

# THE JOURNAL OF TERRORISM & CYBER INSURANCE



JOURNAL  
OF  
TERRORISM  
&  
CYBER  
INSURANCE

[WWW.TERRORISMCYBERINSURANCE.COM](http://WWW.TERRORISMCYBERINSURANCE.COM)

[TEAM@TERRORISMCYBERINSURANCE.COM](mailto:TEAM@TERRORISMCYBERINSURANCE.COM)

## LEGAL NOTICE

*The Journal, its Management Team, Advisory Board and Sponsors do not purport to provide any advice which is legally binding in the process of producing or disseminating the Journal or any information contained within the Journal and should not be relied upon as a sole basis upon which insurance policies are underwritten. It is the expectation that each (re)insurer will do their own due diligence and use the information merely as an aid to understanding the risks and landscape upon which terrorism and cyber insurance is currently offered. Any information provided by the Journal should be used solely for educational purposes. The Journal cannot guarantee the accuracy of all detail within individual articles, rather the contributors individually guarantee the authenticity and originality of the work contributed. Further any of the contributors in providing an article, warrant that the Journal is their own work and does not breach any laws including copyright and/ or intellectual property laws.*

*Legally and from an operational perspective, the Journal is a neutral central party used to co-ordinate ideas, research and promote innovation. The Journal retains the legal rights to republish the research provided to it from contributors, however each contributor may seek the permission of the Journal to subsequently publish their work in other mediums. Similarly, if the article has been published previously in a similar format the author warrants that they have permission to have the article republished in the Journal.*

# THE JOURNAL OF TERRORISM & CYBER INSURANCE



## WELCOME & MISSION

We warmly welcome all our readers to the inaugural issue of the Journal of Terrorism & Cyber Insurance, on the 15<sup>th</sup> anniversary of 9/11. The Journal is founded to collate, decision-aiding information, research, ideas and potentially data sharing on terrorism and cyber (re)insurance.

[RMS catastrophist Dr Gordon Woo comments](#): “Even 15 years after 9/11, knowledge and understanding of terrorism insurance risk modelling across the industry is still relatively low. There is no shortage of literature on terrorism, but much has a qualitative geopolitical and international relations focus, and little is directly relevant to terrorism insurance underwriting or risk management.”.

Ariel Re specialty underwriter Dr Raveem Ismail echoes: “There is plenty of terrorism and cyber material out there, much of it, dross and much of little relevance to insurance. And these niche but increasingly important and material perils are often only a small part of traditional insurance industry media. Hence, the Journal of Terrorism & Cyber Insurance.”.

[Carter Insurance Innovation Limited’s](#) Managing Director, Rachel Anne Carter highlights: “Together we are a stronger force against terrorism. To date we have had a number of warning signs, promoting greater utilisation of combined expertise, intelligence and rationality to make a difference – putting ideas into action and creating a forum to share research and promote innovation with the Journal of Terrorism and Cyber Insurance as an instrumental platform in delivering this. This far surpasses the commercial rationale of any individual player. Rather, such sharing of research which can then be utilised by the different stakeholders to strengthen resilience against terrorism, has the potential not only to benefit the insurance industry but ensure adequate insurance products are offered to provide fiscal protection for individuals against the economic costs of an attack. Together we can make history in changing the way we provide protection against terrorism risks but to do this we need to use the Journal of Terrorism and Cyber Insurance to share ideas, research and promote innovation in product development.”.

We have been pleasantly surprised by the encouragement that the journal has received from across the industry, lending support to our view that it is a much needed nexus. In this inaugural edition, we welcome diverse authors from the (re)insurance industry, as well as insight from practitioners dealing with man-made catastrophes. We hope you find it thoughtful and useful reading.



Rachel Anne Carter, Manager and Co-Founder & Raveem Ismail, Co-Founder.  
October 2016.

## FORMAT & BREVITY

The Journal's staff is keenly aware that industry professionals are busy – hence whilst we consider it important to source, review and edit full length articles of substance, we also facilitate access to the same ideas via shorter summaries, which will also [appear on the website](#) and mailing list, alongside discussions and interviews with the authors.

Each future edition of the Journal will be split into two sections:

- News, shorter articles, and summaries.
- Full length articles.

Thus allowing efficient perusal for all our constituencies.

## EDITORS

The JTCI's founding members, all of whom write for us in this edition, comprise:

- Rachel Anne Carter. Managing Director at Carter Insurance Innovations Limited.
- Dr Raveem Ismail. AVP & Specialty Treaty Underwriter at Ariel Re.
- Dr Gordon Woo. Catastrophist at RMS.
- Padraig Belton. Journalist at the BBC, S&P, and The Spectator.

## JTCI ONLINE

We welcome followers and subscribers on all our online presences. We also encourage readers to sign up to our entirely fascinating and unobtrusive email list ([website, right hand column](#), or email [team@terrorismcyberinsurance.com](mailto:team@terrorismcyberinsurance.com)).



[team@TerrorismCyberInsurance.com](mailto:team@TerrorismCyberInsurance.com)



[www.TerrorCyberInsurance.com](http://www.TerrorCyberInsurance.com)



[www.terrorismcyberinsurance.com/feeds/posts/default](http://www.terrorismcyberinsurance.com/feeds/posts/default)



[www.linkedin.com/company/journal-terrorism-cyber-insurance](http://www.linkedin.com/company/journal-terrorism-cyber-insurance)



[www.Facebook.com/TerrorismCyberInsurance](http://www.Facebook.com/TerrorismCyberInsurance)



[www.Twitter.com/TerrorCyberIns](http://www.Twitter.com/TerrorCyberIns)

## SPONSORS

We are very pleased to welcome [Property Claims Services](#) (PCS, a division of [Verisk Analytics](#)) as our inaugural sponsor.



PCS

[PCS' Tom Johansmeyer](#) stated: "The terror threat is shifting. Adaptation and collaboration is necessary to ensure (re)insurance products are fit for purpose and can be employed to deploy capital efficiently when times are tough... The need for greater focus on improved risk and capital management relative to terror and cyber has only gained momentum over the past year, and the trajectory seems likely to continue. The *Journal of Terrorism & Cyber Insurance* provides a crucial forum for the exchange of thought leadership and commercial insights that can help re/insurers allocate capital more effectively and – more importantly – communities and businesses recover from an event. The role of the insurance industry is to protect the insured and society. The JTCI should provide a forum to help advance that mission."

## Contents

Welcome & Mission .....	3
Editors .....	4
JTCI Online.....	4
Sponsors .....	5
1. JTCI statement on 15 years after 911 .....	6
2. Forecasting Political Violence Frequency .....	7
3. 3 Challenges for the Terrorism Market - 15 Years After 9/11 .....	13
4. Cyber Terrorism & Australia's Terrorism Insurance Scheme .....	15
5. Can Insurance Evolve to Meet the New Terror Threat? .....	20
6. Drones & Terrorism.....	25
7. Terrorism, a necessary public-private partnership.....	34
8. Terror Risk Transfer: What We Can Learn From Krasnovia .....	41
9. Decontamination of Buildings after an Anthrax Attack .....	47
10. Methods to Quantify Terrorism Risk.....	61
11. Evaluating The Sunni-Salafi Jihadi CBRN Threat .....	66
12. Non-Conventional Terrorism Hazards <sup>1</sup> .....	79
13. ISIS Attacks in Paris and San Bernardino .....	92



**Pádraig Belton, DPhil (Candidate, Oxon), MA, BA**  
**Journalist**  
**BBC, S&P, The Spectator**

[www.linkedin.com/in/padraigbelton](http://www.linkedin.com/in/padraigbelton)

Pádraig Belton is a journalist who writes for the BBC, S&P, and the Spectator. At the BBC, his particular area of interest concerns technology and business, and has included reporting a number of feature stories involving cyber issues, insurers, and banks. For the S&P financial newswire, he is the chief correspondent for financial services in Europe, writing three articles a week on investment banks, hedge funds, asset managers, financial technology, and exchanges. In Ireland, the Middle East, and Africa, he also covers a wider variety of banking and insurance stories. Conflict areas from which he has reported for the BBC and other media have included eastern Ukraine, the Pakistan-Afghanistan border, and the West Bank.

He is completing a doctorate in politics at Oxford. A former Fulbright scholar, he also has studied at Yale and the School of Oriental and African Studies, where he read Arabic, Urdu, and Persian. In 2013 he won the [Royal United Service Institute's Trench-Gascoigne Prize](#) for an essay on cyber-security, and is chairman of the [Westminster Strategic Studies Group](#). He is based principally between Ireland and London, with frequent travel for reporting.

## **1. JTCI STATEMENT ON 15 YEARS AFTER 911**

This launch issue of our Journal goes to the presses as the world marks fifteen years since the loss of 2,996 lives in the attacks on the World Trade Centre by hijacked passenger aeroplanes on 11th September, 2001. (By comparison, the four decades of political fighting which had recently ended in the north of my own island had killed 1,841 civilians.)

The political tumult which engulfed the world as a consequence, in Afghanistan, Iraq, and now Syria, has left little unchanged in world politics.

Within the world of finance, underwriting insurance products against, say, the recurrence of the \$31.7 billion loss of property has raised difficult questions, the odds difficult to predict and the potential liability enormous.

The same period has seen the thoroughgoing computerisation of our lives, from the ubiquity of first e-mail and then the smartphone, to the first appearance of the Internet of (occasionally, one reasons, bad) Things. Cyber-insurance as a technique of transferring the risks of computer use to an insurer, in return for a fee, is still a novel instrument, but one about which we will hear more, including in these pages.

To those who lost their lives that day, and the people who in the last fifteen years have worked to prevent a similar loss of life through political violence, the launch issue of our journal is respectfully dedicated. At the going down of the sun, and at its rising.



**Dr Raveem Ismail, DPhil, MSc, MPhys (Oxon), MInstP**  
**AVP & Specialty Treaty Underwriter**  
**Ariel Re**

[www.linkedin.com/in/raveem](http://www.linkedin.com/in/raveem)

Raveem is an analytical underwriter with a focus on challenging perils such as political violence (war, terror) and cyber. He is currently a Specialty Treaty Underwriter at Ariel Re, Bermuda, where he has helped create the terrorism book, and Chair of the Insurance Special Interest Group on EU COST Action IS1304: Structured Expert Judgement. He constantly strives to bring analytical strength to bear on challenging underwriting problems.

Raveem was previously Validus Holding's Terrorism & War Underwriting Analyst in London, the dedicated resource on these perils across the Group's operating entities. He started his reinsurance career at Aon Benfield Impact Forecasting, where he rebuilt the ELEMENTS catastrophe model for terrorism. He has also consulted for IHS Exclusive Analysis on quantitative political violence, and worked in finance. Raveem's research background is in atmospheric physics modelling, and he is a triple graduate of Oxford University.

## 2. FORECASTING POLITICAL VIOLENCE FREQUENCY

### *Structured* Expert Judgement for (Re)insurance

*There are no hard facts, just endless opinions. Every day, the news media deliver forecasts without reporting, or even asking, how good the forecasters really are. Every day, corporations and governments pay for forecasts that may be prescient or worthless or something in between. And every day, all of us - leaders of nations, corporate executives, investors, and voters - make critical decisions on the basis of forecasts whose quality is unknown.*

Superforecasting: The Art & Science Of Prediction.  
 Tetlock & Gardner, 2015, Crown Publishers.

### OVERVIEW

(Re)insurers and ILS entities exist to put investor capital at risk in exchange for premium – often with very little relevant data. Some contracts cover very remote perils, such as meteorite strikes, others, like terrorism and cyber, change significantly year to year. Standard statistical methods are little help in these situations, and expert judgment becomes a crucial tool. But experts often disagree, and it can be difficult for decision-makers, aiming at prudent underwriting, to draw strong conclusions from contradictory opinions. A key impediment to securitisation of niche risks such as terrorism (and, in due course, cyber) is the appraisal of future event frequency feeding the models. Here, we discuss a new approach for systematically “making the best guesses” in (re)insurance.

### EXPERT OPINION

Ideally all decision-aiding models (including pricing, capital, and catastrophe models) would be based on objective criteria such as exhaustive data and sound physical principles. This

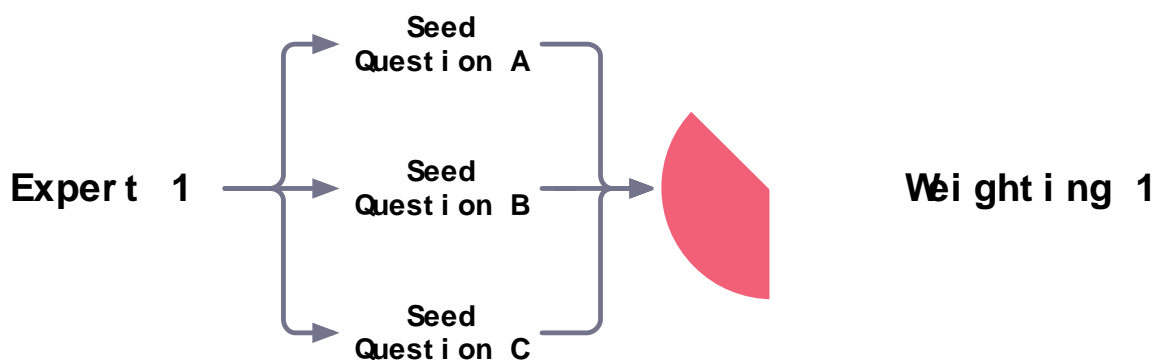
situation rarely occurs, and (re)insurance and ILS entities frequently have to act in data-poor environments, relying heavily on expert judgement. This occurs particularly in low frequency high severity/loss practice areas: rare and catastrophic risk appraisal is almost entirely based on expert judgement. Solvency II, with its requirement of 1-in-200-year event appraisal, implies that the regulatory capital regime across the EU is also based on expert judgement application.

Decision makers can and should demand the most unbiased expert judgement procedures, with objective criteria to appraise expert performance. But how? Referencing a first actual study, we discuss one approach, used in others fields but not yet in (re)insurance. This is *Structured Expert Judgement* (SEJ), which is an auditable and objective combination of multiple judgements, each weighted by its skill in gauging uncertainty. This produces a better overall judgement within a plausible range of outcomes.

A single expert's judgement might be an outlier, but consulting ten experts will yield ten different answers. Each answer is an (unknowable) function of an expert's previous experience, grasp of data, judgemental capability, biases, mood on the day, etc. Without a method of selecting between so many different judgements, the customer (insurance companies) often simply sticks with what they know best: inherited tradition, a longstanding provider/relationship, or market reputation/brand. None of these is any indicator of capability: the client cannot know the quality since no performance-based appraisal of forecasting ability has occurred. Any simple averaging leads to limited gains since each expert is weighted equally without regard for capability: the final answer may actually be less accurate than some individual answers due to outliers.

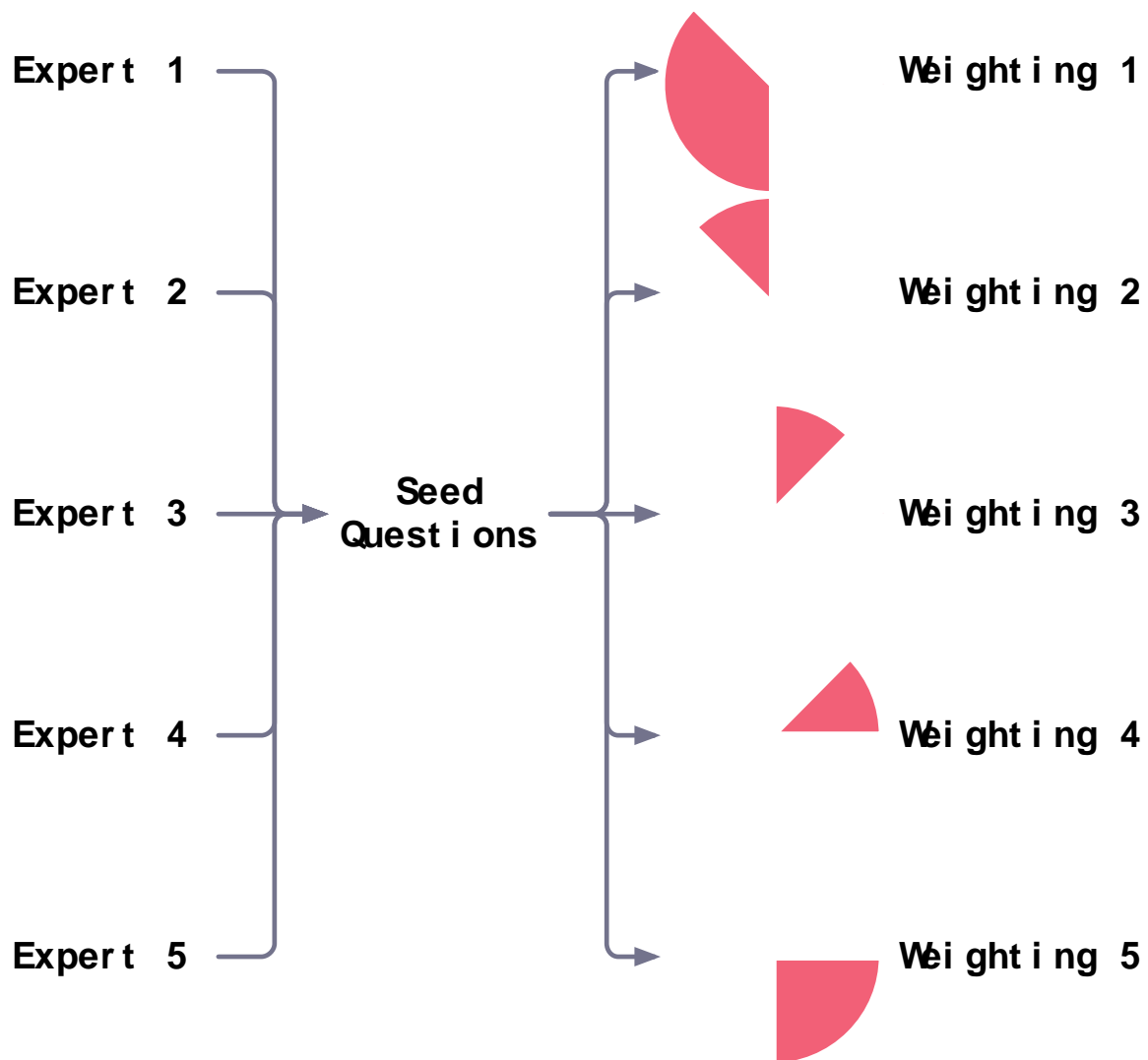
## STRUCTURED EXPERT JUDGEMENT (SEJ)

SEJ differs from and extends previous opinion pooling methods. Each expert is first *rated* with regard to prior performance by being asked a set of *seed questions* to which the answer is *already known* to the elicitation facilitator, but not necessarily to the expert.

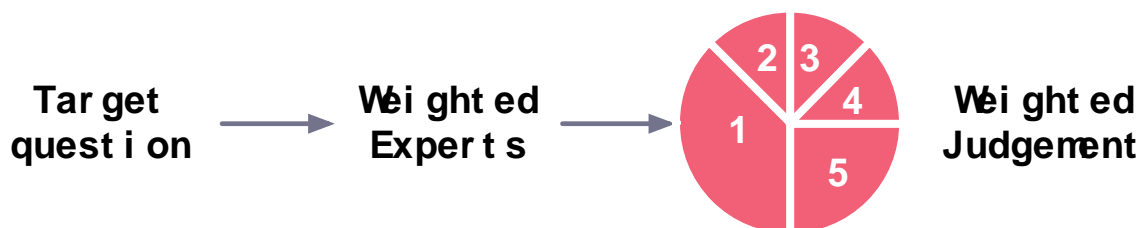


Each expert's performance on these seed questions ascertains that expert's weighting.





Experts are then asked the *target question(s)*; the actual judgements being sought, to which answers are *not* known. Weightings drawn from seed questions are then used to combine the experts' judgements on the target question, producing one outcome which truly combines the different expert judgements in a way which is performance-based, and is thus potentially better than each individual answer.



Seed question design is critical: these must be chosen for their tight alignment with target question(s); testing the same ability required for target questions, thus maximising the utility of performance weighting. The effectiveness of the weighting will be impacted by poorly designed seed questions.

## A FIRST (RE)INSURANCE SEJ ELICITATION: FUTURE POLITICAL VIOLENCE FREQUENCY

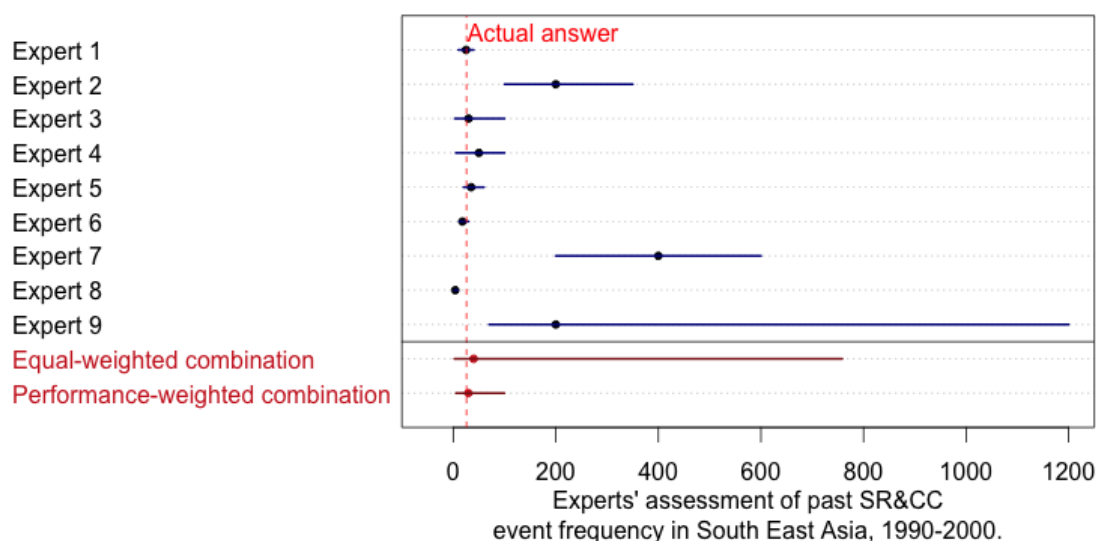
Cooke's Classical Model ([Experts In Uncertainty. 1991, Oxford University Press](#)) for SEJ involves asking each expert for two metrics: a confidence interval between which they think the true value lies (5% to 95%) and a central median value.



These are then used to calculate how well the expert gauges uncertainty spreads ("information"), and how reliably they capture true values within their ranges (statistical accuracy or "calibration").







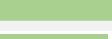





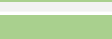















Under the [ISCH EU COST Action IS1304's Reinsurance Special Interest Group](#), a first elicitation was performed in January 2016, with 18 seed and 8 target questions. This was for an inherently unknowable future metric: the 2016 frequency of SR&CC (Strikes Riots & Civil Commotion) in blocs of countries (Central Asia, Maghreb, etc.), with participants drawn from across the (re)insurance profession. An example of their judgements on a single seed question (prior SR&CC events in South-East Asia) are shown in the first figure ("Seed Question 11").

Seed Question 11.



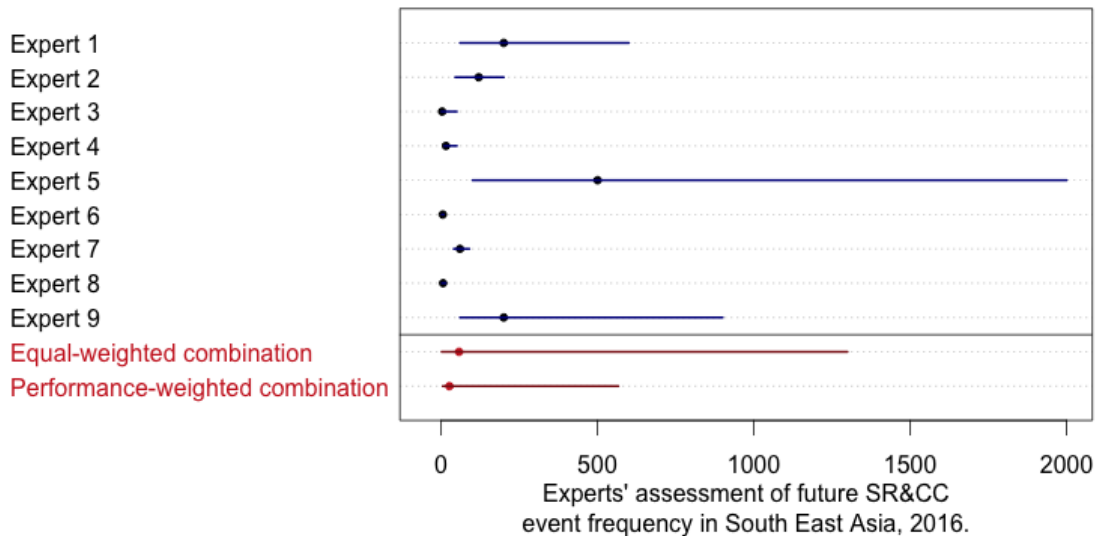
Experts produced a variety of median values and ranges, some having tightly bound ranges which captured the true value (dotted red line). The table shows information and calibration scores across the full seed question set. Two experts emerge with notably strong performance-based weights. If all experts were weighted equally (penultimate column), this discovered capability would be diluted away ("equal-weighted" row, table foot, and penultimate plot line in "Seed Question 11").

## FORECASTING POLITICAL VIOLENCE FREQUENCY

Expert	Calibration	Information	Equal weights	Performance weights
<b>1</b>	 0.2295	 1.864	 0.1111	 <b>0.428</b>
2	<0.0001	 1.783	 0.1111	<0.0001
3	0.002	 2.04	 0.1111	0.0041
<b>4</b>	 0.2274	 1.665	 0.1111	 <b>0.3785</b>
5	0.0002	 2.153	 0.1111	0.0006
6	<0.0001	 3.01	 0.1111	0.0002
7	<0.0001	 1.505	 0.1111	<0.0001
8	<0.0001	 2.495	 0.1111	<0.0001
9	0.0001	 0.734	 0.1111	<0.0001
Equal-weighted combination	 0.6286	 0.869	 0.4242	
<b>Performance-weighted combination</b>	 0.5173	 1.701	 <b>0.7561</b>	

However, if the experts' judgements are combined using the weights from the calibration exercise (last column), then a combination emerges which capitalises on these high performance experts to produce better results than all of them ("performance-weighted" row at table foot, and last plot in "Seed Question 11"). When this performance-weighted combination is used for a target question, the second figure results ("Target Question 7").

Target Question 7.



Now for this forward-looking question, there is *no known answer*, yet we see that the performance-weighted process has allowed the influence of Experts 1 and 4 to provide a much tighter and more informative judgement than would most individual experts, or the equal-weighted combination (which is inflated by outliers). For the performance-weighted

combination, outliers are ameliorated and identified experts, given more weight. Such a final frequency, with associated range, could now feed a underwriting/pricing decisions or catastrophe models with greater assurance than customary approaches.

## CONCLUSION

Structured Expert Judgement is still judgement. But it is not guesswork, being a transparent method of pooling multiple opinions, weighted according to performance criteria aligned to the actual judgements being sought. Where data or models are lacking, it forms an objective and auditable method of producing decision-making judgements and inputs to models. We have described a first SEJ elicitation in our area of interest, where this method has been shown to identify true expertise and outperform uncalibrated methods, opening up the potential for use in innovative risk transfer.

It should be noted that SEJ is not a silver bullet: where there are science-based models or suitable data, these should trump expert judgement (or be used in tandem). But in their absence, in classes of business such as political violence, and for situations where tail risk is being gauged, SEJ would look to naturally provide significant enhancement to decision-making and risk appraisal.

## NOTES

- ISCH EU COST Action IS1304 on Structured Expert Judgement ([www.expertsinuncertainty.net](http://www.expertsinuncertainty.net)). This effort aims to bridge the gap between scientific uncertainty and evidence-based decision making. The political violence elicitation referenced here took place in London in January 2016, kindly hosted by [Dickie Whitaker](#) and the [Lighthill Risk Network](#), run by the COST Action's [Reinsurance Special Interest Group](#), principal investigators being Dr Raveem Ismail, [Christoph Werner \(Strathclyde University\)](#), and [Professor Willy Aspinall \(Bristol University\)](#).
- The full study will be a forthcoming publication in a scientific journal (permanent URL: <http://1drv.ms/1VZkuGh>). A shorter version of this article [Ask The Experts](#), co-authored by [Scott Reid](#), appeared in *The Actuary*. This current version is published both on [www.InsuranceLinked.com](http://www.InsuranceLinked.com) and in [The Journal Of Terrorism & Cyber Insurance](#).



**Chris Holt, MBE**  
**Managing Director**  
**CHC Global**

[www.linkedin.com/in/chris-holt-74a927](http://www.linkedin.com/in/chris-holt-74a927)

Chris Holt is an independent consultant who has spent over 20 years managing and responding to the risks posed by terrorism and other malicious acts. After an initial career in the British Military, Chris joined the insurance market in 2008. He has an interest in harnessing technology to better understand & communicate extraordinary risks.

### **3. 3 CHALLENGES FOR THE TERRORISM MARKET - 15 YEARS AFTER 9/11**

This summer I re-read the excellent book "War Risk and Terrorism" which was published by The Insurance Institute of London in October 2007. In so doing, I was reminded of one of the key moments in the evolution of our market; the deadly bombing of the King David Hotel in Jerusalem in July 1946, in which 91 people lost their lives and 41 were injured.

The event apparently changed the perception in the London Market of what was actually meant by "terrorism", and how property insurers might respond most appropriately. The market responded, but it took 12 years before four standard exclusions were agreed.

I was struck by the similarity between that period and the situation we face today in coping with a threat, our understanding of which is different to the one many of us grew up with.

This year we mark the 15th anniversary of the tragic events of September 2001, and it is worth taking a moment to consider those 15 years from the perspective of our market. In the period since 9/11, Islamist terrorists have repeatedly and successfully targeted people in countries they perceive to be hostile to their ideology. We are all familiar with the tragic scenes from Bali, Moscow, Istanbul, Madrid, London, Mumbai, Paris and most recently Nice to name but a few.

From the information available, it appears that there is routinely a significant gap between the economic impacts of these kinds of events and the scale of insurance indemnification. Thanks to the heroic efforts of the intelligence and security communities in the last 15 years, many planned attacks have been thwarted and we are yet - thankfully - to see the successful deployment of a chemical, biological, radiological or nuclear weapon with widespread impacts. What we do know, is that there are many uncertainties relating to the potential reinstatement costs of a CBRN attack, and that financial recovery after a macro event will likely involve a political component. We also know that we could take steps at construction stage to implement measures that will mitigate the impact of an attack.

