountered if phasing in such a programme in the UK.

[o] Four outbreaks of SARS in China were associated with laboratories between July 2003 and June 2004 following the epidemic which had taken the lives of 800 people.[108]

CBRN weapons use scenarios

The following scenarios have been developed for Lloyd's by Chatham House to capture possible ways in which CBRN weapons could be used by non-state actors to inflict damage and cause disruption. The events described are considered plausible, and are of a type and scale that could have significant impacts on the global (re)insurance market, in addition to wider societal, economic and political consequences. As such, Lloyd's considers these scenarios to be representative of the sort of events that insurers may want to consider their exposure to.



Scenario 1

Chemical: explosion of sodium cyanide containers in a port

The following scenario involves the use of chemical agents detonated using conventional explosives. The explosion causes enormous environmental damage and economic loss. Sodium cyanide is a dual-use substance used in the gold mining industry, and is highly toxic. As a weapon, sodium cyanide can cause harm through inhalation, ingestion or contact with the skin. It can be diffused as a powder, solid or vapour. When used in large quantities, it can cause severe injury and death.

On a weekday in late summer, a marine transport worker affiliated to a well-funded terrorist organisation successfully detonates explosives at a very busy port, close to shipping containers containing 10 tonnes of sodium cyanide awaiting distribution for use in gold mining.

The explosion and subsequent fire damages two vessels in the area, one of which is a crude oil tanker. There is an oil leak from the tanker and the port is shut down for operation. A number of ships designated to arrive in the port are ordered to stay at their locations at sea until further notice. These delays cause a significant loss of domestic revenue, particularly as the port is an oil export hub.

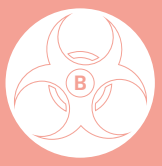
More than 30 people are killed and hundreds of others are injured by the explosions. Fire fighters struggle to control the oil fires. As professional units rush to clean up the site following the attack, toxic hydrogen cyanide gas is released in the air. The cause of this release is uncertain. The death toll increases in the affected area, mainly among professional units, since hydrogen cyanide has high toxicity and kills if a sufficient dose is inhaled.

Within an hour of the explosion, local hospitals are full to capacity with people reporting headaches, difficulty breathing, burns to the skin and nausea. In most cases, doctors cannot confirm exposure to cyanides quickly. Nevertheless, many people remain highly anxious that they may have been exposed and become convinced that they have been misdiagnosed. Emergency rooms are overwhelmed as more and more people come to hospitals in fear. As medical staff struggle to cope, many patients with genuine exposure rapidly begin to deteriorate.

Efficient and rapid triage following a chemical attack is not established in the country. First responder units are neither trained nor prepared for a disaster of this scale. Likewise, hospitals lack a cyanide antidote kit and are unable to manage this incident. The evacuation of the port city does not take place until the day after the incident; people up to 5km downwind of the port are exposed overnight due to the lack of sufficient protection.

Within the next few days, national CBRN units enter the site to dispose of the dangerous chemical. The global company shipping the sodium cyanide has decided to halt future shipments due to domestic pressure after it becomes clear that it has not fulfilled safety and security standards and measures. This has a serious impact on the company's annual revenue. Other companies in the exclusion zone are forced to suspend operations, creating widespread job insecurity. The disruption in exports pushes up the cost of oil globally as the delays are felt as shortages. Clean-up of the port and surrounding areas and insurance and subsequent reinsurance losses come at a substantial total cost.

Following the explosion, high levels of pollution remain at sandy beaches surrounding the port for several months, incurring costs to the tourism industry through loss of business. Large quantities of corals, marine species, birds and mammals perish; some populations do not recover for several years, resulting in significant financial losses for regional fishing and marine-culture businesses.



Scenario 2

Biological: ricin poisoning at a music festival

The following scenario relates to the use of ricin at a music festival. Ricin is derived from the castor bean, which is easily and cheaply purchased in large quantities. It can also be produced using the waste material generated in the processing of castor beans[114] – one million tonnes of which are generated every year.[115] Ricin works by preventing cells from producing protein, causing them to die. Those who manage to live for five days after first ingesting the ricin poison have a high likelihood of surviving. It was famously used in the 1978 assassination of the Bulgarian dissident Georgi Markov in London[116] and has been experimented with in various national bioweapon programmes.

At a two-day music festival attended by 25,000 people – mostly 18- to 35-year-olds – three separate food vendors serve food and drinks that have previously been laced with high concentrations of ricin. A total of 1,000 people eat and drink at these vendors' stalls by the end of the first day of the festival.

Many of these people begin to experience stomach cramping and vomiting within 12 hours of ingesting the poisoned food and drink, but misdiagnose their symptoms as those of gastroenteritis or a hangover. As these individuals consumed food and drink at different stalls, there are no immediate suspicions surrounding a particular vendor, food or drink.

Between 12 to 24 hours after ingesting ricin, symptoms worsen and are combined with dehydration and diarrhoea, but most of those affected still believe that they are suffering from acute gastroenteritis and, in any case, travel home as the festival ends.

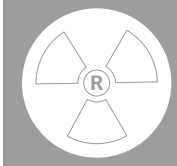
Two days after ingesting ricin, it becomes clear that hundreds have been poisoned either deliberately or accidently. Symptoms intensify as victims begin excreting blood in their urine and suffer hallucinations. Hospitals can only offer palliative care as there is no known antidote to ricin poisoning.