But the major change of the last 15 years has of course been information technology entering every part of our lives, and unsurprisingly, malicious groups now occupy this realm and seek to exploit cyber vulnerabilities.

These three broad factors present three corresponding challenges for our market; the gap between the economic impacts of terrorism and the existing products, how to appropriately deal with CBRN, and what to do about malicious cyber. In all cases there is an opportunity for the market to innovate, attract new premium, and make our societies more resilient. In all three areas we are yet to see a clear way forward. Part of the problem is of course that the insured doesn't always recognise their exposure let alone seek to purchase a product; however until the products and solutions are widely available, it is difficult to create the means to distribute them. And until that is done, it will be difficult to influence behaviour to build resilience as a factor into the insurance buying process.

In the last 15 years, 'terrorism' has evolved significantly and we are therefore in a period where the market is beginning to respond - whether through more flexible non-damage business interruption cover, cover for the kind of lone wolf attacks that have become prevalent and solutions aimed at the SME market. Whilst insurers will innovate and lead as they always have, there is an important role for other institutions to play, not least the national terrorism pools and other schemes that reinsure terrorism risk. In highlighting the gaps the market can fill between economic and insured loss, these institutions might help narrow the so called terrorism insurance gap. In the UK, Pool Re is supporting its members and the UK Government in new ways which ensure broader spread of risk, reduced cost on business, increased resilience and a sizeable buffer protecting the tax payer; and at the same time it's providing the free market with new ways to engage in terrorism insurance. Likewise, Lloyd's will doubtless have a role to play - particularly in any solution that is identified for malicious cyber.

As we enter the 16th year after 9/11 it is worth reflecting on a quote from Hermes Marangos and Andrew Tobin from "War Risks and Terrorism"; *The point is, however, that as 'terrorism' evolves, so must the insurance policy wordings attempting to deal with it.*

It is an interesting time to be part of the terrorism (re)insurance market, where the opportunity now exists to innovate, and as a result, ultimately help make our societies more resilient to terrorism.



**Dr Christopher Wallace BEc (Hons), PhD (Econ), ANZIIF (Fellow), GAICD  
CEO  
ARPC**

[www.linkedin.com/in/cwallaceau](http://www.linkedin.com/in/cwallaceau)

Chris is the CEO of Australian Reinsurance Pool Corporation (ARPC). He was appointed CEO of ARPC in December, 2013. He has more than 30 years' experience in general insurance, workers' compensation, and health insurance. Dr Wallace has worked extensively in insurance underwriting and claims management roles within insurers, and as a consultant to the insurance industry. Previous roles include being General Manager Workers Compensation at GIO, Executive Director at Ernst & Young, and most recently as General Manager Benefits Management at HCF. He has a doctorate in economics, specialising in general insurance pricing and general insurance strategy. He is a fellow of the Australian and New Zealand Institute of Insurance and Finance and is a Certified Insurance Professional.

#### **4. CYBER TERRORISM & AUSTRALIA'S TERRORISM INSURANCE SCHEME**

*A recent white paper by the Australian Reinsurance Pool Corporation (ARPC) explains why physically destructive cyber terrorism is a gap in current insurance coverage.*

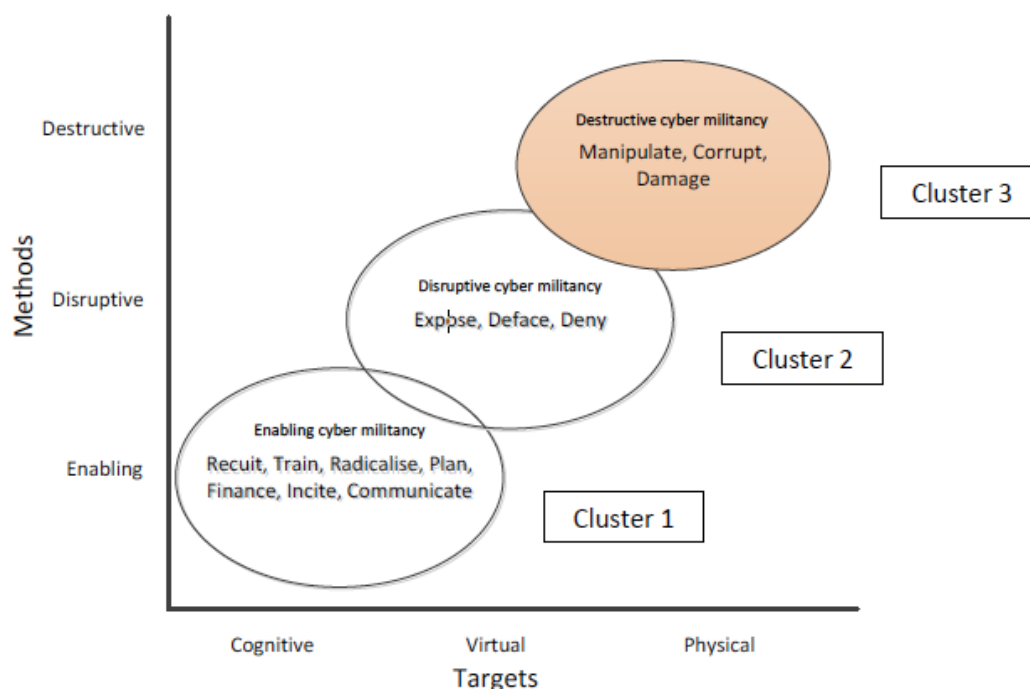
According to Major General Stephen Day, the first Co-ordinator of the Australian Cyber Security Centre, a significant cyber terrorist attack occurred in August 2013. In that attack, the websites of media companies such as the *New York Times*, *The Huffington Post* and Twitter were allegedly hacked by a Syrian group known as the Syrian Electronic Army. During that attack, users who clicked onto those respective websites were redirected to a server controlled by the Syrian group.

So, what constitutes an act of terrorism and what is the range of potential cyber terrorist activities?

#### **DEFINING CYBER TERRORISM**

In an article for the US-based *Combating Terrorism Centre (CTC) Sentinel* in August 2012, Jonalan Brickey sets out a useful classification scheme titled "Clusters of cyber terrorism" as a "qualitative approximation".





**Figure 1: Clusters of cyber terrorism**

(Defining Cyberterrorism: Capturing a broad range of Activities in Cyberspace, Jonalan Brickey, CTC Sentinel, August 2012, VOL 5, Issue 8)

Brickey sees terrorism targets as cognitive (the minds of people), virtual (resources in cyberspace) and physical (the physical things connected with and via cyberspace). Terrorist methods to attack targets are seen as enabling, disruptive and destructive.

Brickey's diagram focuses on terrorists as actors, but he also makes the point that other actors such as nation states, organised criminals and general hackers may also carry out activities in the same clusters and these could be represented as different planes on another third dimensional axis.

He ultimately presents a definition of cyber terrorism as "the use of cyber capabilities to conduct enabling, disruptive and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of political change".

A major concern to governments worldwide, including the Australian Government, is the possibility that a terrorist group could develop the ability to carry out destructive physical attacks by cyber means.

## TERRORISM IN AUSTRALIA

Terrorism is defined in Australia in the *Criminal Code Amendment (Terrorism) Act 2003* (CCA Act), Section 100.1:

*To be classed as terrorism, an action needs to cause harm or serious risk to people or serious damage to property or it may cause serious interference, disruption or destruction. In addition, the action can't be advocacy, protest or dissent where there was no intention to cause harm or risk or damage. The action must also be done with the intent of advancing a political, religious or ideological cause and the action must be done with the intent of coercing or influencing by*



*intimidation a government, Federal, State or Territory or the general public or a foreign country.*

In a recent global survey, PwC estimated the annual global cost of cyber attacks at between US\$375 billion and US\$575 billion. PwC stated that a true figure is ultimately unknowable as many attacks go unreported and costs such as the theft of secrets and intellectual property are largely unquantifiable. The PwC survey reported a dramatic increase in security incidents detected between 2013 and 2014, with a dramatic 41% jump in Europe, 11% in North America and 5% in the Asia-Pacific region.

## **INSURANCE COVER AND CYBER TERRORISM**

In Australia, the Mark IV and Mark V Industrial Special Risks (ISR) policies are industry standard wordings that are the most commonly used starting point for property insurance contracts for large businesses. This would include big businesses with infrastructure such as power stations, chemical plants, dams and refineries.

The standard may be modified with parts removed or added, but the unmodified Mark IV policy contains this section below:

### **PERILS EXCLUSIONS**

*7. Physical loss, destruction or damage occasioned by or happening through: (a) (ii) Access by any person(s) other than the Insured or the Insured's employee(s) to the Insured's computer system via data communication media that terminate in the Insured's computer system.*

Insurers also offer "business package" products to small and medium-sized enterprises and these normally have property and business interruption sections of cover. In line with the Mark IV ISR standard policy, many of these business package products have exclusions for physical loss as a consequence of malicious external access to the insured's computer systems. For example:

#### **Example: Insurer A, business package exclusions**

*We will not pay You under this section for physical loss, destruction or damage caused by, or as a consequence of:*

*24. Computer access – The gaining of access by any person other than You or Your employees to Your computer system via data communication media.*

#### **Example: Insurer B, business property policy section exclusions**

*2. We will not cover You for loss or damage caused by:*

*r) the gaining of unauthorised access to Your computer via any communication system by any person other than You or Your directors, partners, employees, officers or any other person who has an interest in the property.*

Because these exclusions are not terrorism exclusions, they would remain and there would be no effect to the liability of the insurer by the declaration of a terrorism incident.

## **ROLE OF THE TERRORISM INSURANCE SCHEME**

The terrorism insurance scheme was set up as a response to insurance market failure and a need to protect the economy from the financial impact of terrorist attacks. The government passed

the *Terrorism Insurance Act 2003* (TI Act), which renders terrorism exclusions in eligible insurance contracts ineffective if a terrorism incident is declared by the relevant government minister. The TI Act also established the ARPC as a source of Australian terrorism reinsurance.

The scheme covers policies that insure construction sites, commercial property and tangible contents (in Australia) for loss or damage, business interruption and liability as an owner or occupier of eligible property. The scheme covers the additional liability that an insurer incurs if a terrorism incident is declared by the relevant government minister, as this has the effect of striking out terrorism exclusion clauses in an eligible insurance policy.

However, there are several exclusions to the reinsurance coverage provided by the terrorism insurance scheme and these are primarily established in Schedule 1 of the Regulations. Specifically, in the context of this paper, “loss arising from computer crime” is one of the 40 exclusions specified in Schedule 1 of the Regulations.

Exclusion 32 of Schedule 1 of the Regulations states:

*32 A contract of insurance to the extent that it provides cover for loss arising from computer crime.*

## WHAT IS COMPUTER CRIME?

The section below is extracted from the Federal Attorney General’s Department website:

*In Australia, the term ‘cybercrime’ is used to describe both: 1) crimes directed at computers or other information communications technologies (such as hacking and denial of service attacks); 2) crimes where computers or ICTs are an integral part of an offence.*

Even if an insurer’s property policy does cover malicious physical property damage as a result of remote computer access, then that act will likely be defined as computer crime under the Australian Criminal Code and therefore any loss arising would be excluded from coverage by the terrorism insurance scheme.

A major point in the declaration of a cyber-based terrorist incident is that Australia applies a non-disclosure policy for cyber crimes that have state backing. This reduces the possibility that a major cyber attack could be officially declared as terrorism for the purposes of the TI Act, as such a declaration would be contrary to government policy.

## GREY AREAS

It is conceivable that terrorists may use a cyber attack to compromise a physical security system, which then enables a physical attack to take place, such as the bombing of a commercial property.

Would the terrorism insurance scheme respond to this terrorism scenario or was the loss arising from a computer crime?

Unauthorised access to compromise an electronic security system would likely fall under Section 10.7 (computer offences) of the Australian Criminal Code and may not be covered by the scheme. This would likely be contrary to the current expectations of the insurance industry and policyholders.

## NEW CYBER INSURANCE POLICIES

There are a growing number of insurance products in the area of cyber insurance that aim to cover electronic data assets' damage or loss and/or the business interruption and response costs that may arise. The detail of coverage varies considerably. However, cyber insurance products don't generally address physical damage to tangible property caused by a cyber attack other than perhaps damage to computer hardware.

In a December 2014 article, PartnerRe reported that: "Despite the vulnerability and significant loss potential, cyber insurance cover is almost totally absent for physical damage and limited for business interruption (non-physical damage and property damage). For these there remains a lack of clarity amongst insureds over the exact exposure potential, irritation about the limited availability of protection and confusion linked to non-standardised covers. The result of all these factors is that insureds are increasingly asking for cyber protection to be added to their existing liability and property covers either through endorsement or (and where we have particular concern) by removing the cyber exclusion."

For the purpose of terrorism risk reinsured with the ARPC, if the relevant cyber exclusion is removed from property damage policies then, in the event of a terrorism incident, any terrorism exclusion will be struck out and the insurer will be liable for any loss arising. Importantly the insurer will not be able to reinsure a cyber terrorist perpetrated risk with ARPC because of the current computer crime exclusion in the Regulations.

Although the ARPC scheme excludes computer crime, it is technically possible for cyber insurance policies to be eligible insurance contracts under the scheme. One example of a cyber insurance product analysed for this paper could be classified as an eligible insurance contract because it covers an eligible property and loss type combination, being business interruption loss arising from damage to tangible computer hardware property.

However, after the exclusion of computer crime as a source of loss, the only remaining insured sources of loss are accidents and omissions and it is unclear how these might possibly arise from a terrorism incident that is, by definition, deliberate.

## NOTES

You can read the full white paper online on the ARPC [website](#). This article was first published in [The ANZIIF Journal](#) Issue 2, Volume 39, 2016.



**Rachel Anne Carter, PhD (Candidate), MSyI, LLB (Hons), BA**  
**Managing Director**  
**Carter Insurance Innovations Limited**

[www.linkedin.com/in/rachelannecarter](http://www.linkedin.com/in/rachelannecarter)

Rachel is currently the Manager and Co-Founder the [Journal of Terrorism and Cyber Insurance](#). She is also a Managing Director for [Carter Insurance Innovations Limited](#), a consulting firm specialising in terrorism and cyber insurance; operating out of London and Paris.

Rachel is the terrorism insurance and cyber security insurance subject matter expert for the [Security Institute](#) (UK).

Her prior experience working in terrorism insurance and natural disaster insurance includes working for the CEO of Pool Re within a research capacity. Rachel began her terrorism insurance career as an insurance consultant for the OECD in the Directorate for Financial and Enterprise Affairs. During her time at the OECD she was instrumental in designing and implementing the [E-Platform](#) on terrorism risk insurance and had key involvement in the OECD terrorism risk insurance conferences in Paris and in Washington. In addition, Rachel was also involved in natural disaster insurance projects combining efforts of APEC and extending the OECD/G20 Methodological Framework on Disaster Risk Financing. During her time at the OECD, Rachel worked with various government representatives, industry leaders, academics, members the OECD High Level Advisory Board and heads of various natural catastrophe pools and terrorism risk insurance pools/ schemes.

Rachel has also had corporate insurance experience as a Senior Model Evaluation Analyst at Tokio Marine Kiln and as an Executive in the International Regulatory Affairs Department at Lloyd's. At Lloyd's she was also exposed to cyber insurance through her role in co-ordinating internal cyber insurance meetings.

In addition to her corporate and international experience, Rachel seeks to strive for academic excellence. Resultantly, Rachel has undertaken a PhD thesis in designing a natural catastrophe insurance scheme for Australia. Her PhD manuscript is currently under examination.

## **5. CAN INSURANCE EVOLVE TO MEET THE NEW TERROR THREAT?**

France. Belgium. Turkey. Germany. France again...

Terror activity intensity has increased in the past year across Europe, and while we can hope for a reprieve, all indications are that the problem could worsen in the coming months. Absent a change in the trend, we can better prepare ourselves for active assailant and other terror attacks. For the insurance industry, that means developing and distributing broader cover that directly addresses the need for economic recovery from an event with minimal physical damage.

## THE EVOLVING TERROR ENVIRONMENT

Within a period of one week, Europe saw an attempted coup d'état in Turkey, a truck bomb in Nice, and two attacks in Germany. Wielding an axe on a train in Würzburg, one assailant injured 18 people. Roughly a week later, a suicide bombing at a music festival in Ansbach injured 15 people, making it the first Islamist extremist suicide bombing to take place in Germany. Meanwhile, the coup attempt in Turkey resulted in more than 250 fatalities, and in Nice, 87 were left dead. In these cases—like most terror events of the past few years—physical damage was minimal, resulting in little impact to the global insurance and reinsurance industry. A cursory look at the data shows just how the threat has evolved in Europe. Excluding Turkey, Verisk Maplecroft reports approximately 40 terror events, resulting in more than 250 fatalities and more than 850 casualties for the 12-month period ending July 2016. A 68 percent decline in frequency from the prior 12-month period didn't provide relief from aggregate magnitude, however. Fatalities surged from just over 30 in the same period a year prior, with casualties up from nearly 90.

Anthony Canale, Vice President, Verisk Crime Analytics and a former Chief of Police, says, 'Soft targets remain the norm. From Ataturk Airport in Istanbul to the Bastille Day festivities in Nice to the Munich shopping mall, terrorists are striking areas that are frequented by the public and notoriously difficult to secure against a planned, coordinated small arms attack'. The recent events in Germany also reflect the changing norm of attacks on 'soft targets': public transport, shopping centers, and a restaurant.

Canale also notes a similar threat in the United States and believes that school boards, in particular, should be concerned. 'Municipalities face a unique threat in that many public structures are designed, not surprisingly, for public use. By definition, that makes them soft targets'. He continues, 'More than any other organization, municipalities and other levels of government exist specifically to serve their citizens and need to be able to invest in measures to return a community to normal as quickly as possible. The need for a swift recovery paired with the softness of potential targets makes effective post-event financing crucial to any public sector emergency management plan'.

Tom Johansmeyer, Assistant Vice President, PCS Strategy and Development, highlights, 'Reality dictates a need for changes in the insurance situation (as per the insurance products offered). There's been a maintenance of the status quo in relation to terrorism insurance product offerings, whilst other areas of the insurance industry are embracing innovation. Why is innovation not incorporated into terrorism insurance to diversify the products offered and the limits available for cover'?

He continues, 'Although there are inherent challenges, expanding terrorism insurance should be seen as an opportunity for the insurance and reinsurance industry. Primary insurers and capacity providers may start to deal more directly with original insureds to develop solutions to the evolving terror threat. Some activity has occurred in this space this year, particularly with "active assailant" cover to address attacks like the one that occurred in San Bernardino in December 2015. But more still needs to be done'.

According to Johansmeyer, the soft target issue extends naturally into the private sector as well. 'While the obligations of businesses are different from those of government bodies, many of the underlying issues are the same. Customers and shareholders may expect—or even need—a business to resume some degree of operations quickly after a terror event and then return to normal as soon as possible. A hospital is a great example. After an event, it may immediately

be focused on serving the critically injured from an attack, but at some point, it will need to be able to deliver its full range of services to the community. Grocery stores will need to open so customers can feed their families. The sorts of attacks we're seeing this year are particularly difficult, because they have the potential to disrupt a business or a community but are not easily hedged based on the existing structure of the global insurance and reinsurance market'.

The threat is salient and well known. The challenge is action. The global insurance and reinsurance industry remains focused on providing protection for major property losses, such as the terror attacks of September 11, 2001. While it's prudent to consider the implications of such activity on balance sheets, there's a clear need for a different form of cover - one designed to hedge economic losses from smaller events that yield little or no property damage. In addition to fulfilling a societal need - part of the global insurance industry's mission - a cover designed to meet the needs of original insureds facing the current terror threat would provide new opportunities to deploy capital and meet the needs of shareholders worldwide.

### **TRADITIONAL INSURANCE: ONLY PART OF THE ANSWER**

A terror event is a loss event. The question is really just one of who ultimately bears the loss - because somebody always does. If the original insured is covered for terror, and the nature of the event is consistent with the policy, then of course the insurance carrier bears the loss. Based on the size of the loss, it could have reinsurance or retrocessional implications. If there's an active shooter situation, though, an original insured that doesn't have active assailant protection pushes any losses to the shareholders that are forced to absorb them - a prospect not viewed favourably by corporate boards of directors. The problem is that it's difficult for boards and risk managers to take effective hedging action given the nature of the terror insurance and reinsurance market today.

According to Johansmeyer, "It's not uncommon to hear a reinsurance broker claim that he or she can find plenty of traditional capacity and thus doesn't need to turn to an industry loss index or parametric triggers. And there's no acute need to turn to the insurance-linked securities (ILS) market instead of relying on traditional reinsurance". To a certain extent, this is true, but it comes with constraints. If a cedent is looking for a certain type of cover that doesn't fit how terror is normally written, alternative structures and sources of capital become more important.

And underlying the entire market is the fact that the covers available tend to align with demand in the industry. After all, it doesn't make sense to design and market a product that nobody wants. Demand seems to be focused squarely on the major property loss events with the potential to impair insurer and reinsurer balance sheets. The 1993 World Trade Center bombing, Oklahoma City, and the terror attacks of September 11, 2001, come to mind. Canale says, 'Even before the shift to the active assailant model by terrorist organizations, the frequency of major attacks was low, but the consequences potentially severe'.

The industry's bias toward physical damage has translated to very low levels of insured loss from terror events, despite the increase in frequency. And the prevalence of smaller, nimbler attacks means the prospect of insured losses under the current industry model is becoming even more remote.

Canale reminds us about the human elements of terrorism and that the ability of the 'global insurance and reinsurance industry has the capacity to make a real difference to individuals, communities, and business. If the global insurance and reinsurance industry really wants to



make a difference, the industry needs to think about what happens at the most fundamental of levels’.

A more flexible and relevant approach to terror insurance protection could serve several purposes. In addition to providing a broader service to original insureds to help them recover post-event (addressing the industry’s societal purpose), broader terror cover could translate to greater opportunities for profitable growth. For this to happen, the insurance industry will need to expand significantly in relation to how it approaches the terror threat.

## **PARAMETRICS: A MORE EFFECTIVE WAY TO COVER TERROR**

Traditional insurance thinking ostensibly focuses on making the insured whole. The purpose of a policy (or a reinsurance treaty) is to compensate the claimant fully within the terms of the policy relative to the underlying loss. In practice, this usually means focusing on the value lost and delivering a payment tied as closely as possible to it. If a motor claimant has a £2,000 bent metal claim, based on the policy, he should receive £2,000 (less any deductible). While there is a place for this type of insurance in terror, an insured may have more urgent needs that have to be addressed differently.

Let’s consider a commercial insurance customer that has a policy that includes acts of terrorism. An event occurs, causing little physical damage but considerable business interruption. And let’s even assume that the policy is tailored to address economic loss rather than property damage. Terror events can be complex, requiring time and expertise to handle a claim. It could take months (or longer) for appropriate compensation to be determined. Since the insured would ultimately receive a fair and accurate payment, one would think the whole process worked.

In many cases, that may not be true.

Immediately following a terror event, a commercial insured will have to focus on resuming even limited operations as quickly as possible, with the next step being a subsequent return to normal operations as quickly as possible. Doing so requires capital, and its use may not be as straightforward as it would be in a physical damage scenario. For the latter, the insured would use funds from the claim payment to repair the structure.

Business interruption is different. Following a terror event, the insured may need to invest in helping the staff cope with the trauma of the event, increasing security, and advertising and marketing (including crisis communications) to help reassure its customer base that the business is safe, operational, and ready for the public to come back. Action of this sort has to occur quickly. Trying to reassure the public six months after the fact may be too late.

The traditional insurance mechanism may not be a great fit for immediate post-event financing, but alternatives do exist. In fact, the terror market can look to the natural catastrophe space for a solution—specifically, parametrics. Parametric protection uses the magnitude of the event rather than the size of the loss as the trigger for payment. It can be fast, straightforward, and highly effective.

For terror, a parametric policy or industry loss warranty (ILW) would be relatively easy to structure. As an independent reporting agency, Verisk Maplecroft provides data on

approximately 30 attributes for each terror event and has more than 130,000 events in its database, going back to 2004.

According to Johansmeyer, ‘The simplest approach would be to trigger on a stated number of fatalities or casualties. You could refine the trigger by specifying locations, perpetrator groups, or incident types. And you could build in exclusions like hoax, CBRN, or kidnap. For aggregate covers, a “fatality franchise” would work—for example, only events with at least 100 fatalities count toward the aggregate for the coverage period—in addition to using hours clauses to tie together separate events by the same perpetrator group in a coordinated, multiple-location attack’.

With the ability to determine the magnitude quickly—as long as a reliable independent reporting agent is in place—parametric triggers are uniquely capable of delivering an answer well before a traditional commercial insurance claim is sorted out. As a result, the insured would have access to a source of emergency capital that could be used to help quickly recover the business, handle the crisis, and more easily guide the staff and operation back to normal.

## A UNIQUE OPPORTUNITY

Innovation can be difficult, especially the part that involves willingness to change. For the insurance industry to adapt to the latest iteration of the global terrorist threat, however, the necessary components already exist. They’ve even been tested. Active assailant programs are being introduced and marketed to original insureds, and as they’re adopted, the cover will create opportunity all along the global risk and capital supply chain. Parametrics have been in use for years in property catastrophe, and they’re beginning to enter the terrorism sector. What’s missing is scale.

Johansmeyer says, ‘Original risk begins with the original insured. While terrorism does present a variety of pricing and modelling challenges, the people of our industry will find ways to address them. Distribution is the greater obstacle to adoption, although that could become easier with the frequency of terror events the world has seen in the past two years. As new terror insurance products come into the market, the insurance industry will need to communicate the benefits of the cover and ensure that it addresses the concern of boards of directors and shareholders’.

The insurance industry needs new ways to grow, and corporate insureds need a new form of protection. Terror insurance could solve both problems - but not if traditional thinking prevails.



**Anthony Canale**  
**VP (Crime Analytics and CargoNet)**  
**Verisk**

[www.linkedin.com/in/anthony-canale-39a1748](http://www.linkedin.com/in/anthony-canale-39a1748)

Tony Canale, Vice President, runs Verisk Crime Analytics and CargoNet for Verisk Insurance Solutions. He has more than 33 years of experience in law enforcement at the federal, state, and local levels. During his career he supervised numerous national and international high profile cases and spent nine years working as a supervisor of an FBI/DEA joint organized crime and drug task force focusing on national security matters.





**Roger Davies, MBE, QGM**  
**Co-Founder & Director**  
**IMSL**

[www.linkedin.com/in/roger-davies-0324361b](http://www.linkedin.com/in/roger-davies-0324361b)

Roger is a former British Army Counter-Terrorist professional, decorated for his services in countering IEDs. He has briefed the United States House Armed Services Committee on future trends in terrorism and has provided specialised threat analysis support to governments and the insurance industry for the last 16 years. He has been involved in both developing terrorist incident insurance models and conducting PML studies, and advising companies on security measures. He is a member of the United Nations Centre for Counter-Terrorism List of Expert and has advised a number of nations on national response issues, specialising in threat-based procedural development. Mr Davies blogs on such issues, and others on [www.standingwellback.com](http://www.standingwellback.com). Mr Davies is a founder and director of IMSL ([www.intelmsl.com](http://www.intelmsl.com)) which currently provides terrorism threat analyses and associated data to a number of governments, industry and insurance providers.

## 6. DRONES & TERRORISM

### EXECUTIVE SUMMARY

*The rapid technological development, and wide use of Unmanned Aerial Systems (UAS) or drones is already associated with an increasing occurrence of their use for malicious purposes. With limited investment and minimal innovation, groups with nefarious intent are able to use drones to gather information, and to deploy payloads very accurately and quickly. Ultimately, these payloads could include improvised explosive devices or hazardous substances. Whilst the technology and systems to mitigate the risks are developing, they are not currently widely available or deployed routinely. From an insurance perspective, the scale of explosive device that might be deployed by a drone is comparatively small compared to most Realistic Disaster Scenarios (RDS), however, the ability to deploy a device in three dimensions to a specific, vulnerable location, at speed, could be problematic. Equally, the non-damage Business Interruption (BI) implications are potentially significant - even when no actual explosive device is employed. Perhaps most concerning, the scenarios related to a chemical, biological or radiological scenario are troubling as they move from a point, surface release to a much more complex dynamic dispersal at height. Beyond considerations for insuring the legitimate use of Unmanned Aerial Systems, the industry may need to consider in detail the coverage implications of this relatively new threat, and if necessary consider what guidance might be provided to clients about sensible counter measures.*

*Throughout this paper I will use the term “drones” and Unmanned Aerial Systems (UAS), interchangeably.*

### HISTORICAL CONTEXT

The use of Unmanned Aerial Systems (UAS) to strike terror in populations or conduct acts of terrorism, war or sabotage may feel like a new meme, a new concept. But as with many terrorist techniques, history teaches us that what we see as “new”, isn’t new at all.

On August the 22<sup>nd</sup>, 1849, Austrian forces laying siege to the city of Venice carefully fitted explosive charges to 200 unmanned aerial systems. These balloons were released from an

offshore platform for the wind to carry them over the city. Each balloon carried a bomb, a pear-shaped vessel filled with gunpowder. The designer, Austrian artillery officer Franz von Uchatius, was able to “program” the balloon flight by releasing smaller balloons which enabled him to calculate wind speed and direction. The bombs were dropped after 23 minutes by an ingenious burning fuse mechanism.

In World War Two, balloon devices were used by both the British, who sent balloons trailing long bare wires to short circuit German power lines, and the Japanese who sent high altitude balloons driven by the jet stream all the way across the Pacific to drop incendiaries onto North American forests.

With somewhat more proactive control systems than the use of the wind, Nazi Germany employed radio controlled guided bombs designated the “Fritz X”. British sailors are reported as expressing surprise as a high altitude aircraft was seen dropping bombs some miles away, then seeing the bombs track towards them in a manner that was quite unexpected. Later the Henschel HS-293 remotely controlled glide bomb with a range of about 9 miles was used to attack Allied shipping.