Hundreds of deaths are reported across the country on the second and third days, and autopsies are carried out to ascertain the cause of death. It is found that most have died of organ failure caused by ingesting ricin, and there is already speculation in the media that these deaths have been caused by deliberate poisoning. The media begin to link these cases to similar incidents in three further countries.

By 72 hours after first ingestion, 680 people have died and many others are in a critical condition, making this incident – the use of a biological agent as sabotage – the deadliest of its kind in the country's history. The vast scale of the incident becomes more apparent as a terrorist group claims responsibility for not only this attack but also three more in other countries, all in the same continent, which have additionally taken the lives of over 1,000 people and left hundreds of others critically ill. The terrorist group pledges to commit similar attacks in the future.

Police authorities make a number of arrests related to the incident, and begin coordinating their efforts with their counterparts in the three other countries affected. The government eventually makes a formal statement. However, people have already become panicked across the globe, concerned that government authorities are not divulging enough information about the extent of the incident or the risk of further attacks. Across the continent in the weeks that follow the poisoning, thousands of people begin to misdiagnose normal symptoms of gastroenteritis as the onset of poisoning, which places an increased burden on different national health systems. Many others begin stockpiling pre-packaged dried or canned goods and avoid eating anything prepared by others or susceptible to being poisoned. Panic ensues in the other affected countries as similar anxieties force people to present themselves at hospitals and clinics, worried that they have been poisoned.

In response, the government orders that increased security measures be taken at major catering firms across the country – measures that will come at a cost to the country's economy through lost revenues and disruption over the course of at least six weeks.



Scenario 3

Radiological: detonation of an RDD in a busy city centre

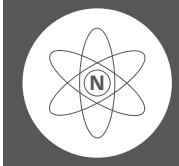
The following scenario considers the potential impact of an RDD being detonated in a busy city centre. The device featured in the scenario uses two radioactive substances: strontium-90 and caesium-137. Strontium-90 has a half-life of 29.1 years and is used in medical and agricultural research. Large amounts of strontium-90 were released as a result of the 1986 Chernobyl disaster. As a beta emitter, strontium-90 is primarily deposited in the bone and can in the long term lead to various forms of cancer. If it contaminates hard surfaces such as concrete, it can require abrasive treatment to be effectively removed.[118] It can be found in nuclear power plants, spent fuel and, it is speculated, in generators found in former-Soviet countries.[119,120] Caesium-137, a gamma emitter, has a half-life of 30 years[121] and is used for drilling and other industrial purposes. As a result of the 1987 Goiânia disaster, 249 people were contaminated with caesium-137, yet 112,000 people presented themselves at hospitals and clinics concerned with symptoms and had to be monitored.[117]

At 08.45, at the peak of rush-hour on a bright summer day, two truck bombs go off in the financial centre of a major capital city outside two different subway stations. The explosions kill 25 people instantly and injure dozens of others, some critically. Members of the public and first responders in the immediate area attempt to help those requiring urgent medical attention. As soon as police, fire and health services arrive at the scene, they begin cordoning off the blast locations and transporting the injured as per existing standard operating procedures governing the response to explosions.

By 10.00, the government is informed of the presence of high levels of strontium-90 and caesium-137 at both locations emanating from the explosion sites. These were picked up by detectors deployed for research purposes by the country's department of energy. After being informed of this, first responders immediately leave the vicinity of the explosions and await further instructions on how to proceed. In the meantime, they expand the cordoned-off area as a precaution. Later that day, a terrorist group claims responsibility and pledges that it has amassed sufficient stocks of radioactive material to commit more attacks in the coming weeks.

Decontamination measures are immediately put into place. The highest priority is given to those injured in the blast and others in the immediate vicinity. Clean-up is expected to be extremely costly. Strontium-90 will be especially difficult to get rid of, given that it is a beta emitter and therefore harder to trace than caesium-137, which is a gamma emitter. As the attack was designed to affect the busiest sections of the city, much of the city will be inaccessible for at least four to eight weeks as a precautionary measure.

This has a cumulative impact on the country, adversely affecting its tourism, commerce and industry. As the city centre remains out of bounds, offices in the capital remain closed and employees are forced to work from home for an extended period. As some of the busiest train, tube and bus routes are halted until further notice, the incident also has a severe impact on transportation. The psychological impact is also enormous: thousands of people now fear radiation poisoning, and will avoid travelling to the city and surrounding areas even after they have been completely decontaminated. Despite the clean-up being rigorous, public confidence remains low over fears that some of the radioactive contamination could have been missed.



Scenario 4

Nuclear: detonation of an improvised nuclear device in a heavily populated city

The following scenario considers the potential impact of a nuclear weapons explosion conducted by a terrorist group. As discussed in this report, this is considered a much more difficult attack for a non-state group to execute compared with the other weapons types, not least because of the scrutiny of intelligence and security agencies in countering the threat. Nevertheless, the risk is not zero. The following scenario is considered to be plausible but extremely unlikely.

With rising oil revenues and supporters, a group affiliated to an extremist terrorist group makes contact with a faction within a country that has nuclear weapons, in order to purchase a plutonium-based ready-made nuclear warhead plus the expertise to ensure its detonation. The warhead is shipped in a container vessel via intermediary traffickers and smuggled through port security,[123] after which it is loaded into a modified, highly secured truck and transported to a busy city.