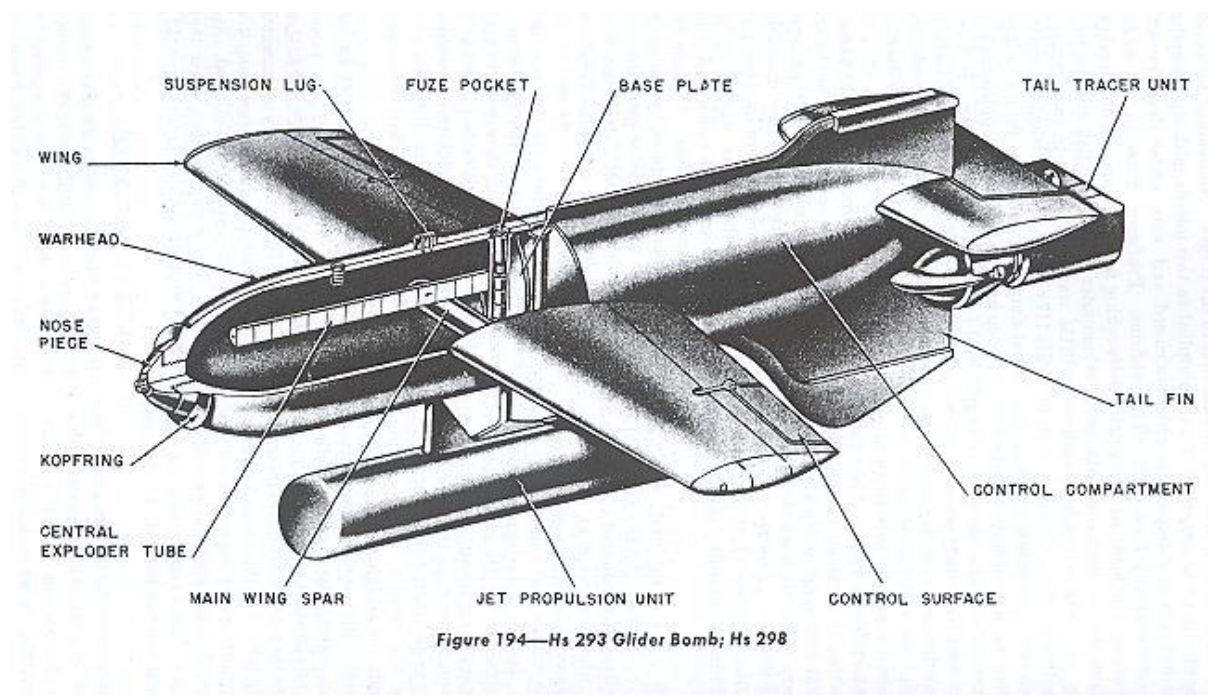


Figure 194—Hs 293 Glider Bomb; Hs 298

*Figure 1 Henschel HS-293 remote controlled glide bomb. Image from [https://en.wikipedia.org/wiki/HMT\\_Rohna#/media/File:Henschel\\_HS\\_293.jpg](https://en.wikipedia.org/wiki/HMT_Rohna#/media/File:Henschel_HS_293.jpg) - Public Domain*

On a larger scale USAAF and the US Navy under “Operation Aphrodite” used remotely piloted B17 and PB4Y bombers as precision guided munitions against hardened enemy facilities such as U-boat pens and V weapon launch sites. Typically, the aircraft were stripped of all unnecessary systems and loaded with a huge amount of explosives. They had a human pilot and flight engineer who “bailed out” after take-off and the plane was fitted with TV cameras and a radio control system, controlled from a nearby aircraft.<sup>1</sup>

<sup>1</sup> [https://en.wikipedia.org/wiki/Operation\\_Aphrodite](https://en.wikipedia.org/wiki/Operation_Aphrodite)

## **WHY DRONES?**

Before examining modern applications of Unmanned Aerial Systems it is worth examining what the ‘drivers’ of their use were and are. There are a number of aspects:

- Weapons systems approaching from the air are likely to avoid static, two dimensional or ground based defence and security measures. In crude terms by using “three dimensions” they can avoid ground based defensive measures.
- They can be launched from some distance away from an area fully in the control of the user.
- By being “unmanned” the risk that a pilot may be killed or injured is taken away – this has two effects – it makes attacks somewhat more efficient and the challenge of finding a pilot willing to risk or sacrifice his life is negated.
- Modern technology allows highly accurate, speedy insertion of a hazard that can outface or avoid security responses. Such an attack becomes more efficient and likely to succeed from a terrorist perspective. Accuracy may enable the quantity or explosive to be reduced increasing penetrative ability of a drone into a secured area.
- All these systems have inherent “surprise” within them, a key military principle.
- Today, the technology is widely available, as are third party adaptations described in the internet, creating very low “barrier to entry”.
- Modern UAS control systems require little training and can be operated by just about anyone.
- Drones therefore are a “low risk” tactical and operational tool for achieving significant potentially strategic advantage.

These factors are worth bearing in mind as we examine the threat posed by modern drones.

## **TECHNOLOGICAL DEVELOPMENTS**

Several developments in technology have now further enabled modern drones or Unmanned Aerial Systems and they provide opportunities for terrorists and challenges to security. These developments include:

- Control technology has advanced considerably. As an example, 20 years ago the British Army examined the utility of “remote control helicopters” for use as a reconnaissance vehicle in support of hazardous bomb disposal operations, but after investigation discarded the effort because of the challenges of training pilots. Essentially 20 years ago one required the same skills to fly a remote controlled helicopter as one did to fly a full-blown helicopter. Modern technology has automated much of the “skill” component in using such a system.
- First Person View (FPV) technology adds further to the potential ability of a controller to seek out and deploy a payload to a target, avoiding obstacles in real time.
- Communications infrastructure available to the public (such as 4G) can be used and exploited by drone users to control drones which may have advantages over the use of more-common ISM band control frequencies.
- Multi-rotor technology has advanced with quad- or octo-systems providing steady, easily controlled platforms.
- Collision avoidance technology is now feeding through to commercially available drones, as are navigation systems such as GPS controlled waypoints and “return to launch” capabilities. “Default to hover” technology which automatically makes the

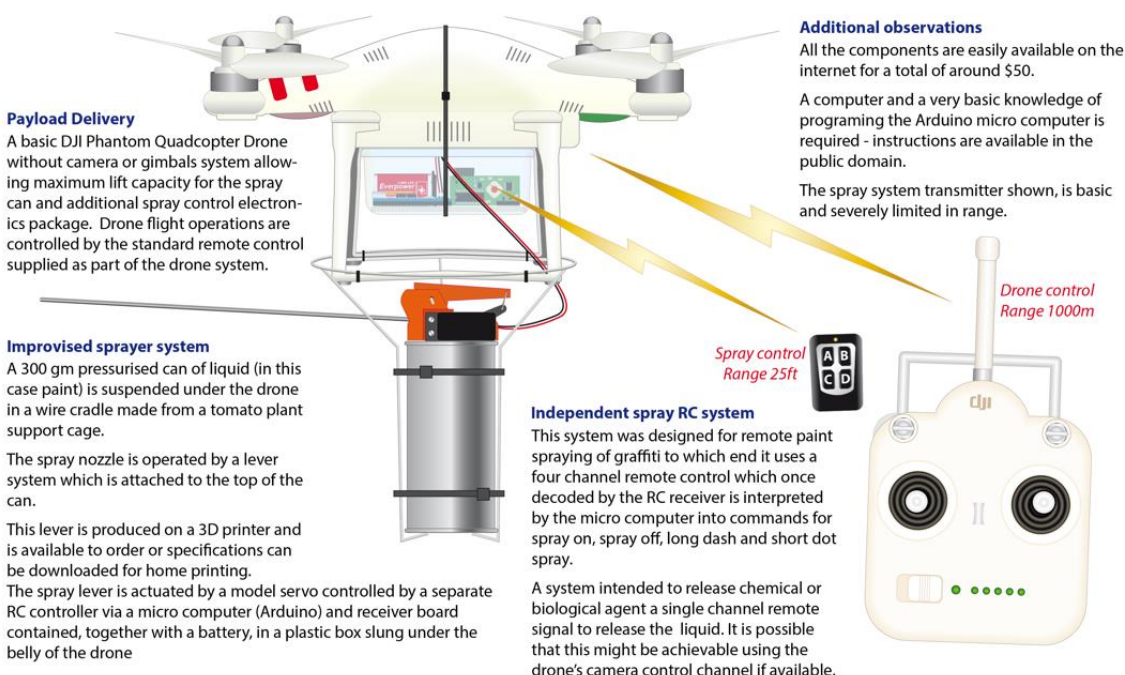
drone hover if hands are taken from the controls was frankly unheard of just a few years ago.

- “Follow me” technology also as the potential to be used for nefarious purposes.
- Battery technology can now provide significant flight duration, and video technology can transmit HD quality video from the drone, aiding piloting, or simply making drones with a greater payload capability.
- Materials are now lighter, and tougher, and cheaper, making drones with more payload and more affordable.
- Modern systems utilise and optimise a range of RF technology that is now cheap and freely available, and indeed utilise commonly available systems such as smart phones and tablets as control systems.
- Internet communication has enabled the easy transfer of third party “add-on” technology to a range of commercial drones. Easily available instructions such as add on aerosol release mechanisms can be downloaded by anybody, anywhere in the world.
- Some specialised drones have ‘useful’ payload release mechanisms or additional circuitry that can be used for nefarious purposes. Drones used for cinematography and crop dusting (spraying) provide just two examples.
- The speed of commercially available drones is increasing, making them faster and more difficult to interdict.
- Swarm control systems are now coming to market allowing users to control multiple drones safely and easily at the same time.
- The size of effective drones has decreased making them more difficult to detect by systems such as radar.
- Cost of these systems have dropped and are globally available. The cost is now so low that the market for drones is now huge and millions are expected to be sold in coming years.
- The legal system is struggling to “catch up” with technology to impose appropriate controls



### UAV (DJI Phantom Drone) Adapted to spray liquid (paint)

From information published in the public domain.



Not to scale - colours and details may be changed for the purposes of illustration

WTP#1023a Feb 2016

© Image reproduced by kind permission of IMSL

## IMPLICATIONS TO THE TERRORIST

The implications of all of the above to the terrorist are as follows:

1. UAS or drones can be purchased easily, anywhere, by anyone for a small amount of money. It will be very difficult to prevent terrorist access to this technology.
2. Drones can easily be adapted for nefarious purposes with little engineering skills required.
3. Drones can be used to insert a hazard at great speed, in three dimensions. Given that one of the key aspects of counter-terrorist security measures is the principle of establishing a secure perimeter, within which a search has removed any hazards, drones can circumvent that basic security measure.
4. The accuracy of the drone in terms of piloting means that targets not previously considered vulnerable even to significant terrorist weaponry are now vulnerable. A drone can approach a critical component or a key person, at high speed in three dimensions, and even enter a building in some circumstances.
5. The piloting skills are minimal, and the range of the system can place the pilot easily outside secured areas.
6. Payloads are still relatively small, but given the ability to place a hazard at very close proximity to a target, this is perhaps less of an issue.
7. Swarms can overwhelm a number of counter measures.
8. A UAS also offers a terrorist a cheap and effective reconnaissance and propaganda tool. A UAS can also carry cyber attack payloads, inserting, say, a spoof wifi point deep within a target area where one might not be expected.

## EXAMPLES OF TERRORIST USE OR SIMILAR INDICATIVE USE OF DRONES

In many ways the issue posed by drones is already extant. Terrorists are using drones today, in Syria and Iraq, albeit for reconnaissance and propaganda, but one cannot imagine that the ingenuity with which terrorists are addressing other weapon systems in the region won't be applied to drones and there are unverified instances of explosives having been incorporated into fixed-wing drones. Indeed the British Prime Minister warned that terrorists have already tried to obtain crop spraying drones for the purpose of spreading radiological material.<sup>2</sup>

Some specific examples of terrorists or other groups using commercial-off-the-shelf for violent purposes include:

- Ukrainian forces using a commercial drone to drop grenades.<sup>3</sup>
- Numerous examples of ISIS/Daesh and al-Nusra using drones to film attacks in Syria and Iraq. Footage is posted almost daily indicating a high degree of expertise. Most frequently used appear to be COTS DJI drones.
- Hezbollah using a range of drones to fly reconnaissance missions over Israel. Some of these missions appeared to also have a specific purpose to incite terror in the population.<sup>4</sup>
- Reports of a significant Hamas drone capability under development.<sup>5</sup>
- In 2011 the FBI arrested a man planning to fly explosively laden model aircraft into the pentagon and US Capitol, to be initiated by a mobile phone signal.<sup>6</sup>
- Recent reports from Hong Kong suggest protestors were planning to use a drone to disrupt the visit of Chinese leader Zhang Dejiang.<sup>7</sup>
- Delivery of radioactive material to Japanese Prime Minister's office building.<sup>8</sup>

---

<sup>2</sup><http://www.foxnews.com/world/2016/04/02/cameron-warns-isis-could-use-drones-to-spray-nuclear-material-over-western-cities.html>.

<sup>3</sup> <http://tass.ru/en/world/863417>

<sup>4</sup> <https://fas.org/wp-content/uploads/2014/06/Hezbollah-Drones-Spring-2014.pdf>

<sup>5</sup> <http://www.bloomberg.com/news/articles/2014-07-16/hamas-bragging-rights-grow-with-drones-use-against-israel>

<sup>6</sup> [http://remotecontrolproject.org/wp-content/uploads/2016/01/Hostile-use-of-drones-report\\_open-briefing.pdf](http://remotecontrolproject.org/wp-content/uploads/2016/01/Hostile-use-of-drones-report_open-briefing.pdf)

<sup>7</sup> <http://www.scmp.com/news/hong-kong/law-crime/article/1946061/hong-kong-police-plan-jam-drones-during-china-state-leader>

<sup>8</sup> <https://www.theguardian.com/world/2015/apr/22/drone-with-radiation-sign-lands-on-roof-of-japanese-prime-ministers-office>



*Figure 2. Syrian rebel drone propaganda footage of an explosion in Aleppo. Note too the artillery projectile that by chance was by chance caught by the drone camera. Screen shot from Al Nusra released video at <https://youtu.be/jcbsJtcxvhM>.*

## IMPLICATIONS TO

## SECURITY MEASURES

Security measures are impacted by the capabilities of drones in a number of ways. These include:

1. There is a need to think somewhat differently about three dimensional security. While many targets could have been attacked by terrorist mortars or rockets in “three dimensions”, the potential accuracy of a drone delivered hazard demands a rethink. Drones can enter buildings through open doors or windows, manoeuvre, and can be placed within inches of a vulnerable target, controlled from great range.
2. Drones can be relatively stealthy. The drone that landed last year on the Japanese Prime minister’s roof carrying a payload of alleged radio-active material was discovered only by chance some days later. Other drones have “crashed” on prison roofs delivering contraband and not been discovered for some time.
3. As well as providing complex threats, drones also provide a simple hazard if control is lost and they fall on people underneath them – security measures need to bear that in mind – causing a drone even without a payload to crash can kill people – and the wide availability of drones will mean even the foolish may have the opportunity to fly what has been described as “an airborne lawn mower” over crowds of people. So mitigation systems that offer the ability to take control and land drones are preferable over those that simply cause drones to fall from the sky.
4. Secure perimeters surrounding a positively cleared sanitised area, may not remain so. A drone can deploy a hazard to the area after it is secured.
5. Technology continues to advance rapidly – the threat posed by drones is and will remain highly dynamic in nature. The ingenuity of third party drone adaptations will reinforce that.
6. The legality of establishing certain drone counter-measures has yet to be tested.
7. Drones pose other security threats beyond terrorism – protection from cyber threats – such as a drone flying a Wi-Fi access point into a secure area, or filming sensitive activities or filming sports events for which TV rights belong elsewhere all pose challenges.
8. The presence of a drone will not always equate to a threat. Drone use for legitimate purposes is likely to mushroom in coming years such that there may well be many legitimate drones in the air near a secured facility. Separating threat drones from legitimate drones will be a challenge and may pose a Business Interruption (BI) threat.
9. Drone threat response plans need to be flexible and integrated both with other security measures and any counter-drone solution. Some counter-drone solutions are not holistic and only answer part of the question.
10. Security measures will need to be compliant with local regulations and legal structures. Some measures will need appropriate authorisation which will need to be balanced with the potential of a drone threat being detected say at 250m, and being immediately

adjacent to a vulnerable target seconds later, 24/7. Drones pose very fast challenges to security responses and will demand speed of decision making. There may be little time for formal, slow time authorisations and so pre-authorisation of certain security measures may need to be in place.

11. The drone threat can be highly dynamic. Let us say a drone lands in facility adjacent to vulnerable component "X". A security plan might be implemented, an evacuated cordon put in place and a command post established... only for the drone, within seconds to "relocate" to vulnerable point "Y" or even to an evacuation point elsewhere in the facility. Theoretically a drone can chase crowds evacuated from a building causing significant panic. Most hazards detected in a secure facility will remain stationary and most security plans assume that – a drone might not, requiring much more agile security plans. A key requirement of counter-drone systems will be to maintain the mitigation effect until such time as the threat is otherwise immobilised.
12. Threat drones used by terrorists or criminals naturally will hold significant forensic intelligence value and security plans should recognise that.
13. It may be difficult to establish the nature of any hazard from payloads. In essence they should be treated like a Radio Controlled IED until such time as the proper authorities have mounted their response.
14. There may be significant challenges from false alarms. A drone such as the one illustrated above with an aerosol can may be designed to simply be a tool for exotic graffiti. But such a drone seen on say Whitehall, or Pennsylvania Avenue, or by L'Arc de Triomphe will likely cause significant disruption until it can be proven to not be hazardous.
15. Swarms of drones need to be considered. Technology to control swarms of drones is already available and counter-drone systems need to be capable of responding to a number of drones at the same time.
16. In some circumstances, a counter-drone system can provide an effective deterrent measure. In this sense, the drone threat and counter-measure situation is unusual. There is no counter-measure that can prevent a shooting completely or a rocket or mortar attack. But the more effective counter-drone systems can mitigate certain drone attacks completely.

## **DRONE COUNTER-MEASURES.**

Just as the market for drones is increasing so too is the market for drone counter measures. It is not the purpose of this article to recommend one or other of the available or soon-to-be-available counter measures. But the following may be considerations:

1. There will be one or more elements to a counter-drone system, that might include:
  - a. Detection
  - b. Alarm
  - c. Identification
  - d. Categorising as a threat
  - e. Tracking
  - f. Mitigating/Active measures

For counter-drone systems that do not offer all of the above, then consideration needs to be addressed to the others in a coherent plan.

2. Depending on the nature of the secured area or potential target for threat drones, there may or may not be a need for a 24/7 capability, and by implication, operations in the dark.
3. Some systems may be automated, some will require man-in-the-loop.



4. Some measures may require appropriate authorisation. “Jammers” may not be legal in certain jurisdictions.
5. “Jammers” which cause a drone to land or crash wherever it is at that moment in time may complicate matters further. In those circumstances more advanced systems that take control of the threat drone and enable it to be landed in a pre-designated safe zone may have attractions.
6. Some counter- measures can deal with “swarms” of threat drones others cannot.
7. Some require line of sight, others do not.
8. Some cannot operate at night, others can.
9. Some require minutes or more to deploy an active counter measure, others can do it at speed.

## **IMPLICATIONS TO THE INSURANCE INDUSTRY**

Drones represent a new terrorist attack vector, which as yet is not being fully modelled. Some potential implications for insurers include:

- Conventional Terrorism Realistic Disaster Scenarios (RDS). Compared to existing explosive scenarios that are run to determine property damage and business interruption assessments, the size of device that might be deployed by a drone is small. However, the ability to deploy to a very specific location needs to be considered in detail for a range of asset types. There is probably limited implication for large urban structures, but it will be prudent to consider RDS implications for energy, power, aviation, communications technology and media carefully.

- Conventional Terrorism Business Interruption (BI) issues. The wide availability and difficulty in effectively countering the use of drones, points towards the potential for them to be used to create fear. Whether or not a payload creates property damage, there are a range of scenarios, particularly in urban environments where significant non-damage business interruption might be generated. These scenarios should be considered in detail to determine whether existing non-damage BI extensions are likely to apply.

- CBR RDS. Most existing RDS with regards to chemical, biological and radiological scenarios are based on a point release at ground level. There will need to be a reconsideration of these RDS to include the potential for a complex, dynamic dispersal at height which has the potential to significantly expand a hazardous area.

- Terror/PV exclusions or extensions. Depending on the possible portfolio impacts of a range of UAS scenarios, it may be appropriate to consider providing guidance to clients in specific sectors on the kinds of mitigation that are considered reasonable. There is also clear potential for insurers and the more effective counter-drone system providers to offer a synergistic solution.

- Specific UAS insurance. It is understood that a market for the legitimate use of UAS already exists. There may be a requirement to include potential liability risks associated with use being confused for an attack. As suggested earlier, the potential BI implications are significant. Also, the telemetry available from a drone may also allow insurers who insure a drone operator to examine the actual commands sent to the drone in the event of a claim.



**Laurent Montador**  
**Deputy CEO**  
**CCR**

[www.linkedin.com/in/laurent-montador-3b41688](http://www.linkedin.com/in/laurent-montador-3b41688)

Laurent graduated from University Pierre and Marie Curie and University Paris Dauphine.

Laurent has more than 25 years of experience in the insurance and reinsurance fields. He has held management positions in various roles within both Actuarial Management and Underwriting Management. The management positions Laurent successfully held were in companies including BNP Paribas, AXA Re, Transatlantic Re and Flagstone Re.

He sits on several boards, including HCFDC (French High Committee for Civil Defence), GAREAT (French terror pool), GAREX (marine risks), and chairs the board of Caissrelux (a CCR captive).

## **7. TERRORISM, A NECESSARY PUBLIC-PRIVATE PARTNERSHIP**

*CCR is a public-sector reinsurer serving the general interest by providing insurers operating in France with coverage against exceptional risks. Since 1983, CCR is accredited to cover property damage resulting from acts of terrorism with the guarantee of the French State. In this framework, CCR has focused its efforts toward improving its understanding of risks – in particular by collecting detailed data and developing fine-scale models of phenomena – in order to actively contribute to industry discussions. The events of the year 2015 shed light on new issues involving insurance coverage, in terms of both property damage and bodily injury. With regard to this new context, it appears necessary to consider possible changes to our existing systems, in order to ensure their sustainability.*

### **THE ROLE OF THE STATE**

The present geopolitical context, marked by conflicts in the Middle East and in sub-Saharan Africa as well as the threat of terrorism that plagues western countries, requires these states to ensure the security of their citizens and provide compensation for damages that may arise. As underscored by the Association of Reinsurance Professionals in France (*APREF*) in its 2012 white paper: "The insurance and reinsurance of terrorism on the principal markets requires the intervention of the states. It is the states who oversee foreign policy and internal security and who are the principal parties in the prevention of terrorism risk, hence their required implication. They (either severally or individually) also have the financial capacity to provide protection against a market's exposure to a major NBCR (Nuclear, Biological, Chemical or Radiological) loss."

In (re)insurance, as emphasised by Michel-Kerjan (2010), "terrorism" risk is quite different from natural risk. Admittedly, it belongs to the category of so-called "Cat" risks, i.e. risks that, by their nature, can generate either several individual major losses, or a large number of smaller losses, with in both cases numerous victims and very high economic costs. Yet one of the principal characteristics that distinguishes terrorism risk is based on the fact that "the

probability of the occurrence of an attack remains intrinsically much more uncertain and ambiguous than that of a natural catastrophe"<sup>9</sup>. Because these aspects are difficult to grasp and despite the differences in their scope, the various coverage schemes implemented in Europe provide for, at one point or another, the use of public intervention (see Table 1).

*Table 1: Principal European coverage schemes that make use of public intervention*

<b>Name</b>	<b>Consortio</b>	<b>Pool Re</b>	<b>Extremus AG</b>	<b>Gareat</b>
<b>Country</b>	Spain	United Kingdom	Germany	France
<b>Inception</b>	1954	1993	2002	2002
<b>Characteristics</b>	Oldest insurance system covering terrorism	Implemented after the terrorist attacks of 1993	Implemented in the wake of the September 11, 2001 terrorist attacks	Implemented in the wake of the September 11, 2001 terrorist attacks
<b>Mechanism</b>	The Consortio is a public insurance body in which participate all insurance companies	The pool acts as a reinsurer and is covered by the government	Insurance company with the backing of the Federal State	The scheme ensures the pooling of major risks and its members benefit from CCR's unlimited guarantee which is backed by the French State
<b>Compulsory cover</b>	Yes	No	No	Yes

These different examples illustrate that the characteristics inherent in terrorism risk have led several countries to combine private and public resources when building their compensation schemes. In the name of national solidarity, France has adopted this policy since the State seeks to strengthen the resilience of its citizens, of its economic stakeholders and of its institutions. CCR participates in industry discussions with the French Treasury Department and the related professional entities while remaining aware of the needs of the market and striving to establish a balanced financial architecture that will provide a sustainable solution in accordance with the demands of the State. The latter is also a stakeholder in a bodily injury compensation scheme, via a guaranty fund (the *FGTI*<sup>10</sup>) that coexists with other contingency instruments including the property damage compensation scheme. For these compensation schemes, CCR is accredited to provide public reinsurance for small and medium risks (capital of less than € 20 million) upon the request of any insurer and for large risks (capital in excess of € 20 million) through GAREAT (French terrorism insurance pool). This reinsurance therefore enables CCR to provide unlimited coverage of losses.

The emergence of new forms of terrorism and the perspective of new types of risks combined with the acute development of genuine technical capabilities of new terrorist groups, such as

<sup>9</sup> Michel-Kerjan, see bibliography.

<sup>10</sup> *FGTI*: Guaranty fund for the victims of terrorism and other offenses.

cyber-terrorism or the development of chemical weapons, serve to emphasize the necessity of involving both public and private stakeholders in the establishment of compensation mechanisms. The latest events occurring throughout the globe demonstrate that there is a high level of human risk involved but also substantial indirect economic impacts such as business interruption, decontamination costs, the cost of clearance operations and of contingent liability, and cyber-terrorism, to name a few.

France was severely affected in 2015, with Charlie Hebdo attack the 7<sup>th</sup> of January, Hyper casher attack the 9<sup>th</sup> of January and November 2015 Paris attacks near the Stade de France and at the Bataclan Theater.

Concerning the November terrorist attacks, the amount of compensation provided to the victims may reach €350 million, with 2 800 reported claims at the 29<sup>th</sup> March, 2016 and potentially a ultimate number of claims near 4 000<sup>11</sup>. The indirect repercussions on the country's economy with the forced inactivity of several areas of the capital, a drop in the activity of restaurants, a decline in the frequency of tourists to public places and fewer visitors are estimated to cost €2 billion<sup>12</sup>.

The latest developments of terrorism in the world in general (in Orlando in June 2016 or in Germany in July 2016) and in France specifically (in Nice the 14<sup>th</sup> of July and in Saint-Étienne-du-Rouvray in Normandy region the 26<sup>th</sup> of July), show that the entire population is exposed to its consequences. Acts of terrorism are no more located exclusively in Middle East or in the capitals of Europe but in every town, whatever their size. The entire population is exposed, regardless of its religious origins or its social status. Therefore, it is difficult to assess the vulnerability of populations or the exposure of different areas.

## RISK KNOWLEDGE EFFORTS

With a perspective to further discussions as to ways of adapting existing terrorism risk compensation schemes, modeling stands out today as a necessary tool. Over and above those acts of terrorism that directly provoke bodily injuries by the use of arms, improvised explosive devices are frequently used in terrorist operations. Thus, over 25,000 terrorist attacks were perpetrated in this manner since 2010 causing approximately 45,000 deaths and 105,000 wounded worldwide<sup>13</sup>.

Today, the use of NBCR weapons comprises one of the most feared scenarios. Due to the very small number of reports of this type of attack, we have only few examples to draw on. Among the most significant events, we may cite the sarin gas attack in the Tokyo subway in 1995 and the presence of a dirty bomb consisting of dynamite and caesium-137 in Izmaylovsky Park in Moscow the same year<sup>14</sup>. With the emergence of terrorist groups backed by considerable financial and human resources such as the Islamic State in Iraq and in Levant (ESIL – DAESH), experts agree that, today, the possibility of such an attack is real.

To fulfil its mission, CCR invests in modelling tools. Unlike natural disasters that encompass a variety of risks, terrorism is a specific risk which can at times be difficult to identify.

---

<sup>11</sup> *Les Echos* (in French), «Attentat de Nice: l'indemnisation des victimes mise à l'épreuve», electronic edition of July 16, 2016.

<sup>12</sup> *Le Figaro* (in French), "The terrorist attacks may cost the French economy two billion euros" electronic edition of November 25, 2015.

<sup>13</sup> START consortium database, University of Maryland, USA.

<sup>14</sup> French foundation for strategic research (*Fondation pour la recherche stratégique*).

Furthermore, the frequency of its occurrence fluctuates in conjunction with global geopolitical tensions. In addition of conventional terrorism (explosions and conflagrations), experts and intelligence officers agree that terrorist groups are intensifying their efforts to obtain and ultimately use NBCR-E type weapons (Nuclear, Biological, Chemical, Radiological and Explosives).

In this context, CCR has invested in the development of impact models for attacks of the type NBCR-E. If an NBCR-E act of terrorism is a credible threat, the specifics of such an attack (where? when? how?) are difficult to predict and make the development of a probabilistic model even more difficult. This type of model appears out of reach for the time being, as the conceptual challenges of formalism and mathematics render such an approach unreliable. Estimating the annual probability of such an event occurring by accurately quantifying the feasibility of an attack, the interest in striking a given target, the motivation of a terrorist and the worldwide geopolitical situation are just some of the challenges limiting our ability to generate a realistic probabilistic view of this risk. This being said, our modeling work has been oriented toward a deterministic approach taking into account a variety of parameters such as the position of the source device, the quantity of explosives, the nature of the dispersed NBCR substances and the meteorological conditions.

CCR thus developed a multivariate model providing a view of this risk, which goes beyond the simple deterministic approach and which lends weight, for any given scenario, to the costs generated by the modeling of many hundreds of deterministic calculations.

The model's design incorporates several modules:

- a potential target catalogue, such as embassies, top tourist attractions, places of worship, airports, train stations and industrial sites – in particular those with links to the petrochemical or nuclear industries;
- a hazard module, developed in partnership with the French Company ARIA Technologies, which draws on state-of-the-art scientific knowledge to:
  - assess the zone affected by the explosion blast,
  - calculate the geometry and mass distribution of the NBCR substances in the plume,
  - plot the course of a plume carrying NBCR substances, taking account of realistic meteorological conditions;
- a loss calculation module, combining hazards and human or financial risk exposures (geolocalized policies) while enabling loss evaluation.

Furthermore, in order to produce as realistic a model as possible, the hazard module takes into consideration the three-dimensional aspect of buildings as this has a significant effect on the dispersal of the contaminating plume. Indeed, buildings may act as a barrier to the flow of the plume, in this case the contaminating substances will affix themselves to the facades exposed to the wind, yet they may also temporarily accelerate the flow creating a vortex and modifying the contaminated area by spreading to the courtyards of buildings or to streets that lie perpendicular to the direction of the wind.

We have simulated the dispersal and contamination of persons and buildings located along a popular tourist Avenue (Champs Élysées, Paris, France) by a dirty bomb combining conventional explosives with radioactive material (see figure 1). This type of device may be easily improvised and transported in a simple backpack, the most difficult aspect would be to collect a sufficient amount of radioactive material. The effect of the blast is clearly visible at



the top of the Avenue. For the different radii, the model provides the excess pressure values to which are associated the irreversible damages to both humans and structures. Once the initial explosion has suspended the radioactive particles in the atmosphere, it is the meteorological conditions – and in particular the wind speed and direction – that will control the dispersal, the settlement and the contamination over the length of the plume. In the scenario we have illustrated, the wind blows gently from the northwest. These types of scenarios, sometimes called "hyper-terrorism" scenarios, may severely impact different insurance lines, generate several tens of billions of euros in losses and, over the long term, give rise to a chain reaction of losses: business interruption, loss of tourist revenues, etc.

Figure 3: Example of a hypothetical "dirty bomb" scenario at the top of the Champs-Élysées



Source: CCR.

## THE CHALLENGES OF TOMORROW

With regard to this new context and the discussions currently underway concerning damages to persons and property, it appears necessary to consider possible changes to our existing systems, in order to ensure their resilience.

### BODILY INJURY COVERAGE

Compensation for victims of terrorist attacks has been provided by a guaranty fund since 1986. The fund became the Guaranty Fund for the Victims of Terrorism and other Offenses (*Fond de Garantie des Victimes des Actes de Terrorismes et d'autres Infractions - FGTI*) following the extension of its missions in 1990. Based on the principle of national solidarity, this fund provided compensation to 4,000 victims of terrorist attacks amounting to € 106 million between 1985 and 2014. With the exception of the terrorist attacks of 1995 which cost the lives of 8 individuals and wounded 200, some severely, the essential portion of compensation was provided in respect of terrorist attacks that occurred outside French territory. The annual

resources of the fund are approximately €285 Million, but so far, compensations due to terrorism represented a small part of the overall amount of compensation.

The stigma left by the terrorist attacks of 2015 lead us to reconsider ways of ensuring the resilience of the compensation system for victims of terrorism. Indeed, since the terrorist attacks of November 2015, almost 4,100 claims have been handled by the *FGTI* – or as many as those processed since the fund's inception. In respect of 2015, the total amount of compensation is estimated at approximately €400 million. At this time, it is not possible to evaluate the compensations for attacks of July 2015, but it should be important with 84 deaths and 286 injured and hospitalized people.

This unprecedented situation requires strict cooperation between the *FGTI* and the different stakeholders, especially the actors from the insurance market. The guarantees to which the victims subscribe generally provide the right to compensation. As suggested in March 2015 by Nathalie Faussat, director of the *FGTI*, the amounts paid to the victims in respect of individual and group policies will be deducted from compensation<sup>15</sup>. In practice, distribution between the intervention of the fund and of life, accident and health policies appears difficult to discern and no doubt merits clarification by both parties.

For prevention purposes and in order to take into account changes in exposure to acts of terrorism, an increase in the contribution component included in property insurance policies from €3.30 to €4.30 was decided by the decree of 30<sup>th</sup> October, 2015, following the attacks of January 2015 but prior to those of November 13. This increase in *FGTI* resources is about EUR 86 Millions and represents a preliminary response to the threat of terrorism. However, given the number of claims handled in the aftermath of the attacks of November, will this measure suffice in the event of terrorist attacks of greater magnitude? This unprecedented situation obliges the different parties to attempt to outline all possible perspectives. In this manner, recourse to the use of the insurance market by way of the establishment of a standard guarantee in life, accident and health policies, or by extension of property policies, could comprise an area of reflection and discussion between the parties involved. In the present context marked by the ever-increasing risk of terrorist attacks, the establishment of a mechanism that could depreciate the cost of major events before they occur could also be used to ensure the financing of compensation costs in the event of wide-scale attacks.

### **PROPERTY DAMAGE COVERAGE**

Made compulsory by the French law of September 1986, this coverage, as is the case for bodily injury coverage, takes the form of a supplementary guarantee that insurers include in property insurance policies<sup>16</sup>. Modifications made to this law in 2006 do not however provide any indication as to the scope or the pricing of the mandatory guarantee which, consequently, is set out by the terms of the policy<sup>17</sup>. Although article R126-2 of the law stipulates to a limited extent the scope of application of the coverage, the first possible change would be to define the limits of compensation by attributing specific rules to the legal guarantee.

Reference to the fire guarantee was carried over from the context in which the coverage was designed, namely acts of terrorism committed using traditional explosives that cause fire and explosion damage. The events of January and November 2015 and July 2016 radically changed

---

<sup>15</sup> *L'Argus de l'assurance*, March 2015.

<sup>16</sup> Law no. 86-1020 of September 9, 1986.

<sup>17</sup> Law no. 2006-64 of January 23, 2006.

the paradigm as the *modus operandi* was entirely different from the attacks perpetrated in the 1980s. Already in 2006, the coverage was extended to include damages resulting from attacks using nuclear, biological, chemical or radiological weapons. Additionally, regarding the damages resulting from the recent shootings, it appears necessary to review the indirect economical consequences of this type of attack in order to enhance the resilience of our societies, including for those risks that lie at the limits of insurability.

Indeed, simultaneous operations of armed terrorist groups within a single area or the explosion of a "dirty" bomb in a location with a high concentration of insured property would potentially have economic repercussions that greatly surpass the amount of compensation provided solely for direct damages. This raises the question of how to compensate for business interruption losses arising from the inaccessibility of premises or defaulting suppliers in the event of the long-term closing of an area to traffic, especially by decision of the authorities, as was the case for the area surrounding the Bataclan concert hall in Paris. Although it is impossible to provide compensation for all losses, clarification of the contours of the coverage appears necessary so that all the parties may contribute to the recovery of the economy and to a restoration of confidence. This clarification of the scope of intervention of terrorist coverage carries with it two important prerequisites:

- the preservation of the role of the State through the intermediary of public reinsurance;
- the assessment of potential loss experience so as to determine, as best as possible, the required financial resources. The specific question of contingent business interruption needs to collect data about interdependence between companies and to model it.

The second condition is based on the supposition that we develop a model that would take into account the different possible scenarios, including the most pessimistic ones. CCR is currently conducting efforts in this area, in the framework of its general interest missions.

## CONCLUSION

Given the disparity of the forms of coverage offered, it appears necessary today to build a common foundation for each type of damage, bodily injury or property, in order to provide a response to acts of terrorism that is backed by sound financial strength and based on solidarity. Using this foundation as a basis, each insurer would then be granted the possibility of enhancing his offer so as to provide coverage that is best adapted to the risk.

A similar paper has been published in French in "Risques" n°105. See [http://revue-risques.fr/revue/risques/html/risques-105/\\$FILE/Risques\\_105\\_edito.html](http://revue-risques.fr/revue/risques/html/risques-105/$FILE/Risques_105_edito.html)

## BIBLIOGRAPHY

APREF, White paper (in French), The reinsurance of terrorism in France, December 2012.  
Michel-Kerjan E, "Terrorism insurance in OECD countries: where do we stand?", *Risques*, no. 84, December 2010. [Published in French]





**Tom Johansmeyer**  
AVP, Strategy and Development  
PCS

[www.linkedin.com/in/tjohansmeyer](http://www.linkedin.com/in/tjohansmeyer)

Tom Johansmeyer is AVP – PCS Strategy and Development at ISO Claims Analytics, a division of Verisk Insurance Solutions. He leads all client- and market-facing activities at PCS, including new market entry, new solution development, and reinsurance/ILS activity. Currently, Tom is spearheading initiatives in global terror, global energy and marine, and regional property-catastrophe loss aggregation. Previously, Tom held insurance industry roles at Guy Carpenter (where he launched the first corporate blog in the reinsurance sector) and Deloitte. He's a veteran of the US Army, where he proudly pushed paper in a personnel position in the late 1990s.

## 8. TERROR RISK TRANSFER: WHAT WE CAN LEARN FROM KRASNOVIA

The global insurance and reinsurance industry's recent experiences with innovation remind me of my final field exercise in U.S. Army basic training. As unorthodox as that may sound, give me a minute to explain.

Our opposing force was the fictional 'Combined Arms Army of the Republic of Krasnovia'. Deep in the 1980s—the era of 'evil empire(s)' and 'trust but verify'—it made perfect sense. And I have little doubt that that's when the name of the opposing force was conceived. By 1994, though, when I went through basic training, much had changed. We saw the Berlin Wall fall, Yugoslavia descend into chaos, and perhaps early signs of a new threat in the Middle East, although the first foray involving Iraq concluded in a mere 100 days.



We were a handful of years into the post-Communist transition period, but our thinking - and training - was clearly focused on the prior threat. And that's not terribly unusual. A few years after I crossed the stage at Fort Sill, a newly minted soldier, my military history professor spent the better part of a semester driving home the notion that the beginning of every new war involves fighting the prior one. It makes sense, of course. You invest in the most recent problem you had and adapt to the next one when it arises. And even if you scan the world for emerging threats, it can take time to pivot. Thus, the Republic of Krasnovia - five years after the Berlin Wall came down.

What does this have to do with insurance and reinsurance?

Until the global financial crisis in 2008, the property catastrophe space focused on lessons from the Florida hurricanes of 2004 and 2005's Hurricanes Katrina, Rita, and Wilma. Following the financial crisis, the discussion turned to clash scenarios. Just recently, in a series of client meetings, the implications of a confluence of economic and natural catastrophes entered into the conversation - with no prompting from me.

This isn't to say that we take a myopic view of the market and advance only through a process of event and reaction. There's plenty of investment and effort being applied to new and emerging risks, analytical innovation, and improved capital management. But it's hard to resist planning for what you know.

While this problem exists across the global industry, it may be particularly acute in the terror space for a number of reasons. Historically, terror has been relatively small. Thanks to the global soft market, much of that has begun to get absorbed into aggregate reinsurance treaties, creating accumulations of exposure where they hadn't existed before.

And that's just the traditional, 'Krasnovian', view of the problem. While traditional appetites are being satisfied, insurers are exploring and writing new forms of terror cover in the face of a shifting threat. Getting better at hedging the old risks clearly won't be good enough in the next few years.

## **IT'S NOT (JUST) KRASNOVIA**

Over the past nine months, nearly every research and development discussion Property Claim Services® (PCS®) had about transferring terror risk led to one request: 'We need a PD number'. Physical damage. During this period, we saw tragic attacks in Paris and Brussels—among many others—leading to high numbers of fatalities, but causing minimal physical damage. The global terror threat is evolving. Major coordinated attacks requiring extensive planning and resource commitment have given way to smaller and more nimble terror organisations and 'active assailant' scenarios. The trend appears to be gaining momentum.

For the global insurance and reinsurance industry, the effect has been an unusual middle ground. Terror activity is on the rise. Businesses are experiencing losses (particularly business interruption), but those losses may not be covered. When they are, it seems that primary insurer losses are simply eroding retentions. If you're covering property, you'll clearly be focused on the property damage caused by an attack. Even for business interruption, there's generally a requirement that property damage reaches a certain threshold.

In the early days, the shifting nature of the threat—from major physical damage to high-fatality/low-damage situations—led to gaps in protection for original insureds and primary insurers. The cover in place was never intended to attach in an active assailant scenario. This could change as original insureds—and then primary insurers—seek protection that's more relevant to the changing nature of the risk.

Of course, this doesn't mean previous hedging needs—such as a multibillion-dollar physical damage terror attack—can be ignored. Krasnovia remains, to a certain extent. History has demonstrated that large physical damage events could occur and, with the right conditions, could lead to massive losses, potentially of the sort that could threaten solvency. Even if the threat is shifting away from what works its way into the global risk and capital supply chain, heightened frequency can embolden perpetrators of terror to swing back to 9/11- and 7/7-style attacks.

As corporate risk managers begin to spend more time talking to their boards of directors about terror risk, demand for cover could increase. That would lead to more original risk being written, which would likely stimulate demand for reinsurance and retrocessional protection. Additionally, heightened frequency could provide a broader base for future action that could shift back toward trophy targets, which would affect insurers and reinsurers.

Insurers and reinsurers thus could see a dual terror threat to their clients and balance sheets in the near future. One would involve getting better at defeating the Krasnovians, so to speak, while the other involves understanding the next likely threat and identifying how to structure cover for the emerging risk effectively.

### **CAPITALISING BEYOND KRASNOVIA**

After dozens of conversations with insurers, reinsurers, reinsurance intermediaries, and catastrophe modellers, it's clear that there's plenty of capacity for terror risk worldwide. At least that's the case superficially. As you dig into the global terror risk-transfer market, you begin to see that there's plenty of capacity for terror, as long as the risks are relatable for the capacity providers.

Are the line sizes familiar? Are the risk areas major market (G20, Western Europe, global)? If the answer is 'yes', then capacity is abundant. However, when the cover you're looking for becomes less conventional—such as nuclear, biological, chemical, and radiological (NBCR) - the capacity available can begin to change. That's why it can seem like there are two divergent views on the global terror market.

To some—who are placing conventional, traditional reinsurance protection - there's little need for parametric or industry loss index solutions. 'I can place as much as I want. All day long'. I've heard that a number of times. But there are still some books of business, types of risk, and capacity needs that lend themselves to alternative forms of risk transfer. The global terror industry loss warranty (ILW) may be fairly small now, but it could grow significantly in the next year.

Be they parametric or industry loss index, the factors likely to drive the growth of the global terror ILW market are (a) an increase in accumulations through traditional reinsurance and (b) the proliferation of new forms of cover and original insured. As reinsurers' exposures grow,

greater need for retrocessional protection for both ‘Krasnovian’ and emerging events could render traditional indemnity cover insufficient for retrocessional needs.

The increase in accumulations has been fuelled recently through a fairly predictable soft market dynamic. To hold the line on pricing, reinsurers have become more flexible on terms. Increasingly, terror has been included in property catastrophe treaties. Some reinsurers have seen an increase in exposures as a result, which has already led to some interest in index-triggered retrocessional opportunities. The need for an alternative solution could grow higher in the first quarter of 2017, depending on how pricing and terms are handled at the January 1, 2017, reinsurance renewal.

Further, conditions are right for new forms of terror cover to enter the market. Active assailant events have become increasingly common, with dozens of fatalities per event almost the norm. As original insureds continue to sustain uncovered losses on this sort of event, demand for protection could grow, especially if the industry continues to explore the use of innovative structures, such as parametric triggers. New products would only serve to increase exposures while also making reinsurer books more complex. That would drive further need for an index-triggered approach to terror risk transfer.

In addition to new products, the organisations seeking unconventional cover should grow in diversity. Community resilience has become the watchword in the public sector, particularly following the events in San Bernardino and Orlando. In addition to making corporate original insureds whole, communities will need to find a way to get back on their feet as quickly as possible after an event. Business interruption clearly affects the community—for example, temporarily creating the inability for people to earn wages and support their families. Community interruption expands this problem. Access to infrastructure and vital services could be impeded. A rapid injection of capital post-event can help ensure that communities are served properly and that they can recover quickly.

## THE POST-KRASNOVIAN TERROR RISK-TRANSFER LANDSCAPE

Depending on how the global terror risk-transfer market evolves in the coming year, we could see four basic types of terror reinsurance and alternative risk transfer emerge: traditional, complex, attritional, and emergency.

**Traditional:** Think of this as Krasnovian - the sort of reinsurance and retrocession currently being written (on an indemnity basis) in the global market. Even with shifting terror patterns and evolving insurer and reinsurer needs, the need for traditional protection is unlikely to disappear.

**Complex:** Related to the traditional need, complex scenarios could involve diverse needs, massive accumulations (and thus risk-transfer needs), or threats that often get excluded (NBCR). Generally, this is where you’d most likely find industry loss index ILWs rather than either indemnity or parametric covers as you see today in the property catastrophe reinsurance sector. The amount of time it could take for an industry loss to emerge makes the approach more effective for large risks and complex books of business, where an industry loss could emerge before a traditional transaction is settled. However, it isn’t fast enough to meet the types of near-term need described below.

**Attritional:** The anti-Krasnovian risk, an increase in coverage for what is today attritional, could have implications further up the global risk and capital supply chain. The nature of the cover would have to depend on the underlying risks being hedged. Contingent business interruption could be written using some combination of fatalities, casualties, and hostages, for example. Workers compensation from terror perhaps could also be written on a parametric basis and even be bundled with parametric workers' compensation catastrophe covers (such as earthquake). Attritional risks could be written on an indemnity basis, subject to the capacity needed and types of risks and regions involved.

**Emergency:** This is protection intended to deliver a rapid injection of capital to an original insured—either a business or a community—to meet immediate cash flow concerns. For a community, this form of protection could take the place of federal aid (at least to some extent) and be deployed to the community much more quickly. If triggered on a parametric basis from a consistent, reliable, and independent reporting agent, post-event funds could be delivered weeks after the event—compared with years, potentially, for government-supplied aid. And it would reduce the burden on taxpayers. Essentially, the community would get better, faster, and more reliable protection while alleviating the financial burden post-event on its citizens.

Of course, the capital will follow the need, and the new, post-Krasnovian market structure above relies on the notion that new types of cover will make it to market. And of course, competing forces are at play. Soft market conditions can favour innovation, as capital providers need to find new ways to deploy. However, those same conditions also make it easier for companies to retain risk or simply enjoy lower pricing on traditional forms of protection. What will make the difference is a combination of prudent risk-transfer product development and savvy, widespread distribution.

Effective distribution will require a clear and compelling value proposition, particularly for corporates and communities. After all, that's the original risk level. Driving adoption there naturally creates demand and opportunity for capital providers at higher links in the chain. Even if the threat is shifting away from what works its way into the global risk and capital supply chain, heightened frequency can embolden perpetrators of terror. As corporates begin to spend more time talking to their boards of directors about terror risk, demand for cover could increase, resulting in more original risk being written and subsequently stimulating demand for reinsurance followed by retrocessional protection. Additionally, heightened frequency could provide a broader base for future action that could shift back toward trophy targets, which would affect insurers and reinsurers.

## POST-KRASNOVIAN CONSIDERATIONS

Well, they aren't necessarily *post*-Krasnovian considerations. Sometimes historical risks do disappear, although it does take an extreme set of developments for that to happen. More often, those risks are absorbed into risk and capital management activity on an ongoing basis. Because of this, our industry can continue to improve how we understand the past threats that remain relevant while also scanning for the new risks that could become devastating tomorrow.

The advancement of risk management, therefore, is mostly additive. We don't replace risks, for the most part. Nobody enjoys a Krasnovian moment when a new enemy is identified. Rather, we accumulate historical foes. Some may become less likely or impactful over time, but they could stick around for quite a bit.

Philosopher Karl Popper proposed that science moves forward through a process of conjecture and refutation. What we're seeing in the terror market—and the broader risk-transfer space - is more a process of conjecture and integration. We take what we've seen and hedged in the past and continue to do so while looking for what could come next. We integrate the new. And then when the emerging threat is validated (that is, through an event), it becomes part of the 'traditional' portion of the analysis.

Like Popper's sciences, we'll never stop scanning the environment for new risks. Doubtless, we'll miss some, catch others too early, and occasionally execute the right treatment at the right time. This process - itself fraught with risk - carries much better benefits than simply focusing on what we've learned from the past.





**Dan Kaszeta**  
**Managing Director**  
**Strongpoint Security**

[www.linkedin.com/in/dankaszeta](http://www.linkedin.com/in/dankaszeta)

Dan is an independent consultant in chemical, biological, and radiological defence and various security disciplines, currently based in London. His 25 year career spans service in the US Army, the White House Military Office, and the US Secret Service, before switching to the private sector in 2008. He is the author of *CBRN and Hazmat Incidents at Major Public Events* (Wiley, 2012) and the author of numerous articles.

## 9. DECONTAMINATION OF BUILDINGS AFTER AN ANTHRAX ATTACK

### THE 2001 ANTHRAX ATTACKS, 15 YEARS ON

#### ABSTRACT

*The 2001 Anthrax attacks in the USA provide a rare example of a manmade event that contaminates large amounts of property with a biological weapon. The so-called “Amerithrax” incidents form basis for numerous conclusions about bioterrorism. Issues raised include, but are not limited technical aspects anthrax, medical countermeasures, detection, forensics, economic impact, and property considerations. The overall cost was likely in the billions of US dollars, but the extent to which this set of incidents can be extended as a model for future planning is highly variable.*

#### INTRODUCTION

In 2001, a small amount of anthrax in powder form caused widespread panic. People died, others were seriously ill, and large amounts of property were contaminated with deadly anthrax spores. It has taken most of the intervening years to examine the aspects of this series of incidents. This article seeks to examine many aspects of the attacks to see if this so-called “Amerithrax” incident provides any lessons for those planning to manage and mitigate risks in the future.

#### WHAT IS ANTHRAX?

Anthrax is a bacteria, also known as *Bacillus anthracis*. It is primarily a disease among plant-eating animals, both wild and domesticated. It is endemic in some parts of the world. Humans rarely get anthrax, and when it does occur naturally, it is generally through contact with sheep or cattle who are sick, or products such as skins, hides, or bones from sick animals. Unlike most bacteria, anthrax microorganisms can form spores on contact with air, effectively going into a state of suspended animation with no metabolism. Anthrax spores are highly resistant to environmental trauma and can last for many years in soil or other environments, as long as they remain dry and out of direct sunshine. It is this sporulated form that makes it eminently usable

as biological weapon, as these spores are already effectively in a powder form that eases dispersal in a fine aerosol of small particles. Of the various available pathogens, scientists found that anthrax was one of the easiest to turn into a weapon to cause mass lethality.

Anthrax in humans generally manifests as cutaneous anthrax, a serious skin disease, but one that is quite treatable with basic antibiotics. Gastrointestinal anthrax is possible, generally from eating contaminated meat, but is quite rare. Pulmonary anthrax, infecting the respiratory system, is unknown in nature but was occasionally noted in textile mills, earning the moniker “wool sorters’ disease”. Historically, pulmonary anthrax was quite lethal on the few occasions when it did occur. The most infamous anthrax outbreak occurred in 1979, in Sverdlovsk, in Russia. An accidental release of an aerosol of anthrax spores that had been produced as an illegal biological weapon (the USSR was party to the Biological and Toxins Weapon Convention) caused at least 66 fatalities.<sup>18</sup>

## THE ANTHRAX ATTACKS

Shortly after the September 11 terrorist attacks on the United States, letters containing the bacterial pathogen anthrax (*Bacillus anthracis*) were sent through the US Postal Service to various addresses in the eastern United States. All of the letters appear to have been posted from a single mailbox in Princeton, New Jersey. The first round of letters appears to have contained at least 5 letters, addressed and delivered to American Media Inc. (EMI) in North Carolina (parent of *National Enquirer*), ABC News, CBS News, NBC News, and the *New York Post*. The latter four were all in New York. Only the *New York Post* and NBC News letters were recovered; the existence of the other is presumed because of the presence of contamination and/or the onset of illness.

A second round of mailings sent two letters to two United States Senators, Patrick Leahy and Thomas Daschle, in their offices in Washington DC on the Capitol Hill complex. A staff member opened the Daschle letter. The Leahy letter was recovered unopened in the course of the investigation, having been misdirected to the US State Department’s mail facility due to the incorrect automated reading of the ZIP code. All of the recovered letters contained a small amount of suspicious powder.

A total of 22 people became sick from exposure to the letters. 11 persons were ill with pulmonary anthrax, of whom 5 died and 6 recovered after intensive treatment. A further 11 persons were made ill with cutaneous anthrax, but recovered. A further 31 people tested positive for exposure to anthrax, but did not become ill, most likely because of widespread administration of prophylactic antibiotics. Tens of thousands of others received such prophylaxis as a preventive measure. The five dead included a photo editor at the AMI building (the first victim), two postal workers, one hospital worker, and an elderly woman. The route of exposure for the latter two victims is somewhat uncertain. The elderly woman, Ms. Otilie Lundgren (aged 94) is presumed to have become ill from exposure to cross-contaminated mail.<sup>19</sup>

---

<sup>18</sup> A. Benenson (ed.), *Control of Communicable Diseases Manual*, 16<sup>th</sup> ed., American Public Health Association, 1995, p. 20.

<sup>19</sup> United States Department of Justice, *Amerithrax Investigative Summary*, United States Government, Washington DC, 2010, p. 4.

The Federal Bureau of Investigation led the subsequent lengthy terrorism investigation, which lasted for many years. The investigation came to be known as the “Amerithrax” investigation and was one of the largest investigations in the history of federal law enforcement. As of 2010, over 600,000 person-hours of investigative labour had gone into the investigation and 10,000 witness statements had been collected.<sup>20</sup>

There is a strong circumstantial case to be made that the perpetrator was Dr. Bruce Ivins, a microbiologist in the employ of the United States government at the US Army Medical Research Institute of Infectious Diseases (USAMRIID). He was a leading anthrax expert. USAMRIID itself was heavily involved in the investigation. However, Dr. Ivins committed suicide in July 2008, at a point when the on-going investigation had focussed on his activities and movements in 2001 during the anthrax mailings. While there does appear to be a strong case that Dr. Ivins committed the murders, and probably did so alone, he was never charged and the evidence against him was never tested at trial. There are strong minority opinions that seek to exculpate Dr. Ivins. A full account of Dr. Ivins’ life and the criminal investigation is beyond the scope of this article but is addressed in considerable detail by D. Willman<sup>21</sup>

### PREMISES CONTAMINATED

Due to the passage of the relatively leaky anthrax-bearing envelopes through the postal system with all of the handling and transportation between facilities and the easily aerosolised nature of the anthrax spores, a significant number of rooms and buildings were contaminated by at least nominal amounts of anthrax spores. At least 42 buildings had some anthrax contamination, based on the compilation done by Schmitt and Zacchia<sup>22</sup>, although this article’s author has personal knowledge of at least two facilities not on their list. These buildings include, but are not limited to the Hart Senate Office Building, mail facilities for the Department of Justice, General Service Administration, and State Department, the publisher American Media Inc. (AMI), and numerous post office facilities. Not included in the Schmitt/Zacchia survey are mailboxes and vehicles, as well as vast quantities of equipment used by responders. There appears to have been no comprehensive inventory of contaminated property ever published or even summarised. It should be noted that in many of the 42 identified buildings, contamination was narrowly circumscribed, often to one room, and in some instances to a single piece of equipment, such as a piece of mail handling equipment.

### THE DECONTAMINATION EFFORT

The deadly nature of anthrax spores and both the practical and symbolic necessity to return rooms and building back into use meant that a serious decontamination effort needed to be undertaken. Rooms and surfaces producing positive test results were cleaned and re-sampled, and often cleaned a second or third time. Numerous agencies and companies were involved in the extensive decontamination effort. At Capitol Hill, the highest profile site, the US Environmental Protection Agency (EPA) took the lead in the decontamination effort, and this effort is well documented. Efforts at other sites are less documented, involving a wide number of agencies and contractors.

---

<sup>20</sup> Department. of Justice, p. 4.

<sup>21</sup> D. Willman, *The Mirage Man*, Random House, 2011.

<sup>22</sup> K. Schmitt and N. Zacchia, ‘Total Decontamination Cost of the Anthrax Letter Attacks’, *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, vol.10, no. 1, 2012, pp. 1-10.

In 2001, a number of techniques and substances were used to decontaminate the affected areas. Surfaces or objects could be treated either *in situ* or off-site, and large volumes were decontaminated using fumigation techniques. Time-honoured techniques such as aging (i.e. waiting for the problem to go away through natural decay or other natural processes) or direct sunlight were simply not useable due to the persistent nature of anthrax spores. As the methods used in 2001 are still largely valid, it is illustrative to briefly survey the techniques and substances used at the time.

Decontamination of relatively non-sensitive surfaces was accomplished with the use of any or all of the following:

- Bleach (a solution of hypochlorite in water)
- Liquid chlorine dioxide, a potent source of chlorine ions
- Commercial antimicrobial solutions
- “Sandia Foam”, a US government proprietary decontaminant

Large volume areas were sealed and fumigated with various substances:

- Chlorine dioxide gas
- Vaporised hydrogen peroxide
- Para-formaldehyde

Items that were considered sensitive and/or important which could be removed for off-site decontamination, by the following means:

- Fumigation with chlorine dioxide gas
- Fumigation with ethylene oxide
- Irradiation

Porous materials (such as carpets) were also, where practical, vacuumed with high efficiency particulate (HEPA) filter vacuum cleaners, which removed (but did not inactivate) the anthrax spores. It should be noted that all of the above methods pose safety issues and can be hazardous to many types of materials. Of particular note, computer equipment, artwork, and documents can be severely affected. Presence of residual amounts of chemicals left over from the decontamination process is also an important factor.<sup>23</sup>

## COST AND ECONOMIC IMPACT

The overall decontamination effort was costly. No single official summary figure of the direct costs of the decontamination effort has been released. Much of this is due to the complex nature of government accounting practices. For example, not every expenditure was transparent. Small purchases and contracts below certain thresholds may not be easily identified or clearly tied to the anthrax clean-up effort. In addition the response effort was, by necessity, spread out over numerous public and private entities. No official figure representing the total cost of decontamination has been published. The Schmitt/Zacchia study<sup>24</sup> applies a fair degree of rigor to the question and estimates the total cost of decontamination to be in the range from 300 to 330 million USD. The largest single component of the total cost appears to be the 130 million USD spent in the fumigation effort to decontaminate the Brentwood postal facility in

---

<sup>23</sup> M. Simpson, *Anthrax-Contaminated Facilities: Preparations and a Standard for Remediation*, Congressional Research Service, the Library of Congress, December 2005, p.6.

<sup>24</sup> Schmitt and Zacchia, p. 8.

Washington DC.<sup>25</sup> It should be noted that these figures are strictly the cost of the decontamination effort, not the cost for replacement of furnishings or redecoration.

Indirect costs were likely high as well, although these costs are difficult to account for. Large quantities of furnishings, mail, and equipment were effectively permanently lost. Many facilities were out of use for long periods of time. The Capitol Hill offices were closed for three months. The Brentwood postal facility was out of use from October 2001 to December 2003. The Trenton New Jersey postal sorting facility was out of use from October 2001 to March 2005. 1.8 million items of mail were quarantined.<sup>26</sup> As recently as 2006, this author witnessed that the Anacostia Naval Yard postal building, which had been fumigated with hydrogen peroxide, was still not in use. Direct and indirect costs to the US Postal Service have been cited as being as much as USD 3 billion and lost revenue of up to USD 2 billion.<sup>27</sup>

In addition, enormous new security measures were put into place at great effort and expense to protect Federal building and employees from biological hazard. While not all of these actions were directly attributable to the Amerithrax attack, it is difficult to ignore the effect that Amerithrax had on both general and specific security and antiterrorism measures during that tense post-9/11 environment.