At 14.00, on a weekday with a moderate southerly breeze, the terrorist group successfully detonates a nuclear warhead in a heavily populated city, causing a nuclear explosion.

People at the epicentre are vaporised in the enormous fireball of the nuclear explosion itself, which then forms the characteristic mushroom cloud. Seconds later, fatal doses of high-energy electromagnetic radiation are absorbed by large numbers of the surviving population, causing initial radiation exposure that will – if they survive subsequent fires and buildings collapse – cause them to suffer a slow death over a period of days from radiation poisoning. Within minutes, the intense thermal energy and overpressures caused by the explosion initiate uncontrollable firestorms across the city. Over a period of the next few weeks, the fallout from the mushroom cloud that contains highly toxic radioactive isotopes exposes many who survived the initial blast, initial radiation and firestorms to radiation that might kill them in the short or long term. It is estimated that, in the first 24 hours, there are at least 100,000 fatalities and more than 200,000 people in need of urgent treatment.[p] The fear factor is high: there is speculation about the possibility of a second attack, and survivors are horrified by the immense devastation. Satellite images of the area reveal large flows of people travelling away from the city centre. Some people head downwind, unaware of the radiation fallout in that area.

At least 85 schools and universities, 18 hospitals and medical facilities and two fire stations are destroyed in the explosion and subsequent firestorms. Nearby hospitals are not able to function at full capacity as their power supply is lost and their stocks of medicine have been contaminated. The explosion creates enormous craters and severely damages the roads leading to airports as people are trying to leave the city. People require immediate assistance for safe evacuation, yet first and second responders cannot get into the area without endangering their own lives. Volunteers without special protective gear or equipment help, but in doing so put themselves at severe risk.

Within a few days, survivors start to suffer from acute radiation poisoning symptoms such as hair loss, vomiting and exhaustion. Internally displaced persons (IDP) get sick from consuming contaminated food and water. Government officials together with humanitarian organisations start to build IDP camps, but cannot establish security in the camp area.

Health workers can do little but follow standard operating procedures. Radiation fallout becomes an increasing problem in the days following the explosion, and a long-term public health crisis is expected. Agricultural products are also contaminated and the World Health Organization advises that milk products should not be consumed. Due to lack of preparedness for a nuclear explosion, the humanitarian catastrophe cannot be prevented.

[p] *The estimated fatalities and injuries as well as the humanitarian impact are calculated using NukeMap.*[124]

Conclusion

Although there is a lower probability that nuclear weapons would be used as part of a terrorist attack than chemical, biological or radiological weapons, given the difficulties associated with obtaining the former, this type of attack could have catastrophic impacts for which there are currently no adequate response measures in place. The humanitarian impact of a nuclear detonation is also likely to be much higher than that of any other type of attack.

However, it is considered more likely that chemical weapons could be used in the future by terrorists or saboteurs, even though the impact would be less severe than that of nuclear weapons. Historical use of chemical weapons – especially agents such as chlorine – indicates that exposure to the most widely available chemical agents is not as deadly as is often assumed. In many cases, the explosion generated from an improvised delivery system would be much more lethal than the chemical agents themselves. Nevertheless, chemical weapons can cause enormous disruption, and the decontamination process – especially if chemical weapons are used in enclosed spaces such as subways – can be extremely costly depending on the nature and scale of the attack. An added complication is that although scientists may assess that decontamination is unnecessary or that decontamination has been successful, these assessments could undermine the confidence of the public, who continue to avoid the impacted area as a precaution.

An analysis of bioweapons use indicates that exposure to biological weapons can be lethal, and the insider threat in biosecurity laboratories remains a concern. Certain professions, such as deployed military forces, are considered to be at higher risk than others. A robust resilience measure for different types of agents and viruses could include large-scale vaccination campaigns for those working in high-risk professions.

The radiation released from an RDD could have long-term impacts, but radiological weapons are considered to have a low probability of use with low impact. The case analysis of the University of Maryland's database shows that radiological weapons have not historically caused severe damage to property.[1] Yet, it should be noted that the low number of incidents of use in the past cannot be taken as an indicator that the weapons will not be used in the future, particularly given the incentives to use radiological weapons, including the immense damage they can cause to an economy in the short-to-medium term.

The key to managing the risk of CBRN weapons use by non-state actors is to recognise that the threat is dynamic, not static: the relative rarity of past events means that historical trends may not provide reliable indicators on the current and future risk. The expertise and capacity to use chemical weapons on the battlefields of Syria and Iraq could be used to plan attacks outside these regional conflicts in the near future. In a similar vein, the dangers and opportunities presented by rapid technological developments – some of which are so revolutionary that they are not initially understood in policy-making, and therefore cannot be quickly accommodated through changes in the law or to resilience measures – may be worthy of more focused study in the field of CBRN threat assessment.

References

1. National Consortium for the Study of Terrorism and Responses to Terrorism (START), 2015. Global Terrorism Database [online]. Available at: http://www.start.umd.edu/gtd/
2. Center for Nonproliferation Studies (CNS), 2015. Monterey WMD Terrorism Database [online]. Available at: wmddb.miis.edu
3. Cornish, P., 2007. The CBRN System: Assessing the threat of terrorist use of chemical, biological, radiological and nuclear weapons in the United Kingdom. Chatham House, International Security Programme Report [online]. Available at: www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/cbrn0207.pdf
4. The Royal Society, 2004. Making the UK safer: detecting and decontaminating chemical and biological agents [online]. Available at: https://royalsociety.org/~/media/Royal_Society_Content/policy/publications/2004/9714.pdf
5. Shea, D.A. and Gottron, F., 2004. Small-scale terrorist attacks using chemical and biological agents: an assessment framework and preliminary comparisons. Congressional Research Service [online]. Available at: http://fas.org/irp/crs/RL32391.pdf
6. Collina, T.Z., 2014. Chemical and biological weapons status at a glance. 4 February, Arms Control Association [online]. Available at: www.armscontrol.org/factsheets/cbwprolif
7. Unal, B., 2015. Growing threat as organized crime funnels radioactive materials to terrorists. 13 October, Chatham House [online]. Available at: https://www.chathamhouse.org/expert/comment/growing-threat-organized-crime-funnels-radioactive-materials-terrorists
8. Organisation for the Prohibition of Chemical Weapons, 2015. Brief description of chemical weapons [online]. Available at: https://www.opcw.org/about-chemical-weapons/what-is-a-chemical-weapon/
9. WebMD, 2015. Biological and chemical weapons [online]. Available at: http://www.webmd.com/a-to-z-guides/secret-weapons-chemical-agents
10. Chief Medical Officer, 2002. Getting ahead of the curve: a strategy for combating infectious diseases (including other aspects of health protection). Department of Health [online]. Available at: http://antibiotic-action.com/wp-content/uploads/2011/07/DH-Getting-ahead-of-the-curve-v2002.pdf
11. Nelson, D. and Hussain, T., 2012. Militants attack Pakistan nuclear air base. 16 August, The Telegraph [online]. Available at: http://www.telegraph.co.uk/news/worldnews/asia/pakistan/9479041/Militants-attack-Pakistan-nuclear-air-base.html
12. Connett, D., 2015. Chlorine bomb attacks by jihadists are growing threat to the UK, warns chemical warfare expert. 25 May, Independent [online]. Available at: http://www.independent.co.uk/news/uk/home-news/chlorine-bomb-attacks-by-jihadists-are-growing-threat-to-the-uk-warns-chemical-warfare-expert-10274947.html
13. Verification Research, Training and Information Centre (VERTIC), 2015. 2015 meeting of experts to the 1972 Biological and Toxin Weapons Convention: statement for Working Session 7 on strengthening national implementation [online]. Available at: http://www.vertic.org/media/assets/Presentations/VERTIC%20GOC%20Statement_BWC%20MX%202015_FINAL.pdf
14. Halliday, J., 2015. Breaking Bad fan found guilty of ordering ricin delivery from FBI agent. 29 July, Guardian [online]. Available at: http://www.theguardian.com/uk-news/2015/jul/29/liverpool-man-who-ordered-breaking-bad-style-ricin-delivery-found-guilty
15. Jihadist Websites, 2006. Mujahidin Shura Council issues Abu-Hamzah al-Muhajir audio calling for use of dirty bombs against US bases in Iraq. 28 September, OSC document GMP20060929637002.
16. Said, S. and Lister, T., 2015. Report: ISIS steps up use of chemicals on battlefields in Iraq and Syria. 20 July, CNN [online]. Available at: http://edition.cnn.com/2015/07/19/middleeast/isis-chemical-weapons/index.html
17. Shoumali, K. and Yeginsu, C., 2015. New report of ISIS using poison gas in Syria. 24 August, The New York Times [online]. Available at: http://www.nytimes.com/2015/08/25/world/middleeast/isis-suspected-of-chemical-attack-in-syria.html?_r=0
18. Geneva Academy of International Humanitarian Law and Human Rights, 2014. Foreign fighters under international law. Briefing No. 7.
19. Prime Minister's Office, 2014. Threat level from international terrorism raised: PM press statement. 29 August [online]. Available at: https://www.gov.uk/government/speeches/threat-level-from-international-terrorism-raised-pm-press-conference
20. Asal, V.H., Ackerman, G.A. and Rethemeyer, R.K., 2012. Connections can be toxic: terrorist organizational factors and the pursuit of CBRN weapons. Studies in Conflict & Terrorism, 35(3), pp. 229-254.
21. McNeilly, W., 2015. Trident whistleblower: nuclear 'disaster waiting to happen'. May [online]. Available at: https://wikileaks.org/trident-safety/
22. Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, on a new approach to the detection and mitigation of CBRN-E risks, COM(2014) 247/F1, final.
23. Broad, W.J., Markoff, J. and Sanger, D.E., 2011. Israeli test on worm called crucial in Iran nuclear delay. 5 January, The New York Times [online]. Available at: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html
24. Orwant, R., 2015. Scientists build polio virus from scratch. 11 July, New Scientist [online]. Available at