### LESSONS LEARNED AND ISSUES RAISED BY THE AMERITHRAX ATTACKS

The contamination caused by the anthrax letters brought to light many issues and considerations which had theretofore only been considered by a narrow fringe of terrorism and public health specialists. Biological decontamination after a widespread hostile dispersal of biological warfare agent material in a civilian environment was largely a theoretical matter before the Amerithrax incidents. New knowledge emerged through hard experience. In addition, new questions and issues were raised. Not every aspect is fully relevant to this paper, but a quick overview is illustrative and points out the complexity issues raised by biological terrorism, which need to be understood by all.

### CHARACTERISTICS OF ANTHRAX

The Amerithrax incidents changed some of the fundamental understanding of anthrax, how it behaves in the built environment, and how it behaves as a medical condition. In defence and security circles, anthrax had long been considered a potential biological warfare threat. It had been produced and weaponized by several countries, including the United States, United Kingdom, and the Soviet Union, in the Second World War and/or the Cold War. However, much of the practical knowledge in the United States about anthrax and its characteristics as a weapon dated from no later than the late 1960s. The US offensive biological warfare programme ceased circa 1970 and much of the knowledge of anthrax and other biological warfare agents was lost, in the minds of elderly retirees, or deeply buried in classified archives.

The treatability of inhalational anthrax was one area where lessons were learned. It was considered conventional wisdom as late as the late 1990s that respiratory anthrax was uniformly fatal after the onset of serious symptoms. In the actual Amerithrax event, respiratory

---

<sup>25</sup> L Wein, Y. Liu, and T. Leighton, 'HEPA/Vaccine Plan for Indoor Anthrax Remediation', *Emerging Infection Diseases*, vol.11, no.1, 2005, pp. 69-76.

<sup>26</sup> Department of Justice, p. 3.

<sup>27</sup> 'A Nation Challenged: The Mail; Postal Service Asks Congress for \$5 Billion', *New York Times*, 9 Nov 2001.



anthrax was not uniformly fatal after onset of symptoms. Six persons who became ill with respiratory anthrax survived, due to intensive treatment. Some of this may be due to newer families of antibiotics, such as fluoroquinolones, which did not exist during Cold War era research. We now know that aggressive medical intervention will save lives. Clinical treatment protocols have been updated. Likewise, we know that chemoprophylaxis – the practice of administering antibiotics to people who might have been exposed – is effective in reducing the number of people who get ill.

The anthrax powder, particularly that in the second batch, used in the Senate letters, provided interesting new knowledge. The size of the particles was interesting. Despite claims that the anthrax letters contained nation-state grade weaponized anthrax, the anthrax particles recovered had a mass median diameter between 22 and 38 microns. This was considerably larger than the 1 to 10 micron diameter that had been previously considered the realistic size for dispersal as a biological weapon<sup>28</sup>, although this was by no means a settled issue. The Amerithrax events demonstrated that anthrax particles large than 10 microns can cause illness and death. However, it is conceivable that there were particles of smaller size, but that none were collected as evidence.

The concentration of the anthrax powder used in the letters was  $4.60 \times 10^{10}$  to  $2.10 \times 10^{12}$  colony-forming units (CFU) per gram<sup>29</sup>. (A CFU is a single viable anthrax microorganism in this instance.) While the exact concentration of anthrax powder used in old Soviet and US biological warfare products remains unpublished, US laboratories made powder of a concentration of  $3.26 \times 10^8$  CFU/g for use in testing biological defences<sup>30</sup>. Clearly, the anthrax powder in the Amerithrax case was unusually high in concentration.

## DETECTION AND IDENTIFICATION

One of the most important issues was, and continues to be, detection. Detecting when biological warfare agents are present is an enormously complex task. Identifying anthrax in particular and discriminating it from a whole host of other biological matter that is normally present in natural background matter is not an easy task. Detection helps responders and decision-makers to react in a proper and efficient manner. Detection technology produces information that answers the following questions:

- Has anthrax been dispersed?
- Where has it been dispersed?
- What is the actual extent of contamination? In other words, what areas and materials need to be contaminated?
- How much anthrax is present?
- Has decontamination been successful? i.e. Has the anthrax been inactivated, removed, or otherwise rendered not harmful to people?

In 2001, none of the available technology was capable of answering these questions in anything approaching a real-time fashion. With radiological contamination, a wide variety of technology and products exist which can readily detect and measure most kinds of radioactivity-emitting contamination. Many kinds of chemical contamination can be similarly measured, with varying

---

<sup>28</sup> J.Grotte, *Frequently Asked Questions Regarding Biological Detection*, Institute for Defense Analysis, Alexandria, Virginia, Nov. 2001, p. 3.

<sup>29</sup> Department of Justice, p. 14.

<sup>30</sup> G. Matsumoto, 'Anthrax Powder: State of the Art?', *Science*, vol 302, November 2003, p. 1495.



degrees of precision. However, no comparable level of instrumentation existed for biological contamination in 2001, nor does it exist today.

In addition to detecting the presence of anthrax, there is the issue of discriminating between living (“viable”) and dead anthrax spores. Living anthrax makes people sick; dead anthrax does not. Several technologies for detection of anthrax (and other pathogens) have considerable difficulty determining whether the material detected is live or dead. Immunoassay techniques, which were the prevalent portable technology available in 2001, rely on immune response to detect microbes of interest. In specific, they test for reactions between antibodies and antigens (in this case, anthrax microbes or specifically related compounds).<sup>31</sup> But, as most who understand the science behind vaccines can understand, a dead microbe may still be able to provoke an immune response. Other techniques, such as DNA analysis, most prevalently the Polymerase Chain Reaction (PCR) analysis technique, are highly effective at detecting anthrax from environmental samples.<sup>32</sup> Again, however, even the casual observer of modern forensic procedure knows that dead things have DNA. Dead anthrax can be detected by PCR assay techniques, as was firmly shown in a study in 2003.<sup>33</sup> There are many situations and application where detection of dead anthrax as well as viable anthrax is important, such as determining whether an attack took place or for myriad forensic, investigative, and intelligence collection purposes. However, such techniques clearly cannot answer the questions of “Have we decontaminated this object/room/building effectively” or “Is this location safe for re-occupancy?” to any sort of level of satisfaction.

The limitations of field technology were well known in 2001. Determining the presence, or lack, of viable anthrax spores during the 2001 decontamination and remediation efforts relied on classic microbiology laboratory techniques. The most definitive method for detection of anthrax has been to take environmental samples and culture these samples in growth media, over many hours or days, to see if anthrax cultures grow. At the US Capitol office buildings, the EPA and their support staff from other agencies and contractors collected three types of surface samples: wet swabs, dry wipes, and HEPA vacuuming (for porous materials such as textiles and wood). Various types of air sampling were performed as well.<sup>34</sup>

In a field setting, particularly a large one like entire office buildings, the microbiological culture technique translates into an enormous commitment of time and labour. Every single surface (walls, floors, ceilings, every facet of furniture items, interiors of duct work, fan blades in the ventilation system, cooling fans inside computers, etc.) needs to be wiped or swabbed thoroughly, using sterile collection media. The sample needs to be safely contained and securely transported to a laboratory so that the sample can be cultured. Quality control is extremely important using this technique. Fastidious procedures are required to ensure that cross-contamination does not occur and that the samples taken provide an effective indication of the quantity of microbes present. US government scientists identified a large number of factors, problems, and considerations relevant to estimating microbial concentrations from

---

<sup>31</sup> A. Peruski and L. Peruski, ‘Immunological Methods for Detection and Identification of Infectious Disease and Biological Warfare Agents’, *J. Clinical and Vaccine Immunology*, vol. 10, no. 4, 2003, pp. 506-513.

<sup>32</sup> C. Ryu et al., ‘Sensitive and Rapid Quantitative Detection of Anthrax Spores Isolated from Soil Samples by Real-Time PCR’, *Microbiology and Immunology*, vol. 47, no. 10, 2003, pp. 693-699.

<sup>33</sup> A. Fasanella et al., ‘PCR Assay to Detect *Bacillus anthracis* Spores in Heat-Treated Specimens’, *J. Clinical Microbiology*, vol. 41, no. 2, 2003, pp. 896-899.

<sup>34</sup> Government Accounting Office (US), *Report to the Chairman, Committee on Finance, U.S. Senate: Capitol Hill Anthrax Incident GAO 03-686*. United States Government, 2003, p. 6.

field samples this year.<sup>35</sup> The cumulative effect these variables and considerations is that there is actually a degree of uncertainty as to how comprehensively effective such sampling may be. In other words, we cannot be certain if there is not a viable anthrax spore lurking around in some crevice.

## DELAYED INFORMATION

Because on-the-spot detection and measurement is not feasible given present technology, there is reliance on laboratory techniques to confirm or deny the presence of anthrax. This means that there is a high degree of delay involved in every step of the remediation process, due to the time lag necessitated by slow laboratory processes and high numbers of samples.

Accounts vary on the overall number of samples taken during the Amerithrax response, although the figure of at least 121,700 samples processed by accredited US laboratories is indicated in one US government document.<sup>36</sup> Certainly, this high volume of samples also means that turnaround time for meaningful test results is long. This means that the period of time a particular room or building is out of use will be seriously lengthened.

## DECONTAMINATION METHODS

The decontamination by fumigation required long periods of time. The chlorine dioxide, such as used at the Hart Senate Office Building can require between 20 and 400 minutes, depending on concentration to achieve a two order of magnitude reduction in anthrax.<sup>37</sup> One does not require a high degree of education in chemistry to realise that large concentrations of chlorine or para-formaldehyde vapour over a lengthy period is likely to be ruinous to some of the typical contents of an office or residence. The need for safety is compelling and the means of detection have serious limitations, so the direct result is a broad-brush approach to decontamination. In late 2001, a surface swipe yielding positive test for an anthrax spore on a 10 cm x 10 cm patch on desk did not mean a drop of bleach just on that one spore, it meant a thorough soaking of the entire surface just to be certain, and possibly fumigation of the entire room. A large amount of uncontaminated material will be, by necessity, subjected to decontamination procedures.

The prevalent fumigation techniques, chlorine dioxide and vaporised hydrogen peroxide, cause a variety of damage to various materials. This has been well document by two US Army studies.<sup>38 39</sup> Ethylene oxide is more useful in specialty chambers rather than in buildings. It is highly reactive, possibly a carcinogen, and is extremely flammable. Formaldehyde is highly odorous long after use, must be neutralized with other substances after use, off-gases from porous surfaces for months after use, and is a potential carcinogen.

The problem of sensitive equipment is particularly acute. Modern buildings have computers and electronic appliances. Soaking a laptop in bleach is not a reasonable method if one wants

---

<sup>35</sup> E. Silvestri et al., 'Consideration for estimating microbial environmental data concentrations collected from a field setting', *J Exposure Science and Environmental Epidemiology*, 2016, pp. 1-11.

<sup>36</sup> Government Accounting Office (US), *Anthrax Detection: Agencies Need to Validate Sampling Activities to Increase Confidence in Negative Results* GAO 05-251. United States Government, 2005, p. 58

<sup>37</sup> A. Richardt et al. eds., *CBRN Protection: Managing the Threat of Chemical, Biological, Radioactive and Nuclear Weapon*, Weinheim, Germany, Wiley-VCH Verlag, 2013, p. 399.

<sup>38</sup> M. Brickhouse et al. *Effects of Vaporized Decontamination Systems on Selected Building Interior Materials: Chlorine Dioxide*, US Army Research, Development and Engineering Command, February 2009.

<sup>39</sup> M. Brickhouse et al. *Effects of Vaporized Decontamination Systems on Selected Building Interior Materials: Vaporized Hydrogen Peroxide*, US Army Research, Development and Engineering Command, January 2009.

to use it ever again. There is no reason why finely milled anthrax powder won't contaminate the interior of such devices. Cooling fans, breezes, and vents mean that a spore settling in a computer or radio might easily be re-suspended at a later time. Some electronics could be irradiated, but that may also damage the item.

### HOW CLEAN IS CLEAN?

Even putting aside the issues of live versus dead anthrax and the theoretical limits of detection, what level of cleanliness should be the standard for post-incident re-occupancy? At the time of the 2001 anthrax incidents there was no existing standard, regulation, or exposure limit set for anthrax. The standard used at the time for anthrax removal by the EPA at the Capitol Hill sites was “zero growth of anthrax surrogates in all post remediation samples.”<sup>40</sup> This is not the same thing as “zero anthrax” – it is basically impossible to prove such a negative. But the de facto standard from 2001 of no anthrax cultured in the environmental sampling is weak in that efficiency of sampling is subject to a wide number of variables and could easily lead to residual risk. Furthermore, there are parts of the world where anthrax is endemic among animals, so there are regions where there is a naturally occurring, albeit low, occurrence of a natural baseline of background anthrax. Specialist and regulators continue to debate the nature and details of an acceptable standard.

### SAFETY AND LABOUR ISSUES

The majority of the buildings contaminated in 2001 were federal property and it is the responsibility of the federal government to manage the fate of those buildings. The federal government has workers that can decontaminate things and the power to write contracts to hire more workers to do the decontamination. However, thorough decontamination is extremely labour-intensive. In the case of private ownership, there is the serious question of who exactly will perform the work. Serious consideration needs to be given to the question of who actually will decontaminate objects and buildings in the event of another attack. It cannot be assumed that there will always be people available to do the work. In the event of a large-scale contamination event involving private property, it is unclear who actually will be available and willing to undertake the work.

Safety of workers performing remediation is an important consideration. It is a great credit to the overall decontamination effort that no workers became ill during the lengthy restoration process. This was due to rigorous use of personal protective equipment and thorough decontamination of the workers themselves so they did not transfer any of the contamination out of the areas where they were working. Any future effort will need to take a similar or higher level of precaution to prevent illness, death, or transfer of contamination.

### FORENSIC AND INVESTIGATIVE CONSIDERATIONS

Expertise in conducting biological weapons-related criminal investigations was rare indeed in 2001. Within the FBI it had been largely limited to a handful of incidents involving either hoaxes or some small incidents involving the biological toxin ricin. The number of people with any kind of experience in this type of investigation, throughout the US government, was quite small.

---

<sup>40</sup> Simpson, p. 8.

The Amerithrax case pointed out that expertise on criminal investigations and forensic evidence collection were in law enforcement agencies, whereas the ability to do work in contaminated environments was largely in the hands of hazardous materials responders, who were largely in the fire services or environmental agencies. The overlap between the two was not large. The Amerithrax response effort pointed out that criminal investigators need to do their jobs in contaminated environments, and that hazardous materials responders need to know how to act in a manner consistent with forensic requirements.

This dichotomy extends to the laboratory. The laboratory that is well equipped to analyse anthrax spores is not the same as the laboratory that is well-equipped and well-trained to handle traditional criminology work. The issue of how to handle conventional evidence that is contaminated by a CBRN substance is not easily answered, nor is the question of how to extract useful conventional evidence (e.g. a fingerprint or fibre sample) from a fragment of a chemical or biological weapon. Until these questions get answered, the ability to identify and prosecute perpetrators will suffer.

Laboratory capacity to process suspected anthrax samples was strained. Laboratories strained under the weight of a weeks or months long backlog. Other laboratory work, some of which was no doubt of great need for medical and public health requirements, no doubt suffered. Serious strains on laboratory workers, equipment, consumable supplies, and procedures were noted in a US government report in 2003.<sup>41</sup> Additionally, many public health laboratories were not used to working to an administrative standard that could live up to forensic evidence standards. Some of the ones that did had problems handling the necessary paperwork. For example every single sample of the up to 700 samples a day processed by USAMRIID generated 25 pieces of paper.<sup>42</sup> Not every sample, of course, needed to live up to such standards, but there would have been a real prospect of evidence being dismissed by a competent defence attorney if some of the laboratory results had been used in court.

## RE-OCCUPANCY AND “PSYCHOLOGICAL CONTAMINATION”

Biological weapons gain some of their adverse impact from the psychological effects of their employment. Humans have a natural and understandable fear of lethal diseases. The presence of a lethal and little-understood microbe, such as anthrax, will make people afraid. There is every prospect of what I term “psychological contamination” of room, building, or area. There are likely to be situations where people are afraid to enter an area long after every feasible effort has been made to decontaminate the premises and every technical indicator shows that re-occupancy is safe. Workers may not return to a building until they feel it is safe to do so, and their decision to do so may be, in turn, based on numerous influences. Forcing workers to work in buildings that they consider hazardous could lead to labour disputes and litigation. Numerous postal workers felt reluctance to return to facilities that had been contaminated with anthrax spores.<sup>43</sup> Property damage and possible residue of decontaminants may also simply make the workplace unpleasant, reducing employee morale and increasing resignations.

---

<sup>41</sup> Government Accounting Office (US), *Public Health Response to Anthrax Incidents of 2001 GAO 04-152*, United States Government, 2003.

<sup>42</sup> D. Heyman, *Lessons from the Anthrax Attacks* (redacted), Center for Strategic and International Studies, Washington D.C., 2002, p. 4.

<sup>43</sup> M. Fernandez, ‘The Ghosts of Brentwood’, *Washington Post*, 18 May 2003.

## DECONTAMINATION VERSUS ABANDONMENT VERSUS DEMOLITION

In some situations decontamination may be the most expensive option available. Demolition or permanent abandonment of facilities may be preferred, particularly in the case of fungible real estate assets like conventional warehouses, office parks, or residences. It should be noted that not every CBRN hazard is as long-lived as anthrax spores, and some types of contamination, such as more fragile microbes or short to medium half-life radioisotopes, may in effect self-remediate over the passage of time.

The AMI building was clearly a case where disposal of the real estate assets was cheaper than decontamination. The owners paid less for the building than the estimated USD 5 million decontamination cost. They moved out and sold the building for very little to Sabre Technical Services, one of the federal decontamination contractors.<sup>44</sup> Clearly, should a similar event happen in the future, some property owners might be persuaded to act similarly.

Neither abandonment nor demolition does anything inherently to protect people from exposure to anthrax spores. Demolition could easily re-suspend spores. In the AMI case, the building was decontaminated and then re-sold. Buildings would still have to be decontaminated before they could be safely demolished. Abandonment may pose serious legal and safety issues. The issues associated with demolition and abandonment have not yet been seriously addressed.

## PROGRESS SINCE 2001

### NEW DETECTION TECHNOLOGY

Products for the detection and identification of biological hazards have been developed and put into service or onto the commercial market since 2001. As a general rule of thumb, however, none of these technologies or products provides accurate and real time detection of viable anthrax in a reliable manner. None of the available products allows for instant or even very quick interrogation of a specific surface or substance for the presence of *viable* anthrax spores. Decisions with health and safety ramifications still rely on confirmatory testing. As far as tools to rapidly identify where contamination is present or to test the efficacy of decontamination efforts, we are still more or less where we were in October 2001.

The area where instrumentation has significantly improved has been the reaction to nuisance and hoax alerts. One by-product of the Amerithrax incidents was the greatly increased number of nuisance (generally innocent situations mistaken for hazards) and hoax/copy-cat alerts. Authorities were deluged with calls to respond to unknown or suspicious powders. From a technical standpoint, detecting and identifying anthrax is much harder than detecting nearly anything else. In the case of nuisances and hoaxes, chemical identification technology can identify or at least classify the large majority of unknown powders, allowing responders to make better decisions as to whether a particular situation is safe or unsafe. Products produced by Smiths Detection, Thermo Fisher Scientific and other technology firms now provide reasonable chemical identification products that cost in the tens of thousands of Euros or dollars, not the millions, and can be used by non-specialist personnel. This has proven to be a sea change in on-site investigation of suspicious powders. Properly equipped hazardous materials responders now have the ability to de-escalate the majority of suspicious powder

---

<sup>44</sup> Schmitt and Zacchia, p. 6.



responses because they can determine that a white powder is, say, baking powder and not biological in origin.

## NEW DECONTAMINATION TECHNOLOGY

New products for decontamination have entered the market. The requirement for decontamination of sensitive items and equipment, not just for Amerithrax-like situations but also for items like military aircraft interiors and sophisticated weapon systems has driven military research and development. Some of this work involves peroxides, which tend to be less damaging than chlorine to many materials. Steris, the US medical company with a long history in medical sterilisation, now has peroxide-based systems for fumigation of large items using vaporised hydrogen peroxide, which is less harsh on electronics. An Italian firm, Cristanini, has a peroxide-based system for decontaminating interior spaces, like a room, as well as a surface decontaminant that works on sensitive electronic items. The author has successfully covered his own laptop in the latter solution without incident.

## MEDICAL IMPROVEMENT

There have been great improvements in medical countermeasures. The United States now has a very large emergency stockpile of medical supplies, including enough antibiotics to treat or give chemoprophylaxis to millions of people, although the origins of the stockpile predate the Amerithrax incidents.<sup>45</sup> Clinical guidelines and training for medical personnel are greatly improved, incorporating some of the knowledge gained from the Amerithrax case histories. Improvements to anthrax vaccination, while slow, are underway.

## OPERATIONAL PROCEDURES FOR RECEIPT OF MAIL AND PARCELS

One area that has seen significant progress is the development of new procedures and facilities for receipt of mail and parcels. The risk of death, illness, or contamination of equipment and property can be greatly mitigated if letters and parcels are directed to a remote off-site location or a quarantined mailroom for screening and handling. A spectrum of options is available for those wishing to prevent or mitigate dispersal of anthrax or similar pathogens.

At the low end of the spectrum, packages can be examined and opened by individuals wearing gloves, under a fume hood or in a glove box that exhausts through an appropriate filter. Any contamination is then contained quite easily. Chemical detection technology can be used to examine unknown substances and to rule out many likely false-alarm producing substances.

The middle of the spectrum is remote delivery and screening, wherein all deliveries go to a remote location, separate from the likely target, for detailed screening and opening. Contents can be sent onward by secure means after opening. The advent of inexpensive scanning and imaging technology means that much correspondence does not actually need to physically go to the recipient if it can be scanned and emailed. At the high end of available options, letters and parcels can be sterilised by gamma radiation<sup>46</sup> or electron beams<sup>47</sup>. However, this is an expensive option and not practical for the routine office building. It is more feasible for critical

---

<sup>45</sup> D. Esbitt, 'The Strategic National Stockpile: Roles and Responsibilities of Health Care Professionals for Receiving the Stockpile Assets', *Disaster Management and Response*, vol. 1 no. 3, 2003, pp. 68-70.

<sup>46</sup> T. Horne, G. Turner, and A. Willis, 'Inactivation of Spores of *Bacillus Anthracis* by G-Radiation', *Nature*, 1959, vol 4659: pp. 475-6.

<sup>47</sup> S. Helfinstine et al. 'Inactivation of *Bacillus Endospores* in Envelopes by Electron Beam Irradiation', *Applied and Environmental Microbiology*, Nov. 2005, p. 7029-7032.



infrastructure protection than for routine security. In theory, there could be economy in scale if commercial users clubbed together to buy sterilisation as a service from a vendor.

### FORENSIC AND INVESTIGATIVE IMPROVEMENTS

The ability to investigate similar incidents has greatly improved in the United States and several other countries, particularly the UK. The UK had a broadly similar contamination problem subsequent to the Polonium-210 poisoning of Alexander Litvinenko. Although many of the technical aspects differed widely, the investigation added greatly to the body of knowledge. The US and UK are, procedurally and forensically, far more prepared for complex investigations in this field. The situation is far less clear in other countries. Criminology laboratories are clearly still well separated from CBRN defence laboratories in most countries.

Much knowledge has been gleaned from other investigative disciplines, such as clandestine drug laboratory investigations and environmental crimes. A number of books and articles have been written to transfer this knowledge into CBRN investigations. One of the best examples, recommended for further reading, is *Hot Zone Forensics* by Steven Drielak,<sup>48</sup> and is the closest thing to a canonical work in this field.

### CONCLUSIONS

In late 2001 a small amount of anthrax powder caused death, injury, loss of property, and loss of use of premises. The total cost remains uncalculated but is easily in the billions of dollars. There is a serious question as to whether, from a risk analysis viewpoint, the Amerithrax case can form the basis for extrapolation to other events. It is inconclusive as to whether we can make anything more than a rough order of magnitude estimate about bioterrorism in the future based merely on the Amerithrax events.

From the perspective of contamination and decontamination, and thus loss of large amounts of property, anthrax spores form a near worst-case scenario. They are the most hardened of biological warfare agents and pose, by far, the highest potential for persistent contamination. Other potential biological warfare agents are far easier to decontaminate. Many pose little risk of actual contamination, as many microbes die quickly in the environment.

Part of the problem in extrapolating from Amerithrax is that small changes in could have resulted in either far lesser or far greater amounts of damage. Some things could have occurred that would have greatly mitigated death, illness, contamination, and property damage. Better sealing of the envelopes would have greatly reduced or eliminated contamination within postal facilities and the spread of secondary contamination, albeit at the risk of making the investigation harder. Likewise, even slightly larger particle size would have likely lead to less illness and death, and smaller areas of contamination as larger and heavier particles do not travel so far. Any moisture or dampness along the way might have mitigated the hazard as well.

Conversely, even rather moderate acts or random events could have created circumstances that would have increased lethality and contamination. If the perpetrator had been able to produce even a moderately larger amount of powder or to reduce its particle size even slightly, it would easily have resulted in more lethality and contamination. Sending the letters from multiple

---

<sup>48</sup> S. Drielak, *Hot Zone Forensics: Chemical, Biological and Radiological Evidence Collection*. Springfield (IL), USA, Charles C. Thomas, 2004.

mailboxes spread out over a larger area could have resulted in an order of magnitude increase in contaminated mail facilities. If an envelope had been mangle in mail-handling equipment, significant amounts of secondary contamination could have arrived in mail to people and addresses not targeted. (This is one possible explanation for the death of the elderly victim in Connecticut.)

Only one thing is certain, and that is the next incident, wherever and whenever it occurs, will have different variables and outcomes. We simply do not have enough case histories to start developing viable models for guessing risks, probabilities, and damage from bioterrorism events. The Amerithrax events were illustrative and informative, and they can guide us in many particular aspects. However, any overall conclusions relevant to the insurance, risk, and security sectors are so broad that they have little predictive value.



**Shane Latchman**  
**AVP**  
**AIR Worldwide**

[www.linkedin.com/in/shanelatchman](http://www.linkedin.com/in/shanelatchman)

Shane Latchman is Assistant Vice President in AIR's London office. Shane also plays a key role in some of AIR's Touchstone initiatives, such as the integration of third-party data and models, expanding AIR's capabilities in marine and energy, the Next Generation Financial Module, and the development of future multi-modelling/blending capabilities. He is a member of catastrophe modelling and actuarial industry groups and interacts heavily with rating agencies and regulators on topics such as Solvency II. After receiving a National Scholarship from Trinidad and Tobago, Shane studied Actuarial Science at City University (London) and received a B.Sc. with honours. Assisted by a Cambridge Commonwealth Trust grant, he earned a Master's in Mathematics from the University of Cambridge.

## 10. METHODS TO QUANTIFY TERRORISM RISK

*When assessing natural catastrophe risk, probabilistic model results have long held centre stage. In terrorism risk quantification, however, simpler techniques have historically been used, revolving largely around accumulating exposed limits within a ring. Today, the options available to underwriters and managers of terrorism risk are far more wide-ranging and sophisticated. This article describes three broad methods and their variations. We also note the sensitivity of analysis results with respect to location, or geocoding accuracy. Finally, some best practices for terrorism loss analysis are presented.*

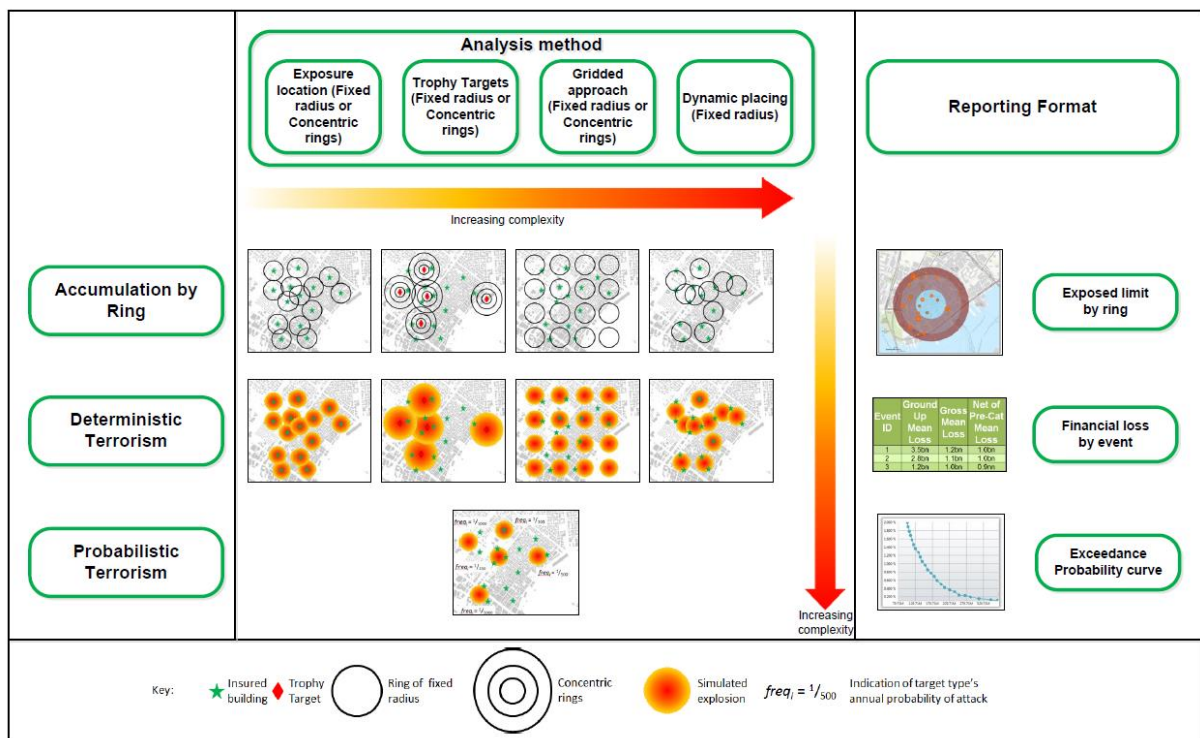


Figure 4: Summary of different types of terrorism risk quantification

## METHODS FOR TERRORISM RISK QUANTIFICATION

### RING ACCUMULATION

For the insurance company wanting to report to ratings agencies the maximum they might lose in any single fire, the industry standard answer has been the exposed limit within a ring, often with a 200m radius, at the centroid of which was “placed” the fire’s ignition. This method relied on a simplified assumption of fire spread, approximating it as a circle of defined radius. The terrorism insurance industry adopted the same method for policies covering blast damage. It was widely used in the aftermath of the 9/11 attacks and is used by regulators today, who, working in the context of Solvency II, ask for the maximum exposure within a 200m radius. AM Best, the ratings agency, also asks for accumulation but within a 500ft (152m) radius. The method, herein called ring analysis, can be performed in a variety of ways with ring centroids being placed on the geocode of each exposed property, or (trophy) targets, or on a grid.

The targets of the simulated terrorist attacks can be chosen in multiple ways - for example, by selecting the types of structures preferred by different terrorist ideologies (e.g. animal testing labs by animal activists, or governmental buildings by domestic anarchists and international terrorist groups). The appropriate selection of potential targets typically requires the input of terrorism risk experts. For a given country, depending on the terrorist threat, the method by which targets are determined, and the size of the country, potential targets can be in the hundreds, thousands, or even tens of thousands.

The grid method uses a ring of fixed radius and moves the ring along a grid of defined spacing. The output is the exposed limit ordered largest to smallest based on the accumulated value within each ring centred at each grid point. Since grid-based methods can fail to find the actual ring of maximum exposure due to the arbitrary constraints imposed by the grid spacing, AIR created a methodology called Dynamic Ring Analysis, which can find the true ring of maximum exposure (assuming no loss of accuracy in projecting the distance calculations from a spherically approximated earth to a flat plane). The method involves placing rings around each insured location; then, where rings intersect a new ring is placed at the centre of the area of intersection of the 2 rings. If more than 2 rings intersect, rings are placed at the centroids of the shapes created by the intersections. Within each created ring, the accumulation is computed and the ring with the maximum exposure (maximum exposed limit) is then identified.

A related methodology to fixed ring analysis is concentric ring analysis. Instead of accumulating 100% of the exposure within a circle of fixed radius, user-defined damage ratios are applied to locations within concentric rings. These damage ratios, or percentages, typically decrease with distance from the centre (the blast site). This methodology is used in Lloyd’s Realistic Disaster Scenarios (RDS) and the Prudential Regulatory Authority (PRA) General Insurance Stress Tests to provide an estimated loss from prescribed events. For example the PRA General Insurance Stress Test 2015 is a 2 tonne bomb detonated in a medium-sized box van next to the Lloyd’s building in London. Losses are to be approximated using circles of radii from 100m to 400m and damage ratios from 60% to 5%.

Another accumulation method, which is not a ring method, is little used due to lack of available data. This method is accumulation of exposure within historical blast footprints, such as the 1992 IRA London bombings. With improved data processing technology, historical images

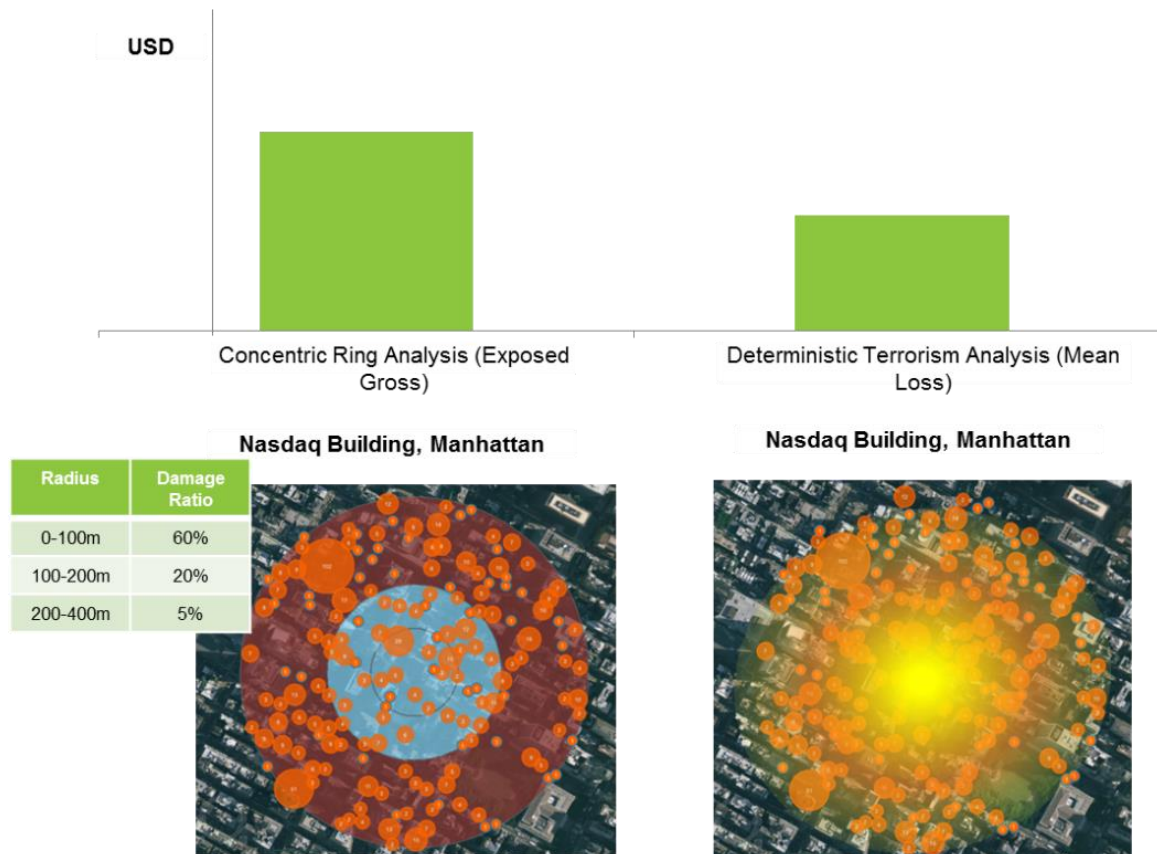
can be geo-tagged and used to create footprints on which to accumulate; such work has been done by some organisations where information is available.

### DETERMINISTIC TERRORISM LOSS ANALYSIS

Whilst ring analysis has been used for some time and is still used today, new methods founded on science (largely physics and engineering) are increasingly being used by underwriters and risk managers as a result of the broad acceptance and use of catastrophe modelling in the (re)insurance industry. Deterministic analysis estimates losses (not exposed limits) from a blast of a defined TNT tonnage and centred at a specific location.

This method is similar to concentric ring analysis except that rather than using defined damage ratios within defined rings, continuous physics-based blast attenuation functions and engineering expertise are used to estimate damage and loss within physically realistic footprints. The simulated blasts are typically placed at trophy targets or at targets specified by regulatory bodies, but can be located anywhere. Three primary pieces of information are used in the deterministic analysis: the urban density of the region where the blast is simulated, the tonnage of the weapon being used, and the vulnerability of the structure to overpressure. As the name suggests, deterministic terrorism scenarios are user defined and are typically not associated with a probability of occurrence.

Clearly, deterministic terrorism analysis will yield different results from concentric ring analysis, which uses prescribed damage ratios at fixed distances from the blast. *Figure 5* illustrates this difference in results for the Lloyd's 2015 terrorism RDS event in New York City. The difference is largely due to the differences in damage ratios applied in each case.



*Figure 5: Example of differences in loss between concentric ring analysis and deterministic terrorism for the Prudential Regulatory Authority (PRA) 2015 General Insurance Stress Tests. Assumed damage*



*ratios are used in the concentric ring analysis and a van bomb (2.5 tonnes TNT) used in the Deterministic case.*

## **PROBABILISTIC TERRORISM LOSS ANALYSIS**

Grappling with the unprecedented scale of losses after the tragic events of 9/11, the (re)insurance industry called for a probabilistic terrorism model and several modelling agencies responded. Probabilistic terrorism modelling requires a large set, or catalogue, of simulated terrorist attacks using a wide variety of weapon types, both conventional and unconventional, at locations across a country but with an associated frequency.

The frequency of attacks by weapon and target type is typically based on the input of security and terrorism experts, whether through the application of game theory, through an iterative technique such as the Delphi method, or some other approach. The Delphi method, initially developed by the Rand Corporation, brings experts to a collective opinion on the frequency of different attack types against specific target types by terrorist group type. Because of the infrequency of major attacks, terrorism models typically incorporate extremely large catalogues (e.g. 500,000 representations of what could happen in a single year) to appropriately capture the range of potential attacks. As with natural catastrophe models, the output of probabilistic terrorism models is an Exceedance Probability (EP) curve giving the probability that a level of loss or greater is experienced in a year.

## **THE IMPORTANCE OF GEOCODING ACCURACY**

Obtaining meaningful results from any of the methods outlined above depends on knowing the location of the exposure. Terrorism risk assessment, like flooding, requires high resolution geocoding since fire or blast radii are typically very small (~100s m). Portfolios coded to a postcode centroid, for example, may not yield sensible results from accumulation or deterministic/probabilistic analyses using conventional weapons (e.g. van bombs) since postcodes can be several square kilometres or larger in area.

To illustrate the sensitivity of results to geocoding, Figure 6 shows how much the modelled loss can vary in a 100m x 100m grid around the Rockefeller Center by moving the centroid of a deterministic terrorism blast in 10m intervals. The difference between the lowest and highest exposed limits (100 values in total) is more than 4x. The loss at a single centroid used to represent Rockefeller Center is shown for comparison and is about 25% of the maximum value in the grid.



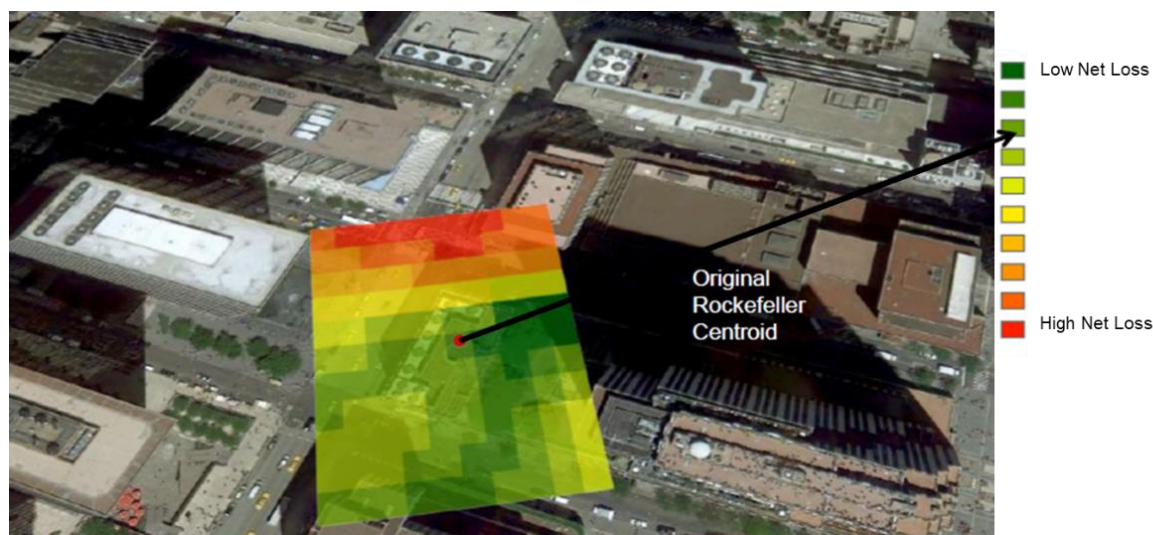


Figure 6: Image showing variation in modelled losses from a van bomb (2.5 tonnes TNT) moved in 10m increments on a 100m x 100m grid outside the Rockefeller Center (used for the Lloyd's 2015 RDS submission). The colours represent the modelled loss with green having the lowest values and red the highest. The red dot is a single lat/long used to represent the Rockefeller centre.

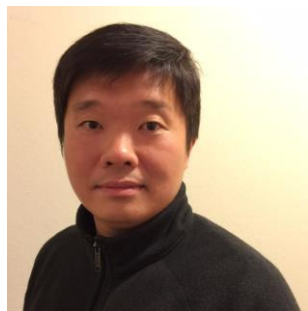
## RECOMMENDATIONS

Today, companies can choose from a variety of tools for assessing and managing terrorism risk. As long as rating agencies and regulators continue to require the results from fixed ring or concentric ring analysis, these methods will remain go-to standards. For internal reporting purposes, however, many companies are relying on the more sophisticated approaches of physically-based deterministic analysis or on EP curves produced by probabilistic terrorism models.

We propose that the best practice for terrorism risk quantification is a multi-faceted one encompassing ring analyses, scenario output and probabilistic results. First, Dynamic Ring Analysis should be run on the portfolio to find the ring of maximum exposure. By varying the radius of the ring used, sensitivity tests can be performed on differing blast radii and to account in some way for geocode uncertainty. The output can then be visualised to identify spatial concentrations of maximum exposure.

Deterministic terrorism loss analysis using a defined weapon type can then be run and the output benchmarked against the accumulation results. Special attention should be paid to areas at high risk, such as those near trophy targets, where deterministic terrorism analysis can be run on high resolution (~tens of metres) grids. Finally, the portfolio can be run against a probabilistic terrorism model and benchmarked against the deterministic and accumulation results, focusing on the return periods relevant to the company's risk appetite.

In combination, these techniques will give a more complete view of risk and help the risk manager understand both the range of potential losses and the probability of their occurrence, ultimately enabling more informed decisions.



**Weimeng Yeo**  
**Principal Modeler, Probabilistic Terrorism Model**  
**RMS**

[www.linkedin.com/in/weimeng-yeo-2104a92](http://www.linkedin.com/in/weimeng-yeo-2104a92)

Weimeng Yeo is a Senior Model Manager at Risk Management Solutions (RMS) for the development of RMS' terrorism modelling solutions. He was previously with the International Centre for Political Violence and Terrorism Research (ICPVTR) a unit of the S.

Rajaratnam School of International Studies (RSIS) Nanyang Technological University, Singapore.

## **11. EVALUATING THE SUNNI-SALAFI JIHADI CBRN THREAT**

One of the more critical elements in the assessment of terrorism risk is the estimation of likelihood of a mass casualty attack using a chemical, biological, radiological, or nuclear (CBRN) agent. CBRN attack is most likely to occur in a commercial business center, potentially generating significant business interruption losses due to evacuation and decontamination, in addition to any property damage or casualties that occur.

The use of chemical, biological, radiological, or nuclear (CBRN) agent by a non-state actor such a terrorist group has always been of great interest among counter terrorism practitioners due to the high severity and low frequency of such events. In the past, there has been a consensus among counter terrorism experts that while there is strong interest by Sunni-Salafi jihadi groups and its affiliates in acquiring a CBRN weapons to execute a mass casualty event, these attacks were unlikely as such agent were expensive, difficult to acquire, complicated to weaponise as well as to deploy. Thus, the conventional wisdom has been that the terrorist intention to acquire and use of CBRN agents has been more or less an aspirational endeavour rather than a tangible one

Nevertheless, recent changes in the security landscape, particularly the upheaval in the Middle East and the rise of the Salafi-jihadi group such as the Islamic State (IS) have made such assertions less convincing. Sunni-Salafi Jihadi groups, such as IS, have shown not only the interest but the resources and capabilities to develop such weapons. By evaluating the Sunni-Salafi jihadi CBRN threat, this paper will offer reasons for this apparent shift and gauge whether current developments indicate a significant change in CBRN terrorism risk. However, before the paper continues, it is prudent to identify potential CBRN weapons and how they will be used.

### **USE OF CBRN WEAPONS**

Although rudimentary CBRN weapons may be relatively easily developed, weaponization of CBRN agents capable of inflicting a mass casualty attack is not a straight forward enterprise. CBRN agents certainly have the potential to inflict significant damage, but this latent effect can only be realized if the agent is actually delivered successfully to the target.

Recent indications of CBRN agent development by Salafi-jihadi groups include the following: In December 2001, U.S. operatives in Afghanistan discovered evidence indicating that Russian scientists were helping al-Qaida weaponize anthrax.<sup>49</sup>

- In November 2002, British security officials arrested three men reportedly plotting a cyanide attack on the Milan, Rome, and Vatican City subways.<sup>50</sup>
- In late 2003, a chemical and biological training manual was recovered from a Jemaah Islamiah safehouse in Cotabato, Philippines. Although crude, the manual displayed an advanced understanding of production of several agents.<sup>51</sup>
- In April 2004, Jordanian authorities reportedly dismantled a large operation where five chemical trucks were being prepared to be used in a strike against five targets.<sup>52</sup>
- In March 2005, Musab al-Zarqawi was believed to be planning a chemical weapons attack in Europe. According to reports, the late Jordanian extremist and his supporters had been trying to get hold of CBRN components in Russia's volatile north Caucasus region and in Georgia.<sup>53</sup>
- In February 2006, a manual for the production of al-Mubtakkar, a crude hydrogen cyanide dispersal device, was published on numerous al-Qaida websites. It now appears to be nearly identical to the device intended for use in the aborted 2003 plot to attack the New York City subway system.<sup>54</sup>
- In October 2006, al-Qaida in Iraq launched this campaign of chlorine bomb attacks by detonating a car loaded with mortars and chlorine tanks in Ramadi, wounding three Iraqi police officers and a civilian.<sup>55</sup>
- In February 2007, insurgents linked to al-Qaida detonated three VBIEDs packed with chlorine in Iraq's Anbar province west of Baghdad. The initial blasts six people, while at least 350 Iraqi civilians and six U.S. troops fell ill as a result of chlorine exposure.<sup>56</sup>
- In January 2011, al-Qaida in the Maghreb closed a base in Algeria after an experiment with unconventional biological weapons went awry, leaving 40 members dead.<sup>57</sup>
- In June 2011, Moldovan police arrested six people suspected of trying to sell a type of uranium that can be used in nuclear weapons. The Associated Press quoted the authorities as saying the uranium had come from Russia and the suspects were trying to sell it to a North African country.<sup>58</sup>
- In August 2014, IS militants attacked Kurdish forces in Iraq with mustard gas. The mustard gas either came from old Iraqi stockpiles produced under Saddam Hussein's rule

<sup>49</sup> Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror*, Columbia University Press, 06/2002, Pg 55.

<sup>50</sup> Rory Carroll, "Four held in Rome after 'Islamist plot to poison water'", *The Guardian*, 02/20/2001.

<sup>51</sup> Rohan Gunaratna, "Attacks of al-Jemaah al-Islamiyah in Southeast Asia", in B. Hoffman (ed.), *The Evolution of the Global Terrorist Threat: From 9/11 to Osama bin Laden's Death*, Columbia University Press, 10/28/2004, pg. 406.

<sup>52</sup> Peter Brookes, *A Devil's Triangle: Terrorism, Weapons of Mass Destruction, and Rogue States*, Rowman & Littlefield, 03/01/2007, pg. 163.

<sup>53</sup> Dan Darling, "Al Qaeda's Mad Scientist, The significance of Abu Khabab's death", *The Weekly Standard*, 01/19/2006.

<sup>54</sup> Ron Suskind, *The One Percent Doctrine*, Simon & Shuster, 07/2006, pg. 102.

<sup>55</sup> Peter Bergen, "Al Qaeda's track record with chemical weapons", CNN, 05/07/2013, <http://www.cnn.com/2013/05/06/opinion/bergen-chemical-weapons-syria/> (accessed 08/01/2013).

<sup>56</sup> Damien Cave and Ahmad Fadum, "Iraqi Militants Use Chlorine in 3 Bombings", *New York Times*, 02/21/2007.

<sup>57</sup> Eli Lake, "Al Qaeda bungles arm experiment", *The Washington Times*, 01/19/2009, <http://www.washingtontimes.com/news/2009/jan/19/al-qaeda-bungles-arms-experiment/> (accessed 08/08/2009)

<sup>58</sup> Andrew Kramer, "Arrests in Moldova Over Possible Uranium Smuggling", *New York Times*, 06/29/2011.

or was manufactured by Islamic State after it seized the University of Mosul. Kurdish soldiers were believed to be poisoned.<sup>59</sup>

- In October 2014, IS militants had used chlorine gas as a weapon against Iraqi police officers in the city of Balad, which is located at the northern part of Iraq. Hospital officials who treated the men, as well as an unnamed Iraqi Defense Ministry official, confirmed the men's suspicion that chlorine gas had been used against them. Eleven officers were made ill, though all survived.<sup>60</sup>
- In August 2015, IS has been suspected of firing a mortar filled with a chemical agent on Kurdish fighters in Northern Iraq. The attack sickened dozens of their troops. The Kurds provided U.S. officials with fragments of shells that later tested positive for the presence of mustard gas.<sup>61</sup>
- In March 2016, IS fighters launched two chemical mortar attacks near the city of Kirkuk. The attack killed a young girl and wounded 600 people. It is believed that the chemical agent was mustard gas.<sup>62</sup>

## CHEMICAL AGENTS

Experimentation with crude chemical agents was common in al-Qaida's training camps in Afghanistan prior to 9/11. Today, however, it appears that the use of chemical agents has largely been left to the discretion of individual cells plotting smaller-scale attacks outside the direct control of the al-Qaida core leadership.

Examples of smaller-scale chemical-related activity include a Bahraini terrorist cell's plot to use a crude cyanide gas device called the "mobtaker" (an Arabic word roughly meaning "invention") in an attack on the New York City subway in early 2003 and Abu Musab al Zarqawi network plotting to use cyanide in multiple attacks planned in Europe in late 2005.<sup>63</sup> An analysis of plots linked to salafi-jihadi groups indicates that sarin, hydrogen cyanide, mustard gas and industrial toxic chemicals such as chlorine compounds have been the chemical weapon of choice for these jihadist groups.<sup>64</sup>

Apart from leveraging a chemical agent, a direct attack on an industrial chemical facility or an assault of a rail car full of toxic chemicals in order to cause a toxic vapor release is a plausible attack scenario. Although not a terrorist attack, the Union Carbide accident that caused a leak of methyl isocyanate gas and other toxic chemicals in Bhopal, India in 1984 illustrated the catastrophic scale of damage that is possible from a chemical release.<sup>65</sup> More than 3,800 fatalities resulted from the accident's initial chemical release, and estimates indicate that more than 200,000 people have been medically affected in the years since.

<sup>59</sup> Kareem Shaheen, Spencer Ackerman and Ian Black, "Mustard gas 'likely used' in suspected Islamic State Attack In Syria, The Guardian, 26/09/2015.

<sup>60</sup> Loveday Morris, "Islamic State militants allegedly used chlorine gas against Iraqi security forces", *The Washington Post*, 10/23/2014

<sup>61</sup> Helene Cooper, "ISIS Is suspected of a Chemical Attack Against Kurds in Syria," *New York Times*, 08/14/2005.

<sup>62</sup> Qassim Abdul Zahra, "ISIS is accused of chemical attack in Iraq that wounds hundreds, kills child," *Washington Post*, 03/12/2016.

<sup>63</sup> Michael Scheuer, "New York Subway Plot and al-Qaeda's WMD Strategy, Terrorism Focus," Terrorism Focus, Volume: 3 Issue: 24  
[http://www.jamestown.org/programs/gta/single/?tx\\_ttnews\[tt\\_news\]=814&tx\\_ttnews\[backPid\]=239&no\\_cache=1](http://www.jamestown.org/programs/gta/single/?tx_ttnews[tt_news]=814&tx_ttnews[backPid]=239&no_cache=1).

<sup>64</sup> Rene Pita, "Assessing al-Qaeda's Chemical Threat," *International Journal of Intelligence and Counter Intelligence*, Vol 20, Issue 3, September 2007, pg. 480.

<sup>65</sup> Alan Taylor, "Bhopal: The World's Worst Industrial Disaster, 30 Years Later", *The Atlantic*, 02/12/2014.



## BIOLOGICAL

Producing and dispersing large quantities of biological agents is a complex and expensive endeavour. But a determined terrorist group could potentially obtain these weapons and the means to deliver them from one of the many countries that are known to have stockpiled biological weapons or have the acumen and capability to produce such agents.

Since 2000, there have been several reports that terrorist groups have been trying to procure and weaponize anthrax bacteria, botulism toxins, and ricin. After the U.S.-led invasion of Afghanistan, American soldiers found at least one chemical weapons laboratory used by al-Qaida.<sup>66</sup> Now, with the growing threat of IS, analysts are concerned that the group may gain access to bio-laboratories in Syria or Iraq.

Be that as it may weaponizing biological agents is not a straight forward process. Most non-state actors do not possess the technology necessary to make such agents a weapon. In addition, each potential biological agent also has individual reasons why it would not make an effective weapon of terror. For example, infectious diseases such as Ebola are only transmitted via direct contact with the bodily fluids of someone infected with the disease. Anthrax is not easily transmitted across individuals and is unlikely to spark an epidemic.<sup>67</sup> Even deadly biological agents like ricin and botulinum are hard to use in mass attacks due to the difficulty in converting them into a weaponized form that can be readily dispersed.

## RADIOLOGICAL MATERIAL

Among the CBRN weapons that a terrorist could launch, a radiological weapon or “dirty bomb,” is the most plausible<sup>68</sup>. The logic behind this argument is three-fold. First, radiological materials are readily available, and relatively easy to obtain. Second, terrorists of the intended target could transport the weapon. Third, the required skills needed to manufacture such a bomb are minor compared to other unconventional weapons.

A “dirty bomb” is designed to spread fissile radioactive material over an extensive area by combining radioactive material with a conventional explosive. The destructive power of a dirty bomb is a function on the size of the bomb and the amounts of radioactive isotopes used. Such attacks do not involve a nuclear explosion and would be unlikely to result in many immediate deaths, but it can still cause significant physical disruption, interruption of economic activity, and psychological trauma to the general populace<sup>69</sup>.

Terrorist groups may have the opportunity to pilfer military, industrial or medical facilities. From time to time there are also incidents of illegal smuggling from former Soviet countries and attempts to sell small quantities on the black market.

Nuclear power plants and related facilities may also be targeted to produce a radioactive release while also causing a significant disruption in power.

---

<sup>66</sup> Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror*, Columbia University Press, 2002, Pg 120.

<sup>67</sup> “Busting the Anthrax Myth, Security Weekly”, *Stratfor*, 07/30/2008, [https://www.stratfor.com/weekly/busting\\_anthrax\\_myth](https://www.stratfor.com/weekly/busting_anthrax_myth).

<sup>68</sup> Bruce Hoffman, “CBRN, Terrorism Post 9-11,” in Russell D. Howard and James Forest (eds.) *Terrorism and Weapons of Mass Destruction*, McGraw-Hill, March 2007.

<sup>69</sup> Ibid.

## NUCLEAR DETONATION DEVICES

A nuclear attack perpetuated by a terrorist group would likely involve the use of a tactical or larger nuclear weapon against a population center or other key target. A device could be built from scratch using local expertise or from recruiting the appropriate scientist from countries with a current nuclear program.

Given the difficulties in building one from scratch, the more likely manner in which a device will be obtained is that it will be stolen from a country's existing inventory or purchased from a rogue state. According to a report done by the Associated Press in October 2015, the FBI successfully foiled four plots by criminal gangs in Eastern Europe to sell nuclear material to IS.<sup>70</sup>

Moreover, major security gaps still exist in Russia's nuclear arsenal. With Russia's violation of key aspects of nuclear international cooperation programs in recent years, it is now unclear how intact are the Russia's nuclear arsenal inventory.<sup>71</sup>

## SALAFI-JIHADI GROUPS AND THE USE OF CBRN AGENTS

Salafi-jihadism is a revivalist Islamic movement that seeks to recreate the true Islamic community and way of life.<sup>72</sup> The Salafi-jihadi movement is broken down into a hierarchal three-tier structure with the groups such as IS or al Qaida core on top, the affiliate groups in the middle and homegrown jihadi groups at the bottom. Framing its cause as a defensive jihad to protect the Muslim population, the group's leaders create a narrative that resonates within the Salafi-jihadi community, motivating them to take up arms to fight for their goals.<sup>73</sup>

While there have not been extensive studies on why terrorist groups acquire and use CBRN weapons, it is still possible to make a number of cogent observations.<sup>74</sup> CBRN agents appeal more to religious terrorist groups such as Salafi-Jihadi groups than to other kinds of terrorist organizations such as ethno-nationalist or separatist terrorist groups. The rationale behind this is that while more "secular" terrorists groups might be hesitant to kill a great number of civilians for fear of alienating support, religious terrorist organizations regard such violence as not only morally justified but expedient for the attainment of their goals. As Bruce Hoffman who was one of the first scholars to look into the lethality of religious terrorist groups, succinctly points out that religion "*functions as a legitimizing force, specifically sanctioning wide-scale violence against an almost open-ended category of opponents*" for the Salafi-Jihadi community.<sup>75</sup>

---

<sup>70</sup> 'FBI Has Foiled Four Plots By Gangs to Sell Nuclear Material to ISIS', *Associate Press*, 10 July 2015.

<sup>71</sup> Amy F. Woolf, "Russian Compliance with the Intermediate Range Nuclear Forces (INF) Treaty: Background and Issues for Congress", *Congressional Research Services*, 04/13/2016, pg. 11.

<sup>72</sup> Mary Habeck, "Knowing The Enemy: Jihadist Ideology and the War On Terror," Yale University Press, 01/04/2006, pg. 30.

<sup>73</sup> Ibid, pg 85.

<sup>74</sup> Due to the lack of any substantial CBRN attacks, empirical analysis of any CBRN attacks has been poor and it is difficult to comprehend the potential motive of attacks by non-State groups using CBRN weapons. For more information, please see Reshmi Kazi, "The Correlation between Non-State Actors and Weapons of Mass Destruction", *Connections: The Quarterly Journal*, Vol. 10, Number 4, 2011, pg. 2.

<sup>75</sup> Bruce Hoffman, "Holy Terror: The Implications of Terrorism Motivated By a Religious Imperative," *Studies in Conflict and Terrorism*, Vol 18, No.4, Winter 1995.



Religiously oriented groups also tend to be more rigid, violent, and less willing to negotiate, in part because they view their conflict in a binary fashion of good against evil. These groups also present a greater threat given their higher proclivity toward mass casualty attacks relative to their secular counterparts. The resurgence of this type of terrorism on such a violent scale over the last decade is unprecedented and will remain the most dangerous category.