https://www.newscientist.com/article/dn2539-scientists-build-polio-virus-from-scratch
25. Shea, J., 2013. How is NATO dealing with emerging security challenges? 26 July, Georgetown Journal of International Affairs [online]. Available at: http://www.ies.be/files/private/14)%20Shea%20-%20NATO%20Emerging%20Challenges.pdf
26. The Federation of American Scientists, 1997. The Chemical Weapons Convention [online]. Available at: http://fas.org/nuke/control/cwc/news/cwcfs.htm
27. Ito, M., 2015. Cult attraction: Aum Shinrikyo's power of persuasion. 14 March, The Japan Times. Available at: http://www.japantimes.co.jp/news/2015/03/14/national/history/cult-attraction-aum-shinrikyos-power-persuasion/
28. Olson, K.B., 1999. Aum Shinrikyo: once and future threat? Emerging Infectious Diseases, 5(4), pp.513-516.
29. European Parliament, 2015. CBRN terrorism: threats and the EU response. EU briefing [online]. Available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/%202015/545724/EPRS_BRI(2015)545724_REV1_EN.pdf
30. Monterey Institute of International Studies, 2001. Chronology of Aum Shinrikyo's CBW activities. James Martin Center for Nonproliferation Studies. [online]. Available at: cns.miis.edu/reports/pdfs/aum_chrn.pdf
31. Nuclear Threat Initiative (NTI), 2015. Understanding chemical threats [online]. Available at: http://www.nti.org/threats/chemical/
32. Organisation for the Prohibition of Chemical Weapons, 2015. Riot control agents [online]. Available at: https://www.opcw.org/about-chemical-weapons/types-of-chemical-agent/riot-control-agents/
33. Weitz, R., 2014. Syria and beyond: the future of the chemical weapons threat. Institut français des relations internationals, Proliferation Papers, 51, p.33.
34. Arnaz, F., 2015. Police: Syria returnees tied to Depok chlorine bomb. 25 March, Jakarta Globe [online]. Available at: http://jakartaglobe.beritasatu.com/news/police-syria-returnees-tied-depok-chlorine-bomb/
35. Breivik, A.B., 2011. 2083: A European Declaration of Independence [online]. Available at: http://fas.org/programs/tap/_docs/2083_-_A_European_Declaration_of_Independence.pdf
36. Lord Lyell (general rapporteur), 1996. Chemical and biological weapons: the poor man's bomb. North Atlantic Assembly Draft General Report [online]. Available at: http://fas.org/irp/threat/an253stc.htm
37. Acid Survivors Foundation, 2015. Acid attack statistics [online]. Available at: http://www.acidsurvivors.org/Statistics
38. De Castella, T., 2013. How many acid attacks are there? 9 August, BBC News Magazine [online]. Available at: http://www.bbc.co.uk/news/magazine-23631395
39. USA Today, 2004. Feds: what did Texas couple plan to do with cyanide? 30 January [online]. Available at: http://usatoday30.usatoday.com/news/nation/2004-01-30-texas_x.htm
40. Bar-Yaacov, N., 2015. What if ISIS launches a chemical attack in Europe? 27 November, Guardian [online]. Available at: http://www.theguardian.com/global/commentisfree/2015/nov/27/isis-chemical-attack-europe-public
41. NPR, 2011. Timeline: how the anthrax terror unfolded. 15 February [online]. Available at: http://www.npr.org/2011/02/15/93170200/timeline-how-the-anthrax-terror-unfolded
42. United States Department of Justice, 2010. Amerithrax investigative summary. 19 February [online]. Available at: http://www.justice.gov/archive/amerithrax/docs/amx-investigative-summary.pdf
43. Nuclear Threat Initiative (NTI), 2015. Understanding biological threats [online]. Available at: http://www.nti.org/threats/biological/
44. Centers for Disease Control and Prevention (CDC), 2015. Anthrax. [Online]. Available at: http://www.cdc.gov/anthrax/
45. United States Department of State, 2009. Preventing biological weapons proliferation and bioterrorism. 9 December [online]. Available at: http://www.state.gov/t/us/133335.htm
46. Leitenberg, M., 2005. Assessing the biological weapons and bioterrorism threat. Strategic Studies Institute, US Army War College [online]. Available at: http://www.strategicstudiesinstitute.army.mil/pdffiles/pub639.pdf
47. Defense Science Board Task Force, 2009. Department of Defense Biological Safety and Security Program [online]. Available at: http://www.acq.osd.mil/dsb/reports/ADA499977.pdf
48. Centers for Disease Control and Prevention (CDC), 2001. Recognition of illness associated with the intentional release of a biological agent. 19 October, Morbidity and Mortality Weekly Report [online]. Available at: http://www.cdc.gov/mmwr/preview/mmwrhtml/mm5041a2.htm
49. Jernigan, D.B. et al., 2002. Investigation of bioterrorism-related anthrax, United States, 2001: epidemiologic findings. Emerging Infectious Diseases, 8(10), p.1025.
50. Dudley, J.P. and Woodford, M.H., 2002. Bioweapons, bioterrorism and biodiversity: potential impacts of biological weapons attacks on agricultural and biological diversity. Revue scientifique et technique – Office international des Epizooties, 21(1), pp.125-138.
51. US Congress, 1993. Proliferation of weapons of mass destruction: assessing the risks. Office of Technology Assessment [online]. Available at: http://www.au.af.mil/au/awc/awcgate/ota/9341.pdf
52. Federation of American Scientists (FAS), 2013. Biosafety Level 4 labs and BSL information [online]. Available at: http://fas.org/programs/bio/biosafetylevels.html
53. The Japan News, 2015. BSL-4 facility OK'd to handle deadly viruses. 3 August [online]. Available at: https://www.questia.com/newspaper/1P3-3766686621/bsl-4-facility-ok-d-to-handle-deadly-viruses

54. BBC News, 2015. 'Dangerous' radioactive material stolen in Mexico. 16 April [online]. Available at: http://www.bbc.co.uk/news/world-latin-america-32332271
55. Haines, J.R., 2015. The case of Poland's stolen radiological material. Foreign Policy Research Institute [online]. Available at: http://www.fpri.org/articles/2015/03/case-polands-stolen-radiological-material
56. Nuclear Threat Initiative (NTI), 2015. Understanding radiological threats [online]. Available at: http://www.nti.org/threats/radiological/
57. International Atomic Energy Agency (IAEA), 2015. Incident and Trafficking Database (ITDB) [online]. Available at: http://www-ns.iaea.org/security/itdb.asp
58. McCloud, K. and Osborne, M., 2001. WMD terrorism and Usama Bin Laden. James Martin Center for Nonproliferation Studies, CNS Reports [online]. Available at: cns.miis.edu/reports/binladen.htm
59. HM Government, 2010. The United Kingdom's strategy for countering chemical, biological, radiological and nuclear (CBRN) terrorism [online]. Available at: http://webarchive.nationalarchives.gov.uk/20100418065544/http:/security.homeoffice.gov.uk/news-publications/publication-search/cbrn-guidance/strat-countering-use-of-CBRN?view=Binary
60. United States Nuclear Regulatory Commission (USNRC), 2008. Information sheet: radiation source use and replacement study [online]. Available at: http://www.nrc.gov/security/nas-facts-sheet.pdf
61. Pomper, M., Murauskaite, E. and Coppen, T., 2014. Promoting alternatives to high-risk radiological sources: the case of cesium chloride in blood irradiation. James Martin Center for Nonproliferation Studies, Occasional paper no. 9 [online]. Available at: http://www.nonproliferation.org/wp-content/uploads/2014/03/140312_alternative_high_risk_radiological_sources_cesium_chloride_blood.pdf
62. Cordesman, A.H., 2001. Radiological weapons as means of attack. Center for Strategic and International Studies (CSIS) [online]. Available at: http://csis.org/files/media/csis/pubs/radiological[1].pdf
63. Porter, W.C. and Sokova, E., 2002. Illicit nuclear trafficking in the NIS: what's new? What's true? The Nonproliferation Review [online]. Available at: cns.miis.edu/npr/pdfs/92potsok.pdf
64. Borger, J., 2010. Nuclear bomb material found for sale on Georgia black market. 7 November, Guardian [online]. Available at: http://www.theguardian.com/world/2010/nov/07/nuclear-material-black-market-georgia
65. The Telegraph, 2011. Six people arrested in Moldova over bomb-grade uranium. 29 June [online]. Available at: www.telegraph.co.uk/news/worldnews/europe/moldova/8607235/Six-people-arrested-in-Moldova-over-bomb-grade-uranium.html
66. Nuclear Threat Initiative (NTI), 2015. Understanding nuclear threats [online]. Available at: http://www.nti.org/threats/nuclear/
67. Kimball, D., 2015. Nuclear weapons: who has what at a glance. Arms Control Association [online]. Available at: http://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat
68. Kile, S. and Schell, P., 2015. Nuclear forces. Stockholm International Peace Research Institute (SIPRI) [online]. Available at: http://www.sipri.org/research/armaments/nuclear-forces
69. Corcoran, E.A., 2012. Threats and challenges: strategies in a new century. Colorado: Edward A. Corcoran.
70. Koren, M., 2013. Top ten cases of nuclear thefts gone wrong. 4 February, Smithsonian [online]. Available at: http://www.smithsonianmag.com/science-nature/top-ten-cases-of-nuclear-thefts-gone-wrong-10854803/?no-ist
71. Atomic Archive, 2015. Fission module [online]. Available at: http://www.atomicarchive.com/Education/Exercises/FissionSoln.shtml
72. Pomper, M.A., Bieniawski, A.J. and Sokova, E. The Case for Highly Enriched Uranium-Free Zones. NTI Paper [online]. Available at: http://www.nti.org/media/pdfs/The_Case_for_Highly_Enriched_Uranium-Free_Zones_Final.pdf?_=1436298789
73. Health and Safety Executive (HSE), 2015. What is nanotechnology? [online]. Available at: http://www.hse.gov.uk/nanotechnology/what.htm
74. National Nanotechnology Initiative, 2015. What is nanotechnology? [online]. Available at: http://www.nano.gov/nanotech-101/what/definition
75. Tripp, J.L., Demmer, R.H. and Meservey, R.L., 2001. Decontamination. In: Oh, C.H. (ed.), 2001. Hazardous and radioactive waste treatment technologies handbook. Boca Raton, FL: CRC Press, pp.8-16.
76. Guidotti, M., Ranghieri, M. and Rossodivita, A., 2010. Nanosystems and CBRN threats: a resource worth exploiting, a potential worth controlling. In: Trufanov, A., Rossodivita, A. and Guidotti, M. (eds), 2010. Pandemics and bioterrorism: transdisciplinary information sharing for decision-making against biological threats. Amsterdam: IOS Press, p.123.
77. The Royal Society, 2013. The Chemical Weapons Convention and convergent trends in science and technology [online]. Available at: https://royalsociety.org/~/media/policy/projects/brain-waves/2013-08-04-chemical-weapons-convention-and-convergent-trends.pdf
78. Ibrügger, L. (rapporteur), 2005. 179 STCMT 05 E – The security implications of nanotechnology. NATO