For transnational Salafi jihadists like al-Qaeda and IS, a major CBRN operation in West also strengthens their narrative that their jihad is legitimate. Religious credibility and legitimacy are especially important for these groups' recruitment and viability. This point was echoed by the late leader of al-Qaida in 1988<sup>76</sup>:

*"Acquiring weapons for the defense of Muslims is a religious duty. If I have indeed acquired these weapons [of mass destruction], then I thank God for enabling me to do so."*

Salafi jihadi groups know that to recruit new fanatics, it must offer a coherent narrative of strength and divine purpose. With the group's leaders styling themselves as "defenders of their faith", a successful major attack in the West using a CBRN agent will help to reinforce such a narrative.

Together these factors offer reasons for the salafi-jiahdi groups to pursue a CBRN agent for a mass casualty event. But, does intent to use CRBN as a weapon equate to capability?

### THE CAPABILITY: TECHNOLOGICAL AND LOGISTICAL HURDLES

In general, the technological hurdles involved in perpetrating a mass CBRN incident still remain significant. In fact, there have in reality been few successful large-scale terrorist attacks using CBRN agents. The most notable exception is biological and chemical attacks inflicted by the Japanese cult, Aum Shinri Kyo, on the Japanese populace.<sup>77</sup> The attacks killed 19 individuals and injured more than 5,000. The success of Aum Shinri Kyo was likely a result of their operational capabilities: the cult was believed to have \$1 billion in assets at its disposal, a dozen biologists working in research facilities, and the access as well as the autonomy to experiment and develop the agents.<sup>78</sup>

Moreover, if we look at the information on CBRN agents being disseminated by salafi-jihadi groups via cyberspace, it does not instill much "confidence" on whether these groups have the technical acumen to execute such an attack. While most of the technical data found on jihadi websites are valid and accurate, the literature does not offer specific instructions on other important variables of deployment of such weapons. This includes weaponization, manufacture of agents and setting up of an effective delivery system. These are crucial technical considerations when one wants to orchestrate a successful CBRN attack.<sup>79</sup>

The concerns of a nation state covertly providing a CBRN weaponized agent to a terrorist group appear exaggerated as well. National governments are unlikely to provide such materials to

---

<sup>76</sup> Rahimullah Yusufzai, "Osama bin Laden: Conversation With Terror" Time Magazine, 11 January 1999, <http://content.time.com/time/magazine/article/0,9171,989958,00.html>.

<sup>77</sup> Gavin Cameron, "Multi-track Microproliferation: Lessons from Aum Shinrikyo and Al-Qaeda," *Studies in Conflict and Terrorism*, Vol. 22, Number 4, November 1999, pg. 278.

<sup>78</sup> Ibid.

<sup>79</sup> Salama, Sammy & Hansell, Lydia, "Does Intent Equal Capability? Al-Qaeda and Weapons of Mass Destruction," *Non-Proliferation Review*, Vol. 12, Number 3, <http://cns.miis.edu/pubs/npr/vol12/123/123salama.pdf>.

terrorist organizations as they have no control over such groups. In addition, giving a terrorist group a CBRN agent would also expose the donor state to a massive retaliation once the attack has been executed. Just as states will not provide CBRN agents to any terrorist organization, they are highly unlikely to sell them either. This leaves the alternative of stealing one from a nation state, but most states are very meticulous about the security measures implemented around such weapons.<sup>80</sup>

## FORCES OF POSSIBLE PARADIGM SHIFT

Despite these technological and logistical hurdles, there appears to be a possible paradigm shift in terms of CBRN terrorism risk. The current instability in the Middle East, particularly in Iraq, Libya and in Syria has emboldened terrorist groups, particularly IS and other Sunni-Salafi Jihadi groups to increase their interest in acquiring or using CBRN weapons. There are at least seven reasons for this apparent shift.

## ASPIRING TERRORIST GROUPS

First, the conflict in Syria and the insurgency in Iraq have energized the Salafi-jihadi groups. They have emboldened their supporters to orchestrate large scale casualty attacks. More harrowing is the fact that Salafi-jihadi groups have been linked to several CBRN terrorist attacks. Horrific images and witness accounts have led to allegations that militants have used chemical weapons against Kurdish militants in Syria and security forces in Iraq.

In Iraq and Syria, the strongest Salafi-jihadi group is the Islamic State (IS). Apart from their ideology, an even more virulent view of jihad than their counterpart, al-Qaida, the IS with more than 30,000 fighters has shown the willingness and the capability to orchestrate successful large-scale attacks overseas.

Counter terrorism experts have warned that the IS has been working to build out the capabilities to execute mass casualty attacks out of their area of operation, a departure from the group's focus on encouraging lone wolf attacks, outside their domain. Since June 2015, IS has been linked to more than 23 international attacks.<sup>81</sup> The reasons for these attacks would seem to be twofold. First, striking foreign soil helps to divert attention from its territorial losses in order to retain credibility and an aura of potency. Second, jihadi operations overseas are designed to deter further attacks by Western forces in IS strongholds in Iraq and Syria.

## COMPETITION BETWEEN AL-QAIDA AND IS INTENSIFIES

To compound the security situation there is now an intense rivalry between IS and al-Qaida. In 2014, a schism between IS and Al-Qaida arose when the leader of IS, Abu Bakr al-Baghdadi,

---

<sup>80</sup> Peter Bergen, "Reevaluating Al-Qaida's Weapons of Mass Destruction Capabilities," Combating Terrorism Center (CTC) Sentinel, September Issue, <http://www.ctc.usma.edu/posts/reevaluating-al-qaida%E2%80%99s-weapons-of-mass-destruction-capabilities>.

<sup>81</sup> Karen Yourish, Derek Watkins, Tom Giratikoanon and Jasmine C. Lee, 'How Many People Have Been Killed in ISIS Attacks Around The World', [website] *The New York Times*, 16 July 2016. <http://www.nytimes.com/interactive/2016/03/25/world/map-isis-attacks-around-the-world.html?version=meter+at+1&module=meter-Links&pgtype=Multimedia&contentId=&mediaId=&referrer=https%3A%2F%2Fwww.google.com&priority=true&action=click&contentCollection=meter-links-click&r=1>.

proclaimed his 'Caliphate' independently, without the assent of al-Qaida's senior leadership.<sup>82</sup> Since then, both entities have been vying for pre-eminence within the global jihadi movement and the rivalry is entrenched. Both may be at war with the West and committed to the ultimate revival of an Islamic caliphate, but they are deeply divided over strategy, leadership and who should be at the vanguard of the jihadi cause.

As such, attacks by IS have been designed to garner more recruits, financial donors, and prestige away from al-Qaida and vice versa. As rival jihadist groups vie for support and recruits, the risk is that a CBRN weapon would give an additional boost to the status of the first group, thus making such weapons a highly sought after prize. In addition, a group armed with a significant CBRN arsenal would no doubt have some claim to be leading salafi-jihadi group, which carries obvious appeal for recruitment purposes.

### GROUPS ARE LOOKING AT MORE SOPHISTICATED WEAPONS

While conventional attacks such as car bombs will continue to be the attack mode of choice, terrorist groups such as IS will continue to increase their attack repertoires and use more sophisticated weapons. Groups such as al-Qaida and IS - regardless of their goals - need to stay credible to their supporters. Thus, they are compelled to orchestrate more ambitious, 'spectacular' attacks to keep their supporters engaged. Militants already have used experience on the ground in Iraq and Syria to experiment with new technology, which could translate to more catastrophic attack scenarios. For example, IS has been working on using radio-controlled model aircraft to deliver improvised explosive devices.<sup>83</sup> Jihadists in Iraq and Syria are also known to have developed remote-control systems for driverless vehicles to deliver IEDs without using suicide bombers.<sup>84</sup> Such innovation by these groups could lead them in pursuing more advanced weaponry such as an advanced CBRN arsenal.

### SOURCES OF WEALTH

A study done by Thomas Reuters in October 2014 estimates that when IS took over the city of Mosul, the group possessed assets of more than of US\$2 trillion, with an annual income via taxes to population amounting to US\$2.9 billion.<sup>85</sup> While this is a conservative estimate and much of their financial resources would be allocated to run their organization as well as maintain control of their territory, it still offers them ample funding to have a credible viable CBRN program.

In addition, several news sources have also reported that IS has gained considerable wealth from oil. Such sources of funding will make it difficult for opponents of IS to track and limit its funding. Security agencies can target the individuals or groups funding terrorist organizations, but it is much more difficult to crack down on this kind of funding, be it "taxes" paid by the populace to IS, or sale of oil.<sup>86</sup>

---

<sup>82</sup> Charles Lister, "The Syrian Jihad, Al-Qaida, The Islamic State And The Evolution Of The Insurgency", *Hurst*, 2015, pg. 70.

<sup>83</sup> Clay Dillow, "Islamic State Ups The Size and Sophistication of Its Drone Fleet" *Fortune*, 18 April 2016, <http://fortune.com/2016/04/18/islamic-state-ups-its-drone-fleet/>.

<sup>84</sup> Jack Sommers, "Islamic State Experts Modify Missiles And Build Remote-Controlled Car Bombs, 'Jihadi University' Footage Claims" *Huffington Post*, 1 June 2016, [http://www.huffingtonpost.co.uk/2016/01/06/islamic-state-driverless-car-bombs\\_n\\_8920460.html](http://www.huffingtonpost.co.uk/2016/01/06/islamic-state-driverless-car-bombs_n_8920460.html).

<sup>85</sup> Jean-Charles Biscard and Damien Martinez, "Islamic State: The Economy-Based Terrorist Funding," Thomson Reuters, October 2014, pg 3, [http://cat-int.org/wp-content/uploads/2016/06/White-Paper-IS-Funding\\_Final.pdf](http://cat-int.org/wp-content/uploads/2016/06/White-Paper-IS-Funding_Final.pdf).

<sup>86</sup> Ibid, pg. 6.

Such level of funding makes the procurement of supplies to develop CBRN agents a smaller hurdle to overcome. These funds could be applied to the purchase of CBRN weapons, precursor technologies, or the services of scientists who could build same for IS.

#### INCREASED NUMBER OF SAFE HAVENS

A failing state can offer a safe haven in which militants can function freely and provide shelter away from authorities seeking to disrupt their activities. This point was stressed by Abu Bakr Naji, a key salafi-jihadi ideologue, in his book, *Idarat al-Tawahush* (Management of Savagery), where he discusses the importance of establishing safe havens and wrote that for the Salafi-Jihadi movement to be successful it will need to secure multiple safe hinterlands for indoctrination and building capacity purposes<sup>87</sup>.

During the late 1990s to early 2000, al-Qaida adopted such an assessment and leveraged the safe haven facilitated by the Taliban in Afghanistan. They not only set up training camps but also established weapon exploration and procurement centers, including one that was to research and develop CBRN agents.<sup>88</sup> By accepting a partition of these countries or even tacitly allowing IS to maintain control of these areas, the international community risks providing the same opportunity to them.

Despite military efforts against IS, the group still control significant swathes of land in several areas of Iraq, Syria and Libya. A safe haven is of immense strategic value to terrorist groups as it allows them to operate safely and exercise control over subordinates and allocate their resources more efficiently. Thus, members of the IS are not merely fighting on the front lines but they also have authority over substantial swath of territory in both Iraq and Syria. The fear that most counter terrorism practitioners have is that there are people working in IS-controlled campuses of the University of Mosul or in some CBRN facility in the Syrian city of Raqqa, the group's de facto capital, to develop such weapons.

#### ACCESSIBILITY OF A CBRN ARSENAL

International pressure compelled the Assad regime to join the Organization of the Prohibition of Chemical Weapons (OPCW) and the Syrian Defense ministry was forced to turn over its chemical weapon stockpiles. According to the OPCW, the Syrian government declared more than 1,000 tons of chemical weapons.<sup>89</sup> This included blister agents such as mustard gas as well as sarin nerve agents. The OPCW oversaw the destruction of these chemicals. However, while this has reduced the number of chemical agents in the country, it does not preclude the possibility that such agents still exist in undeclared stockpiles. There have been several news reports that indicate that unaccountable stockpiles of chemical weapons still exist in the

---

<sup>87</sup> Abu Bakr Naji, *Idarat al-Tawahush*, "Management of Savagery: The Most Critical Stage through which the Umma Will Pass", *Center for Islamic Studies and Research*, 2005. <http://www.tawhed.ws/a>; English translation available at: <http://www.wcfia.harvard.edu/olin/images/Management%20of%20Savagery%20-%202005-23-2006.pdf>

<sup>88</sup> Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror*, Columbia University Press, June 2002, pg. 105.

<sup>89</sup> Organisation for the Prohibition of Chemical Weapons (OPCW), "Syrian Chemical Destruction Data," 20 October 2014, <http://www.opcw.org/special-sections/syria/destruction-statistics/>.

country.<sup>90</sup> Moreover, unlike the efforts to destroy Syria's chemical weapons no equivalent attempt have been made concerning Syrian's biological weapon arsenal.<sup>91</sup>

As such, access to CBRN materials in Syria is still a significant concern as there are many potential CBRN sites that could be pilfered by a terrorist group. For example, in April 2013, militants targeted the al-Safira chemical facility, a pivotal production center for Syria's chemical weapons program.<sup>92</sup> There have also been strong indication that IS has developed a small-scale chemical weapons program and have manufactured low-quality blister agent from undeclared government stocks.<sup>93</sup>

Another dimension to this issue is the availability of dual use technologies that could be weaponised by militants in Syria, Libya and perhaps even Iraq. It was reported in July 2014 that Islamic State fighters were able to seize more than 80 pounds of uranium from the University of Mosul.<sup>94</sup> Although the material was not enriched to the point of constituting a nuclear threat, the radioactive uranium isotopes could have been used to make a crude radiological dispersal device (RDD).

## ROLE OF FOREIGN JIHADISTS

Finally, the role played by the foreign fighters who have travelled to Syria and Iraq in the past few years also needs to be taken account. The IS success in attracting foreigners has been unparalleled. As of December 2015, there were more than 20,000 foreign individuals joining their group.<sup>95</sup> There are many reasons why so many individuals have travelled to Iraq and Syria to wage jihad. Many have been drawn in by predictions in a version of Islamic ideology that the apocalypse will take place in Greater Syria. Such narrative has been inflamed by stories of atrocities against Sunni Muslims alleged to be committed by the Alawite Assad regime.

Several of these foreign jihadists have attended universities providing the IS a pool of individuals with the requisite scientific expertise to develop and use CBRN weapons. To illustrate this point, in August 2014, a laptop owned by a Tunisian physics university student fighting with the IS, was discovered to contain a document on how to develop bubonic plague and weaponized it.<sup>96</sup>

Many in the counter terrorism field have concerns that individuals with such a background could be given a CBRN agent and then be trained to orchestrate such an attack. With their

---

<sup>90</sup> Most of the facilities and stockpiles that the OPCW were in areas controlled by the Assad regime, However, Walid Muallem, Syria's foreign minister revealed that 7 of the 19 declared sites were in combat zones inaccessible to the OPCW. For more information, see "Can It Be Done?" *The Economist*, 11 May 2013, <http://www.economist.com/news/middle-east-and-africa/21587239-destroying-chemical-arsenal-midst-civil-war-unprecedented-can-it>.

<sup>91</sup> Gary Ackermen and Ryan Pereira, "Jihadist and WMD: a re-valuation of the future threat" CBRNEWorld, 24 October 2010, pg. 27, [http://www.cbrneworld.com/uploads/download\\_magazines/Jihadists.pdf](http://www.cbrneworld.com/uploads/download_magazines/Jihadists.pdf).

<sup>92</sup> Colin Freeman, "Syria: Al-Qaeda's battle for control of Assad's chemical weapons plant" *The Telegraph*, 27 April 2013.

<sup>93</sup> Kareem Shaheen, Spencer Ackerman and Ian Black, "Mustard gas 'likely used' in suspected Islamic State Attack In Syria", *The Guardian*, 26 September 2015.

<sup>94</sup> Caroline Mortimer, "Highly dangerous' radioactive material stolen, sparking fears of Isis 'dirty bomb'" *The Independent (UK)*, 17 February 2016.

<sup>95</sup> An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq, The Soufan Group, December 2015, [http://soufangroup.com/wp-content/uploads/2015/12/TSG\\_ForeignFightersUpdate3.pdf](http://soufangroup.com/wp-content/uploads/2015/12/TSG_ForeignFightersUpdate3.pdf).

<sup>96</sup> Harold Doornbos and Jenan Moussa, "Found: The Islamic State's Terror Laptop Of Doom", 28 August 2014, <http://foreignpolicy.com/2014/08/28/found-the-islamic-states-terror-laptop-of-doom/>.



training, they might even return to their countries of origin to conduct such attacks back in their homeland.

## CONCLUSION

This paper has explored and discussed the threat and consequences emanating from CBRN weapons by Salafi-jihadi groups. Recent development in the Middle East support the assessment that terrorist groups such as IS continue to show keen desire to acquire and develop such weapons. Based on anecdotal evidence, there is already enough credible information to show that IS has at least a nascent CBRN program. Fortunately, obtaining a CBRN capable of killing hundreds, much less thousands, is still a significant technical and logistical challenge. Al-Qaida in the past has tried unsuccessfully to acquire such weapons, while the counter-terrorism forces globally have devoted significant resources to prevent terrorist groups from making any breakthrough.

Current evidence suggests that the Salafi-jihadists are still far from such capabilities, and at best can only develop crude chemical or radiological agents that are more suited for smaller attacks. Despite these challenges, interest in advanced CBRN arsenal has yet to diminish thanks to the potential for high severity outcomes that cannot be produced by conventional attacks such as car bombs. What is compounding the CBRN risk landscape is that groups such as IS with their sizeable financial resources, their success in recruiting skilled individuals, and the availability of CBRN materials in Iraq and Syria, has increased the probability that they could carry out a successful large CBRN attack. These groups will be relentless in its pursuit and will someday overcome their capability constraints.

## BIBLIOGRAPHY

- Abu Bakr, Naji, Idarat al-Tawahush, "Management of Savagery: The Most Critical Stage through which the Umma Will Pass", Center for Islamic Studies and Research, 2005. [http://www.tawhed.ws/a/](http://www.tawhed.ws/a;); English translation available at: <http://www.wcfia.harvard.edu/olin/images/Management%20of%20Savagery%20-%202005-23-2006.pdf>
- Abdul Zahra, Qassim, "ISIS is accused of chemical attack in Iraq that wounds hundreds, kills child," *Washington Post*, 12 March 2016.
- Ackermen, G. and Pereira, R. "Jihadist and WMD: a re-valuation of the future threat". CBRNEWorld, 24 October 2010, [http://www.cbrneworld.com/uploads/download\\_magazines/Jihadists.pdf](http://www.cbrneworld.com/uploads/download_magazines/Jihadists.pdf)
- Bergen, Peter, "Al Qaeda's track record with chemical weapons", CNN, 7 May 2013, <http://www.cnn.com/2013/05/06/opinion/bergen-chemical-weapons-syria/>.
- Bergen, Peter, "Reevaluating Al-Qaida's Weapons of Mass Destruction Capabilities," Combating Terrorism Center (CTC) Sentinel, September Issue, <http://www.ctc.usma.edu/posts/reevaluating-al-qaida%E2%80%99s-weapons-of-mass-destruction-capabilities>.
- Biscard, Jean-Charles and Martinez, Damien, "Islamic State: The Economy-Based Terrorist Funding," Thomson Reuters, October 2014, [http://cat-int.org/wp-content/uploads/2016/06/White-Paper-IS-Funding\\_Final.pdf](http://cat-int.org/wp-content/uploads/2016/06/White-Paper-IS-Funding_Final.pdf).
- Brookes, Peter, *A Devil's Triangle: Terrorism, Weapons of Mass Destruction, and Rogue States*, Rowman & Littlefield, 1 March 2007.
- Dillow, Clay, "Islamic State Ups The Size and Sophistication of Its Drone Fleet" *Fortune*, 18 April 2016, <http://fortune.com/2016/04/18/islamic-state-ups-its-drone-fleet/>.



- Cameron, Gavin, "Multi-track Microproliferation: Lessons from Aum Shinrikyo and Al-Qaeda," *Studies in Conflict and Terrorism*, Vol. 22, Number 4, November 1999.
- Cooper, Helene, "ISIS Is suspected of a Chemical Attack Against Kurds in Syria," *New York Times*, 14 August 2005.
- Darling Dan, "Al Qaeda's Mad Scientist, The significance of Abu Khabab's death", *The Weekly Standard*, 19 January 2006.
- Cave, Damien and Fadam, Ahmad, "Iraqi Militants Use Chlorine in 3 Bombings", *New York Times*, 21 February 2007.
- Doornbos, Harold and Moussa, Jenan, "Found: The Islamic State's Terror Laptop Of Doom", 28 August 2014, <http://foreignpolicy.com/2014/08/28/found-the-islamic-states-terror-laptop-of-doom/>.
- Freeman, Colin, "Syria: Al-Qaeda's battle for control of Assad's chemical weapons plant" *The Telegraph*, 27 April 2013.
- Gunaratna, Rohan, *Inside Al Qaeda: Global Network of Terror*, Columbia University Press, June 2002.
- Gunaratna, Rohan, 'Attacks of al-Jemaah al-Islamiyah in Southeast Asia', in B. Hoffman (ed.), *The Evolution of the Global Terrorist Threat: From 9/11 to Osama Bin Laden's Death*, Columbia University Press, 28 October 2004.
- Habeck, Mary, "Knowing The Enemy: Jihadist Ideology and the War On Terror," Yale University Press, 4 January 2006.
- Hoffman, Bruce, "CBRN, Terrorism Post 9-11," in Russell D. Howard and James Forest (eds.) *Terrorism and Weapons of Mass Destruction*, McGraw-Hill, March 2007.
- Hoffman, Bruce, "Holy Terror: The Implications of Terrorism Motivated By a Religious Imperative," *Studies in Conflict and Terrorism*, Vol 18, Number 4, Winter 1995.
- Kazi, Reshmi, "The Correlation between Non-State Actors and Weapons of Mass Destruction", *Connections: The Quarterly Journal*, Vol. 10, Number 4, 2011.
- Kramer, Andrew, "Arrests in Moldova Over Possible Uranium Smuggling", *New York Times*, 29 June 2011.
- Lake, Eli, "Al Qaeda bungles arm experiment", *The Washington Times*, 19 January 2009, <http://www.washingtontimes.com/news/2009/jan/19/al-qaeda-bungles-arms-experiment>
- Lister, Charles, "The Syrian Jihad, Al-Qaida, The Islamic State And The Evolution Of The Insurgency", Hurst, 2015.
- Rory, Carroll, 'Four held in Rome after 'Islamist plot to poison water,' *The Guardian*, 20 February 2001.
- Meulenbelt, Stephanie and Nieuwenhuizen, Maarten, "Non-State actors' pursuit of CBRN weapons: From Motivation to potential humanitarian consequences", International Review of the Red Cross (2015). [https://www.icrc.org/en/download/file/24548/irc97\\_17.pdf](https://www.icrc.org/en/download/file/24548/irc97_17.pdf)
- Morris, Loveday, "Islamic State militants allegedly used chlorine gas against Iraqi security forces", *The Washington Post*, 23 October 2014
- Mortimer, Caroline, "Highly dangerous' radioactive material stolen, sparking fears of Isis 'dirty bomb'" *The Independent (UK)*, 17 February 2016.
- Pita, Rene, "Assessing al-Qaeda's Chemical Threat," *International Journal of Intelligence and Counter Intelligence*, Vol. 20, Issue 3, September 2007.
- Scheuer, Michael, "New York Subway Plot and al-Qaeda's WMD Strategy, Terrorism Focus," *Terrorism Focus*, Vol. 3, Issue 24, [http://www.jamestown.org/programs/gta/single/?tx\\_ttnews\[tt\\_news\]=814&tx\\_ttnews\[backPid\]=239&no\\_cache=1](http://www.jamestown.org/programs/gta/single/?tx_ttnews[tt_news]=814&tx_ttnews[backPid]=239&no_cache=1).
- Shaheen, Kareem, Ackerman, Spencer and Black, Ian, "Mustard gas 'likely used' in suspected Islamic State Attack In Syria", *The Guardian*, 26 September 2015.

Sommers, Jack, "Islamic State Experts Modify Missiles And Build Remote-Controlled Car Bombs, 'Jihadi University' Footage Claims" *Huffington Post*, 1 June 2016, [http://www.huffingtonpost.co.uk/2016/01/06/islamic-state-driverless-car-bombs\\_n\\_8920460.html](http://www.huffingtonpost.co.uk/2016/01/06/islamic-state-driverless-car-bombs_n_8920460.html).

Suskind, Ron, *The One Percent Doctrine*, Simon & Shuster, July 2006.

Taylor, Alan, "Bhopal: The World's Worst Industrial Disaster, 30 Years Later", *The Atlantic*, 12 February 2014.

Woolf, Amy F., "Russian Compliance with the Intermediate Range Nuclear Forces (INF) Treaty: Background and Issues for Congress", Congressional Research Services, 13 April 2016.

Yusufzai, Rahimullah, "Osama bin Laden: Conversation With Terror" *Time Magazine*, 01/11/1999, <http://content.time.com/time/magazine/article/0,9171,989958,00.html>.

Salama, Sammy & Hansell, Lydia, "Does Intent Equal Capability? Al-Qaeda and Weapons of Mass Destruction," *Nonproliferation Review*, Vol. 12, Number 3, <http://cns.miis.edu/pubs/npr/vol12/123/123salama.pdf>.

Yourish Karen, Watkins Derek, Giratikoanon Tom and Lee C. Jasmine, "How Many People Have Been Killed in ISIS Attacks Around The World", [website] *The New York Times*, 16 July 2016, <http://www.nytimes.com/interactive/2016/03/25/world/map-isis-attacks-around-the-world.html?version=meter+at+1&module=meter-Links&pgtype=Multimedia&contentId=&mediaId=&referrer=https%3A%2F%2Fwww.google.com&priority=true&action=click&contentCollection=meter-links-click&r=1>.

Organisation for the Prohibition of Chemical Weapons (OPCW), "Syrian Chemical Destruction Data," 20 October 2014, <http://www.opcw.org/special-sections/syria/destruction-statistics/>.

"An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq", The Soufan Group, December 2015, [http://soufangroup.com/wp-content/uploads/2015/12/TSG\\_ForeignFightersUpdate3.pdf](http://soufangroup.com/wp-content/uploads/2015/12/TSG_ForeignFightersUpdate3.pdf).

"Busting the Anthrax Myth, Security Weekly", Stratfor, [https://www.stratfor.com/weekly/busting\\_anthrax\\_myth](https://www.stratfor.com/weekly/busting_anthrax_myth).

"Can It Be Done?" *The Economist*, 5 November 2013, <http://www.economist.com/news/middle-east-and-africa/21587239-destroying-chemical-arsenal-midst-civil-war-unprecedented-can-it>.

"FBI Has Foiled Four Plots By Gangs to Sell Nuclear Material to ISIS", *Associate Press*, 10 July 2015.



**Jerry Smith, OBE**  
**Managing Director**  
**Ramehead Consulting**

<https://uk.linkedin.com/in/jerrysmith77>

Jerry Smith, OBE is an independent security risk management consultant, specialising in CBRNE threat management. He has over 25 years experience of global security risk management within Bomb-Disposal, Counter-Terrorism, Humanitarian De-mining and WMD Counter-Proliferation.

## 12. NON-CONVENTIONAL TERRORISM HAZARDS

### SUMMARY

In the latter part of the twentieth century, terrorist attacks in OECD countries typically consisted of direct assaults on the forces of government, or large bombs abandoned (with a warning) to damage and destroy property of significance. In the recent past there has been a palpable shift in targets and method of attack. The terrorist of today is willing to take life indiscriminately and utilises the access of the internet to propagate terror on a global scale.

There is much conjecture that these changes are still evolving. There are a number of hazards today that can be considered as potential tools for a future terrorist attack. However predicting the chance and consequence of such attacks is an extremely complex and challenging task. In many cases the perception of risk based on the unknown effects is perhaps greater than the actual effect.

The paper outlines the principal issues for non-conventional terrorism insurance products that cover such events in the future.

### BACKGROUND

On 22 July 2011 the Norwegian fascist Anders Breivik marked a sea-change in terrorist attacks in OECD countries. After abandoning a one tonne vehicle-borne improvised explosive device (VBIED) in Oslo's government quarter,<sup>97</sup> he travelled to a political rally being held on the island of Utøya. Dressed as a police officer and armed with a rifle and pistol, he killed indiscriminately. 77 people died as a result of the bomb and his firearms attack. A further 300 were injured, with property damage to the Prime Minister's Office and other buildings.<sup>98</sup>

Whilst terrorist bombs targeting property were considered 'conventional terrorism', mass shootings by politically motivated individuals were more of a rarity. Most terrorist gun attacks in Western Europe occurred in counties suffering internal conflict, such as the UK (Northern Ireland) and Spain, with the occasional international incident such as the 1972 Munich Olympics attack.

---

<sup>97</sup> Dagbladet "Unique" that bomb just killed eight people' (translated from Norwegian) [http://www.dagbladet.no/2011/08/01/nyheter/innenriks/terror/anders\\_breivik/17510788/2011](http://www.dagbladet.no/2011/08/01/nyheter/innenriks/terror/anders_breivik/17510788/2011).

<sup>98</sup> BBC News. 'How Norway's terror attacks unfolded' <http://www.bbc.co.uk/news/world-europe-14260297/2012>.

Non-conventional hazards can be described as methods or materials that have seldom been employed in the past by terrorists, but have a potential to be used in the future. In the latter part of the twentieth century, terror groups operating in OECD States tended to impose limits on themselves as to what they considered to be legitimate means or targets. Typically there was an emphasis on attacking economic, political or military targets and an avoidance of mass civilian casualties.

This situation has now shifted. Structured and measured political terrorist organisations have been displaced by nihilistic extremist ideas. The global advance in mass, anonymous and mobile communication has allowed such concepts to be propagated, reinforced and directed by a remote leadership.<sup>99</sup> This shift has been compounded by the use of suicide bombers, a technique rarely seen in the past.