Parliamentary Assembly, 2005 Annual Session [online]. Available at: http://www.nato-pa.int/default.asp?SHORTCUT=677

79. Bradley, L.D., 2013. Regulating weaponized nanotechnology: how the international criminal court offers a way forward. Georgia Journal of International and Comparative Law, 41(3), pp.728-729.
80. Van Aken, J. and Hammond, E., 2003. Genetic engineering and biological weapons. EMBO Reports, Volume 4 (Special Issue), p.57.
81. Dando, M., 1994. Biological warfare in the 21st century: biotechnology and the proliferation of biological weapons. New York: Macmillan, p.210.
82. Ainscough, M.J., 2002. The next generation of bioweapons: the technology of genetic engineering applied to biowarfare and bioterrorism. The Counterproliferation Papers, Future Warfare Series No. 14, USAF Counterproliferation Center [online]. Available at: http://fas.org/irp/threat/cbw/nextgen.pdf
83. Park, J. (ed.), 2014. Science and technology to prevent and respond to CBRN disasters: ROK and US perspectives. Asian Institute for Policy Studies, Asan Report [online]. Available at: http://www.aaas.org/sites/default/files/reports/Asan-Report_Science-and-Technology-to-Prevent-and-Respond-to-CBRN-Disasters.pdf
84. Lentzos, F., Jefferson, C. and Marris, C., 2014. The myths (and realities) of synthetic bioweapons. 18 September, Bulletin of the Atomic Scientists [online]. Available at: http://thebulletin.org/myths-and-realities-synthetic-bioweapons7626
85. United Nations Interregional Crime and Justice Research Institute (UNICRI), 2012. Security implications of synthetic biology and nanobiotechnology: a risk response assessment of advances in biotechnology [online]. Available at: http://www.unicri.it/in_focus/files/UNICRI%202012%20Security%20Implications%20of%20Synthetic%20Biology%20and%20Nanobiotechnology%20Final%20Public-1.pdf
86. Mondloch, J.E. et al., 2015. Destruction of chemical warfare agents using metal–organic frameworks. Nature Materials, 14, pp.512-516.
87. Medical Research Council, 2014. MRC Review of Vaccines Research [online]. Available at: http://www.unicri.it/in_focus/files/UNICRI%202012%20Security%20Implications%20of%20Synthetic%20Biology%20and%20Nanobiotechnology%20Final%20Public-1.pdf
88. Murphy, D. et al., 2008. Why do UK military personnel refuse the anthrax vaccination? Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science, 6(3), p.239.
89. Baylon, C., 2014. Drones are an increasing security issue for the nuclear industry. 18 December, Chatham House Expert Comment [online]. Available at: https://www.chathamhouse.org/expert/comment/16539
90. Baylon, C., 2015. Leveraging Drones to Improve Nuclear Facility Security and Safety. 22 January, Chatham House Expert Comment [online]. Available at: https://www.chathamhouse.org/expert/comment/16722
91. Matishak, M., 2010. Nation's nuclear power plants prepare for cyber attacks. 27 August, NTI Global Security Newswire [online]. Available at: http://www.nti.org/gsn/article/nations-nuclear-power-plants-prepare-for-cyber-attacks/
92. US Department of Homeland Security, 2012. Chemical sector security awareness guide: a guide for owners, operators, and chemical supply-chain professionals [online]. Available at: http://www.dhs.gov/xlibrary/assets/oip-chemsec-case-for-action-042011.pdf
93. Stoye, E., 2015. Security experts warn chemical plants are vulnerable to cyber-attacks. 10 June, Chemistry World [online]. Available at: www.rsc.org/chemistryworld/2015/06/chemicalplants-vulnerable-cyber-attacks
94. XL Catlin, 2013. Environmental risks: cyber security and critical industries [online]. Available at: http://xlgroup.com/~/media/fff/pdfs/environmental_cyber%20risks_whitepaper_xl.pdf
95. ECA Group, 2015. Mini UAV for counter CBRN: the best resilience in non-secure environment [online]. Available at: http://eca-media.ecagroup.com/player/pdf?key=f918b622fdb66c0aac1409be62c7b8e6
96. Johnson, S., 2010. Come fly with me... CBRNe World, p.80.
97. Johnson, S., 2013. Through hard work to the stars., CBRNe World, p.77.
98. Kaszeta, D., 2014. CBRN robotics: unmanned recon and decon systems needed. 19 November, Cicero Magazine [online]. Available at: http://ciceromagazine.com/?s=robotics+unmanned
99. Guardian, 2015. Drone 'containing radiation' lands on roof of Japanese PM's office. 22 April [online]. Available at: http://www.theguardian.com/world/2015/apr/22/drone-with-radiation-sign-lands-on-roof-of-japanese-prime-ministers-office
100. Medalia, J., 2011. "Dirty Bombs": technical background, attack prevention and response. 24 June, Congressional Research Service Report for Congress, p.9.
101. Alion Science and Technology, 2014. Alion Awarded $2.8M DTRA Contract to Develop Improvements to Nuclear Detection Technology [press release]. 29 May [online]. Available at: http://www.alionscience.com/Top-Menu-Items/News-Room/Press-Releases/2014/Alion-Awarded-DTRA-Contract-to-Develop-Improvements-to-Nuclear-Detection-Technology
102. Oswald, R., 2014. Pentagon funds development of new tech for detecting 'dirty bombs'. 3 June, NTI Global Security Newswire [online]. Available at: http://www.nti.org/gsn/article/pentagon-funds-research-new-tech-detecting-dirty-bombs/

103. Rood, P., 2014. New nuclear detection technology set to thwart development of 'dirty bombs'. 12 December, The Engineer [online]. Available at: http://www.theengineer.co.uk/new-nuclear-detection-technology-set-to-thwart-development-of-dirty-bombs/
104. Wright, O., 2012. Dirty bomb terror threat breakthrough: British scientists build machine to detect smuggling of nuclear materials. 1 November, Independent [online]. Available at: http://www.independent.co.uk/news/uk/crime/dirty-bomb-terror-threat-breakthrough-british-scientists-build-machine-to-detect-smuggling-of-8273751.html
105. Chu, K.D., and Winfield, G., 2014. I, Printer. December, CBRNe World [online]. Available at: http://www.cbrneworld.com/_uploads/download_magazines/I_Printer.pdf
106. Sternstein, A., 2014. The FBI is getting its own, personal 3D printer for studying bombs. 13 June, Nextgov [online]. Available at: http://cdn.nextgov.com/nextgov/interstitial.html?v=2.1.1&rf=http%3A%2F%2Fwww.nextgov.com%2Fdefense%2F2014%2F06%2Ffbi-getting-its-own-personal-3d-printer-studying-bombs%2F86476%2F%3Foref%3Dng-dropdown
107. US Department of Homeland Security, 2011. Securing industrial control systems in the chemical sector: a roadmap awareness campaign – a case for action [online]. Available at: http://www.dhs.gov/xlibrary/assets/oip-chemsec-case-for-action-042011.pdf
108. Fleck, F. 2004. SARS outbreak over, but concerns for lab safety remain. Bulletin of the World Health Organization, 82(6), p.470.
109. Sample, I., 2014. Revealed: 100 safety breaches at UK labs handling potentially deadly diseases. 4 December, Guardian [online]. Available at: http://www.theguardian.com/science/2014/dec/04/-sp-100-safety-breaches-uk-labs-potentially-deadly-diseases
110. Sample, I., 2014. Revealed: 100 safety breaches at UK labs handling potentially deadly diseases. 4 December, Guardian [online]. Available at: http://www.theguardian.com/science/2014/dec/04/-sp-100-safety-breaches-uk-labs-potentially-deadly-diseases
111. Lentzos, F., 2015. 3D bio: declare, document and demonstrate. EU Non-Proliferation Consortium, No. 45.
112. Royse, C. and Johnson, B., 2002. Security Considerations for Microbiological and Biomedical Facilities, Anthology of Biosafety V - BSL4 Laboratories, Chapter 6. American Biological Safety Association [online]. Available at: http://www.absa.org/0200royse.html
113. Bender, B., 2014. Blood irradiators cited as threats to security: process uses radioactive power. 12 May, The Boston Globe [online]. Available at: http://www.bostonglobe.com/news/nation/2014/05/11/despite-safety-concerns-effort-phase-out-radioactive-medical-material-faces-resistance/fhNknm7ELLZBHSHC3AKI8L/story.html
114. CDC, 2013. Facts about ricin [online]. Available at: http://www.bt.cdc.gov/agent/ricin/facts.asp
115. Balint, G.A., 1974. Ricin: the toxic protein of castor oil seeds. Toxicology, 2(1), pp.77-102.
116. Edwards, R., 2008. Poison-tip umbrella assassination of Georgi Markov reinvestigated. 19 June, The Telegraph [online]. Available at: www.telegraph.co.uk/news/2158765/Poison-tip-umbrella-assassination-of-Georgi-Markov-reinvestigated.html
117. United States Environmental Protection Agency (EPA), 2015. Radionuclide basics: strontium-90 [online]. Available at: http://www.epa.gov/radiation/radionuclide-basics-strontium-90
118. 118.Alexander, G.A., 2006. Radiation decontamination. In: Ciottone, G.R. (ed.), 2006. Disaster Medicine. Philadelphia: Elsevier Health Sciences, p.468.
119. Boyle, A., 2002. Dirty bomb's biggest hazard: panic. 10 June, NBC News [online]. Available at: http://www.nbcnews.com/id/3077203/ns/technology_and_science-science/t/dirty-bombs-biggest-hazard-panic/#.VdG273FVhHw
120. International Atomic Energy Agency (IAEA), 2002. Inadequate control of world's radioactive sources. 24 June [online]. Available at: https://www.iaea.org/newscenter/pressreleases/inadequate-control-worlds-radioactive-sources
121. EPA, 2015. Radionuclide basics: cesium-137 [online]. Available at: http://www.epa.gov/radiation/radionuclide-basics-cesium-137
122. IAEA, 1988. The radiological accident in Goiânia [online]. Available at: http://www-pub.iaea.org/mtcd/publications/pdf/pub815_web.pdf
123. Vicinanzo, A., 2015. Lawmakers concerned over threat of dirty bomb to US ports. 4 November, Homeland Security Today [online]. Available at: http://www.hstoday.us/industry-news/general/single-article/lawmakers-concerned-over-threat-of-dirty-bomb-to-us-ports/36b591a8e4a6100190d65ad4bf6ccfcc.html
124. Wellerstein, A. 2012-2014. Nukemap [online]. Available at: http://nuclearsecrecy.com/nukemap/