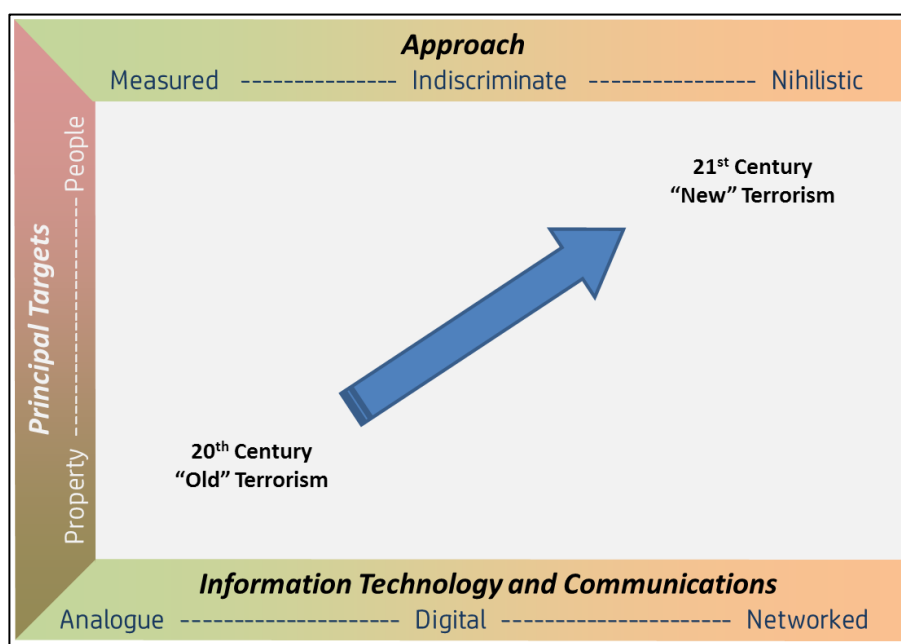


Figure 1. The shift in threat (Adapted from a Pool Re presentation, September 2015)

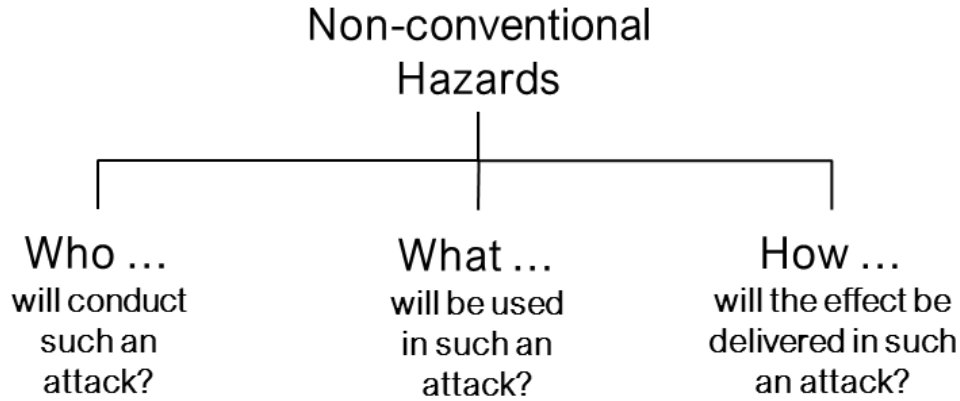
The UK government introduced the term Marauding Terrorist Firearms Attack (MTFA) to describe the Mumbai / Paris-type events where a roaming team of terrorists seek out targets of opportunity and employ military-style close-quarter battle techniques with firearms, grenades and suicide vests. It is these types of attacks, significantly more challenging to counter than a relatively static bomb incident, that are likely to be the norm for the foreseeable future.

## AIM

The aim of this paper is to outline the principal issues and potential requirements for non-conventional terrorism insurance products that cover such events in the future.

This paper is divided up into the Who? What? & How? of non-conventional terrorist hazards.

<sup>99</sup> Aon. 'The changing face of terrorism.' <http://www.aon.com/forms/2015/2015-Terrorism-White-Paper.jsp>



## WHO ...

Currently the multifarious individuals and groups that are a part of, or align themselves with, Da'esh / ISIS pose the greatest terror threat to the West.<sup>100</sup> As well as fighting a quasi-conventional war to gain and hold territory in the Middle East and North Africa, the group encourages and supports direct terrorist actions in the West. In order to take the fight to their enemy, Da'esh can call upon a number of different capabilities.

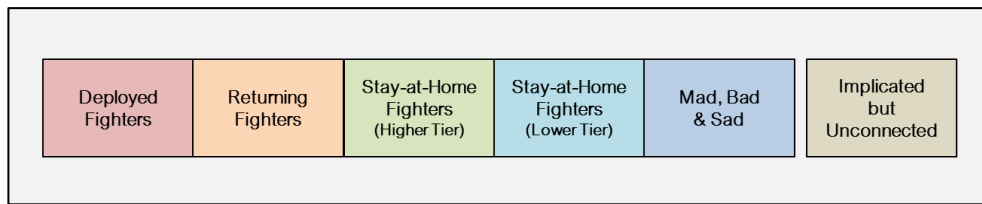


Figure 2. Da'esh offensive human resources.

The people who make up these hazard capabilities are not homogeneous, but can be categorised into a number of distinct types:

- **Deployed Fighters:** Sent from Da'esh territory to conduct specific tasks / missions, they are likely to have a higher-tier capability such as combat experience as well as knowledge of military tactics and weapons. An example is the three-man group that attacked Istanbul airport with small arms and suicide vests in late June 2016.<sup>101</sup>
- **Returning Fighters:** Returning to their home nations from Da'esh territory. No specific mission planned, but available to conduct attacks as opportunity presents. They also possess higher-tier capabilities and can gain access to weaponry and explosives. An example is the group that carried out the Brussels suicide bombings in March 2016.<sup>102</sup>
- **Stay-at-Home Fighters (Higher-tier):** Online and/or local radicalisation with a particular high-tier capability such as scientific knowledge (chemistry, biology, physics) or bomb making. An example is the group that conducted the London 7/7 bombings in 2005 (although the leader probably received training in Pakistan).

<sup>100</sup> US State Department. 'Country reports on terrorism.' <http://www.state.gov/documents/organization/258249.pdf>

<sup>101</sup> Doherty et al. The Guardian. 'Istanbul airport attack' <https://www.theguardian.com/world/live/2016/jun/29/istanbul-ataturk-turkey-airport-attack-explosions-rolling-report-updates>

<sup>102</sup> Henley, 'Brussels attacks', *The Guardian*, 2016, <https://www.theguardian.com/world/2016/mar/24/brussels-police-attacks-identify-man-suicide-bomber-accomplice>

- **Stay-at-Home Fighters (Lower-tier):** Online and/or local radicalisation with non-specific lower tier capability (bladed weapons, motor vehicles). An example is the two who attacked Fusilier Lee Rigby in Woolwich in May 2013.

The added advantage for Da'esh is that with global communication, unconnected individuals can be identified as being part of their movement, despite no previous particular religious conviction.

- **Mad, Bad & Sad:** Unconnected self-loathing individuals with little / no specific radicalisation pathway. Possessing a lower-tier capability, they employ the terminology and imagery of radical religion to gain attention and seeking to justify self-immolation whilst murdering as an act of penance. Examples include the 2016 attacks in Orlando and Nice.
- **Implicated but unconnected:** Criminal acts involving participants that can be easily / lazily identified as fitting one of the other profiles. Whilst the perpetrators do not claim any Da'esh affiliation, the participants and nature of the attack may lead news and social media commentators to draw inaccurate conclusions.

## WHAT ...

Whilst MTFA-style attacks are becoming less uncommon; chemical, biological and radiological (CBR) weapons have yet to play a significant part in terror attacks.

Although it is convenient to group these hazards together, it can sometimes be misleading. Many CBR agents' characteristics, such as their speed of action, effect and fragility, vary greatly. And despite the tomes written on their threat, it is perhaps the general fears of the unknown that these weapons possess which is their greatest effect.

## THE RADIOLOGICAL HAZARD

The sheer quantity and variety of use of radiological sources in OECD States suggests that it might be the easiest of the non-conventional hazards to be employed as a terror weapon. Such material cannot easily be manufactured; it would need to be stolen or otherwise acquired.

There is the theoretical possibility of employing nuclear fuel (either attacking it in-place or removing it off-site) as a radiological weapon. But such material is very heavily guarded and its' inherent hazard can pose a significant danger to those who might use it as a weapon. The International Atomic Energy Agency (IAEA) plays a very active role in developing and maintaining safety and security standards for power stations.<sup>103</sup>

The most-discussed radiological hazard is the dirty bomb. These weapons are commonly characterised as having a payload of hazardous radioactive material, combined with a high explosive charge. The aim is to use the explosive to atomise and disperse the radioactive material in order to cause a wide area effect.<sup>104</sup>

However there are many other ways in which radiological material can be used to do harm. Material could be suspended in a liquid and sprayed or laced into food or drink (à la

<sup>103</sup> The IAEA Vienna Declaration, 'Reaffirming the emphasis on civil nuclear safety.' [https://www.iaea.org/sites/default/files/cns\\_viennadeclaration090215.pdf](https://www.iaea.org/sites/default/files/cns_viennadeclaration090215.pdf)

<sup>104</sup> Federation of Atomic Scientists. 'Weapons of mass disruption.' <http://fas.org/ssp/docs/021000-sciam.pdf>



Litvinenko).<sup>105</sup> An incendiary device could be built that disperses radiological particulate within a smoke plume. And an unshielded gamma / X-ray emitter could be just left in a high footfall / population area, where passers-by may receive a radioactive dose.

The IAEA categorises radiological material depending on its nature, effects and availability.<sup>106</sup> Of particular concern are sources used in hospital radiation therapy (Iodine-125, Cobalt-60 & Caesium-137), research and industrial radiography (Cobalt-60, Caesium-137, Iridium-192 & Radium-226). Strontium-90 also has some industrial application, and larger quantities are used in remote-area electrical generation power-packs and were popular in the former Soviet Union.

In 2013 a cobalt-60 medical treatment source was stolen in Mexico, probably by opportunistic thieves.<sup>107</sup> There had been concern that the device had been taken to produce a dirty bomb. It was later abandoned, but not before they had tried to open the shielding, possibly exposing themselves to near-fatal doses of gamma radiation.



*Figure 3. A Mexican official examines a stolen cobalt-60 source, 2013 (Associated Press)*

The IAEA's Incident and Trafficking Database recorded an average of 35 radiological source thefts every year between 2008 and 2015.<sup>108</sup> The report noted that *"A small number of these incidents involved seizures of kilogram quantities of potentially weapons-usable nuclear material, but the majority involved gram quantities."*

Unless accompanied by an explosion, a radiological attack may go unnoticed for days. It will take the recognition by health services of uncommon effects or a concentration of radiological-poisoned victims. Once identified, and depending on the isotope(s) involved, it may take more time to identify the source location. Furthermore radiological material cannot be neutralised or decontaminated. All that can be done is for it to be removed and stored in a secure location until the hazard has reduced naturally; for some isotopes this can be many decades.<sup>109</sup>

<sup>105</sup> Owen, 'The Litvinenko Enquiry', 2016, <https://www.litvinenkoinquiry.org/files/Litvinenko-Inquiry-Report-web-version.pdf>

<sup>106</sup> IAEA 'Categorization of Radioactive Sources.' [http://www-pub.iaea.org/MTCD/publications/PDF/Pub1227\\_web.pdf](http://www-pub.iaea.org/MTCD/publications/PDF/Pub1227_web.pdf)

<sup>107</sup> BBC, 'Medical radioactive material truck stolen.' <http://www.bbc.co.uk/news/world-latin-america-25212648>

<sup>108</sup> IAEA. 'Incident and Trafficking database'. <http://www-ns.iaea.org/downloads/security/itdb-fact-sheet.pdf>

<sup>109</sup> NDT-resource Centre. 'Radioactive Half-lives' <https://www.nde-ed.org/EducationResources/HighSchool/Radiography/halflife2.htm>

Whilst the radiological hazard primarily affects people, caesium-137 is of particular interest. Given sufficient time, it can chemically bind to concrete; rendering it extremely difficult to remove for disposal. In this case the contaminated part of the concrete may have to be removed; with potential to significantly increase building clean-up and rebuild costs.

## THE CHEMICAL HAZARD

An attack involving a chemical hazard is likely to be noticeable within minutes - hours. Along with multiple casualties displaying similar signs and symptoms, there may be particularly pungent odours or an absence of living wildlife.

Acquisition of the classic 'war gases', such as Mustard or Nerve agent, will become even more challenging as the last remaining declared stockpiles are destroyed. A few countries such as North Korea, Egypt and Israel, remain outside the international chemical treaty and may still possess significant quantities. Other states, including Iran and Syria, are openly accused by the US of maintaining an offensive chemical weapon capability.<sup>110</sup> Given that it can be possible to identify the manufacturers of chemical weapon material from residual samples; potential rogue states might be quite reticent in supplying a terror group for fear of being identified.

The improvised manufacture of chemical weapons is not an insignificant challenge. International treaties and agreements, such as the Chemical Weapons Convention<sup>111</sup> and The Australia Group,<sup>112</sup> place substantial efforts into regulating and monitoring the manufacture, movement and consumption of potentially hazardous chemicals. The technical challenges also require specific knowledge and equipment. There also remains the major difficulty for terror groups to contain, move, store and weaponise such material acquired in the Middle East for use in OECD countries.



Figure 4. Sampling and analysis of a legacy chemical weapon in SE Asia. 2012 (Author)

Rather than seeking to employ chemical material specifically designed as a poison, terrorist could consider using industrial chemicals. Whilst few of these materials have anywhere near the toxicity of war gases, they are likely to be easier to acquire. One approach would be to attack a chemical storage facility, forcing an uncontrolled leak. Whilst not terrorism, the 1984 Bhopal incident<sup>113</sup> demonstrated the potential consequences of a covert attack on a chemical industrial site.

<sup>110</sup> US Department of State. 'Comment on countries' adherence to international arms-control agreements.' <http://www.state.gov/documents/organization/255776.pdf>

<sup>111</sup> OPCW. 'The CWC.' <https://www.opcw.org/chemical-weapons-convention/>

<sup>112</sup> The Australia Group. <http://www.australiagroup.net/en/>

<sup>113</sup> Broughton. US NIH. 'The Bhopal Disaster.' <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1142333/>

An alternative is to acquire a quantity of toxic material and move it to a location where it might cause the most effect. Hundreds of tonnes of hazardous materials are shipped on roads, railways and by sea. Hijacking one such container and opening it explosively could cause major disruption in a city centre or transport hub.

In 1996 a multi-national working group developed a structured approach to defining risk of toxic industrial chemicals (TICs).<sup>114</sup> Subsequently the list was refined into a hazard index that takes into consideration the dangerous chemicals' availability, toxicity and other characteristics.<sup>115</sup> The highest hazard chemicals include: Ammonia & sulphur dioxide (particularly common), chlorine (the first effective chemical weapon in war and still being used in Syria) as well as phosgene & hydrogen cyanide (particularly toxic). Methyl isocyanate, the chemical responsible for several thousand fatalities in the Bhopal tragedy, is rated as a medium hazard.

### THE BIOLOGICAL HAZARD

In spite of the complexity of the natural world, the number of potentially hazardous biological organisms is relatively small. The US Centre for Disease Control (CDC) has three levels of hazard classification; based around a pathogen's transmissibility, lethality and treatability.<sup>116</sup> The highest, level-A, pathogens include: smallpox, anthrax, plague, ebola and tularaemia. These and other pathogens were investigated for weapons' research for much of the 20<sup>th</sup> Century.

The principal issue of managing a biological weapon event is simply identifying whether an attack has actually taken place. Signs and symptoms usually take hours - days to appear and if the attack was covert, then it could be weeks before it was recognised as such. Clues might include the outbreak of a new or unusual disease, or a disease that is particularly virulent a non-endemic area. As well as treating the infected, mass prevention strategies such as vaccination and infection control may also be implemented. All these measures are likely to contribute to a heightened concern amongst the public and the potential for significant disruption, by which time the perpetrators may be long gone.

Another challenge to an effective international approach to a biological weapons hazard is the relatively small size and scope of the Biological Weapons Convention (BWC). Unlike the organisations that monitor and control the radiological, nuclear and chemical treaties, the BWC unit comprises of a handful of people; whose primary role is to simply administer the convention.<sup>117</sup> However UN members are increasingly improving their engagement with the 1540-Committee; a body charged with improving the international response on all WMDs, and with a focus on biological weapons.<sup>118</sup>

---

<sup>114</sup> Wikileaks. 'CANUKUS work on TICs.' [http://download.cabledrum.net/wikileaks\\_archive/file/us-uk-ca-mou-ittf25-1996.pdf](http://download.cabledrum.net/wikileaks_archive/file/us-uk-ca-mou-ittf25-1996.pdf)

<sup>115</sup> US Department of Labor. 'TICs Guide.' <https://www.osha.gov/SLTC/emergencypreparedness/guides/chemical.html>

<sup>116</sup> US CDC. 'Bioterrorism overview.' <http://emergency.cdc.gov/bioterrorism/overview.asp>

<sup>117</sup> UN Geneva Office. 'The BWC ISU.' [http://www.unog.ch/80256EE600585943/\(httpPages\)/16C37624830EDAE5C12572BC0044DFC1?OpenDocument](http://www.unog.ch/80256EE600585943/(httpPages)/16C37624830EDAE5C12572BC0044DFC1?OpenDocument)

<sup>118</sup> UN. 1540 committee. <http://www.un.org/en/sc/1540/>

Effective healthcare plays a significant role in the response to a disease outbreak. Many of the issues that prolonged the Ebola outbreak in West Africa in 2014 - 15 were as a result of a slow response by the international community and a chronically underfunded healthcare system. This was compounded by limited infrastructure and communication, as well as a poorly educated and informed population.<sup>119</sup> However it would be extremely difficult to employ Ebola as some sort of suicide terror weapon. The period of infectiveness coincides with when a carrier is almost completely incapacitated.



Figure 5. International biological experts training in pathogen sampling, 2015. (Author)

An attack on agriculture, particularly livestock, is another potential cause for concern. For many countries, the rapid infection of farm animals could have a devastating effect on a national economy.<sup>120</sup>

In spite of the many difficulties in detecting, protecting and responding to biological hazards, there are significant challenges facing terrorist organisations who wish to employ them. Aum Shinrikyo, the Japanese cult that released Sarin nerve agent in the Tokyo subway, also had plans for biological terrorism. They possessed anthrax cultures and botulinum toxin as well as significant quantities of growth medium. They had developed various dissemination techniques including aircraft sprayers. In 1992 members of the group travelled to Zaire in an attempt to acquire samples of Ebola virus. In spite of their large, technically proficient and well-funded capability, Aum Shinrikyo failed to conduct a significantly successful biological weapons attack.<sup>121</sup>

Whilst a large scale bio-attack is unlikely, crude smaller scale attacks, remain a possibility.

## THE NUCLEAR HAZARD

Commonly tagged onto the CBR acronym, nuclear weapons share their primary characteristics with conventional or improvised explosives. There are some aspects of radiological hazards,

<sup>119</sup> World Health Organisation, 'Ebola response: What needs to happen in 2015.' <http://www.who.int/csr/disease/ebola/one-year-report/response-in-2015/en/>

<sup>120</sup> Bates, BBC, 'When foot-and-mouth disease stopped the UK in its tracks.' <http://www.bbc.co.uk/news/magazine-35581830>

<sup>121</sup> Danzig et al. CNAS. 'Aum Shinrikyo: Insights Into How Terrorists Develop Biological and Chemical Weapons' [http://www.cnas.org/files/documents/publications/CNAS\\_AumShinrikyo\\_Danzig\\_0.pdf](http://www.cnas.org/files/documents/publications/CNAS_AumShinrikyo_Danzig_0.pdf)



but they pail into insignificance against the sheer destructive power of a nuclear detonation. As an illustration, the nuclear artillery projectile in Figure 6 has an explosive yield equivalent of between 5 - 10 kilotons. To create a similar effect would require up to ten-thousand Oslo car bombs.



Figure 6. Cold-War era, 8" nuclear artillery projectile. (Date and photographer unknown)

The security of special nuclear material for weapons is the responsibility of the nuclear possessor states. Since the end of the Cold War, the US in particular has spent extraordinarily large amounts of money to ensure the safekeeping of the most vulnerable elements of the former Soviet nuclear arsenal. There have been a number of suspected approaches by various terrorist organisations to acquire nuclear weapons. And as the A.Q. Khan network demonstrated, nuclear technology has been shared around to those whom we might not consider appropriate.<sup>122</sup>

It is conceivable that a nuclear weapon could be constructed by a terrorist organisation. However, it would be an extremely challenging proposition. Some weapons designs are more straightforward to construct than others, but all require minimum quantities of special nuclear material.<sup>123</sup> In the 1980s and 1990s, Iraq spent billions of dollars with thousands of staff on a nuclear programme and still failed to develop even a crude bomb.<sup>124</sup> However it was under an external monitoring programme and had its principle reactor destroyed by Israel.

## How ...

Whilst CBRN material presents an inherent peril, the last two elements of non-conventional hazards focus on a means of delivery; the effect vectors.

## THE CYBER HAZARD

There is currently no formal definition of cyber-terrorism in the UK. The differences between it and *cyber-crime* (Data theft or disruption for financial gain), *cyber-vandalism* / *hacktivism*

<sup>122</sup> NTI. 'The AQ Khan revelations.' <http://www.nti.org/analysis/articles/aq-khan-revelations/>

<sup>123</sup> Belfer Center, Harvard University. 'Nuclear Terrorism Fact Sheet.' [http://belfercenter.ksg.harvard.edu/publication/20057/nuclear\\_terrorism\\_fact\\_sheet.html](http://belfercenter.ksg.harvard.edu/publication/20057/nuclear_terrorism_fact_sheet.html)

<sup>124</sup> IAEA Website. Iraq's Nuclear Weapon Programme. <https://www.iaea.org/OurWork/SV/Invo/factsheet.html>

(Data loss and service disruption), *cyber-espionage* (State-sponsored data theft) or *cyber-war* (State-on-state attack) can be subtle and subjective.

One approach is to define Cyber-terrorism as an attack on an IT system that results in physical damage to a target and associated structures. Of course other effects are possible; service disruption or data loss. So the distinctions between the perpetrator and intent to cause mischief or terror might be quite nuanced.

In order to achieve physical damage, a cyber-terror attack is likely to focus on process control systems, commonly characterised as DCS (Distributed Control Systems) or SCADA (Supervisory Control And Data Analysis system); the terms are becoming indistinguishable. They are both the interfaces between the electronic monitoring / processes control and the real world.

Stuxnet is the well-known example of a cyber-attack that resulted in physical damage. The virus subtly altered the DCS/SCADA system, forcing it to vary the speed of the centrifuges it controlled. Over a period of months these variations caused excessive stresses on the equipment. This eventually resulted in 20% of them being damaged beyond repair. If the rumours are to be believed, this is perhaps more of a cyber-war attack.<sup>125</sup> But the outcome amounts to the same thing; significant property damage along with long-term service disruption.

DCS/SCADA systems used to be proprietary to particular systems and unconnected to other networks. More recent generic systems, working on common platforms, have been introduced. Whilst this has increased usability and reduced costs, it does allow new exposure pathways to be exploited and threaten systems.<sup>126</sup> The UK government, amongst others, is placing an increasing emphasis on supporting critical infrastructure and industry in defending DCS/SCADA systems and data networks. The recently formed National Cyber Security Centre (NCSC) will also focus on protection advice for the UK financial sector.<sup>127</sup>

Possible attacks might include the disruption of smoke detection sensors inhibiting a fire-monitoring system, or taking command of the flight control surfaces of an aircraft. Both scenarios involve potentially devastating material losses to people and property. A recent example in the US is the suspension of use of medical infusion pumps that were considered at risk from hackers.<sup>128</sup> However research by the City University London suggests that the costs and skill requirements of an effective cyber-terrorist attack are currently prohibitive for most terrorist organisations.<sup>129</sup>

There is also much discussion of the next stage of information technology and global networking; the so -called *internet of things*.<sup>130</sup> In essence this is where everyday aspects,

---

<sup>125</sup> Kushner, IEEE Spectrum. 'Real story of Stuxnet.' <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>

<sup>126</sup> UK CPNI. 'Good practice guide process control and SCADA security.' [https://www.cpni.gov.uk/documents/publications/2008/2008031-gpg\\_scada\\_security\\_good\\_practice.pdf](https://www.cpni.gov.uk/documents/publications/2008/2008031-gpg_scada_security_good_practice.pdf)

<sup>127</sup> HM Cabinet Office. 'New Cyber Centre.' <https://www.gov.uk/government/news/new-national-cyber-security-centre-set-to-bring-uk-expertise-together>

<sup>128</sup> Finkle. Reuters. 'FDA warns of security flaw.' <http://www.reuters.com/article/us-hospira-fda-cybersecurity-idUSKCN0Q52GJ20150731>

<sup>129</sup> Terrorists' Use of the Internet: Symposium Report. <http://www.cyberterrorism-project.org/wp-content/uploads/2014/06/2014-Symposium-Report.pdf>

<sup>130</sup> De Clerck. iScoop. 'The IoT explained.' <http://www.i-scoop.eu/internet-of-things/>



objects and systems have sensors and communications integrated into their design to allow data on their status (location, condition, etc.) to be communicated with other connected or dependant systems. Smart buildings with automated access control, HVAC systems and services already exist. In the near future it will include urban traffic control systems integrating with driverless vehicles. This potentially huge increase in opportunity targets for the terrorist, coupled with their ability to remain remote and anonymous during an attack, is an attractive proposition.

A further blurring of the division between the cyber and real world threats is the theft and publication of sensitive information on government and security forces personnel. In an attempt to encourage and enable returning or stay-at-home fighters to conduct attacks, the names and addresses of service personnel were released.<sup>131</sup>

### THE DRONE HAZARD

Whilst posing limited significant hazard in themselves, unmanned aerial vehicles (UAVs / drones) do offer the possibility of a novel approach to delivering a hazard to its intended target. Easily obtainable versions currently have typical payloads of around 1 kg and a maximum endurance of 20 minutes. However larger models can have payloads up to 50 kg and endurance measured in hours. Acquiring these more capable types is difficult, with licences and registration schemes in many countries.

It is not difficult to imagine the employment of a drone such as the Hercules-30 (see Figure. 7) in a non-conventional attack. However converting them to carry and effectively disseminate a chemical, and particularly a biological weapon payload, may not be an easy process. There are particular engineering and scientific aspects that need to be correct if an effective weapon is to be produced.



*Figure. 7. The US-built Hercules UAV crop sprayer, with a payload of 30 kg (HSE-UAV)*

As well as disseminating a vapour, droplet or aerosol payload, drones could also be used to deliver an IED. Whilst probably insufficient to cause significant structural damage, a credible

---

<sup>131</sup> Clapper. CIA. 'Worldwide threat assessment of the US intelligence community.' [https://www.dni.gov/files/documents/SASC\\_Unclassified\\_2016\\_ATA\\_SFR\\_FINAL.pdf](https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf)

explosive drone threat could significantly affect business activities, particularly in an urban environment.

Defensive systems are now available, utilising a variety of approaches to disable or destroy drones. There are implications that come with these devices; not least the potential liability should one be forced down and cause damage / harm to third parties.<sup>132</sup>

## CONCLUSIONS

The spate of terror attacks in Europe and the US in the first half of 2016 have again brought into focus the hazards posed within our own society. The insurance industry rightly reflects these concerns by offering products that allows that transfer in risk ownership.

In reviewing hazards that have not commonly been employed in the past, due attention must be given to the balance between the chance of an event occurring and its consequence. There are multiple and complex reasons why CBR weapons have rarely been used; despite of the aims and warnings associated with these groups. Terrorist want to succeed. Given the choice between tried and tested methods versus a novel technique, history suggests that usually the preference is for a conservative approach.

There are also a number of inhibitors worthy of note against the selection of CBR material to be used as a terror weapon. Firstly, such material does require a great deal of technical knowledge in certain critical stages; particularly in manufacture and weaponisation. Whilst such skills are not rare, they are certainly not abundant.

Secondly, it has been demonstrated that large, more intricate a terrorist organisation leave much greater 'intelligence footprint'; resulting in a greater chance of discovery and interdiction by security forces. The technical skills required to successfully develop and use a CBRN weapon would demand such complexity, therefore exposing them to detection.

Thirdly, a simple cost-benefit analysis is likely to highlight the relative inefficiency of all but the most sophisticated CBR attacks. A crude comparison is the estimated \$30M spent by Aum Shinrikyo on acquiring chemical materials (This does not include the attempts to acquire biological, radiological and nuclear material).<sup>133</sup> Their subsequent attacks in Matsumoto and Tokyo killed 21 people. Juxtapose that with the 7/7 bombings in London that killed 52 and cost a few hundred pounds.<sup>134</sup> The attack in Nice was perhaps the price of a day's truck rental.

In spite of people being the principal target of a CBR hazard, there are likely to be significant material losses. It is estimated that the total decontamination costs of the 2001 US anthrax attacks was \$320M.<sup>135</sup> An important contribution to this was the challenge to determine the success criteria conditions (how clean is clean?).<sup>136</sup> The AMI newspaper offices in Florida

---

Penn-Hall. Cipher Brief. 'Rise of Counter-Drone Technology' <https://www.thecipherbrief.com/article/techcyber/rise-counter-drone-technology>

<sup>133</sup> The Economist. 'Terror next time?' <http://www.economist.com/node/806202>

<sup>134</sup> Buchanan. BBC. 'London bombs cost just hundreds' <http://news.bbc.co.uk/1/hi/uk/4576346.stm>

<sup>135</sup> Schmitt & Zacchia. 'Total decontamination cost of the anthrax letter attacks.' [http://spectrum.library.concordia.ca/974056/1/Schmitt\\_Spectrum.pdf](http://spectrum.library.concordia.ca/974056/1/Schmitt_Spectrum.pdf)

<sup>136</sup> Simpson. CRS. 'Anthrax-Contaminated Facilities: Preparations and a Standard for Remediation.' <https://www.wbdg.org/pdfs/crsreport anthrax lessons.pdf>

stood unused for six years.<sup>137</sup> The total cost for all the disruption was likely to be significantly higher.

The ever increasing pace of change in technology improvements has the potential to open opportunities for terrorist use. The merging of biology and chemistry, as well as the miniaturisation of technologies, are of particular note.

Whilst the CBRN risk may not be large at the moment; the use of emerging technologies is a viable proposition. A cyber-terrorist attack may be prohibitively costly at the moment, but is liable to change. Unlike CBRN weapons, if the main impediment to developing a hazard is simply money; then perhaps it is only a matter of time. A clear example is the increasing capabilities and reducing costs of drones. The development of the ‘internet of things’ will only compound the issue and represents a whole new set of significant challenges.

Within industry and wider society, we are observing ambitions to leverage the benefits of such technology into many aspects of life. However there remains a potential lag between the introduction of such technologies and the incorporation of robust countermeasures to maintain the safety and security of the systems.

Ultimately the insurance market will find a way. But in doing so, emphasis should be placed on continual, robust and, where possible, quantitative assessment of the hazards and threats. In the UK Pool Re is leading this approach. It is currently running a major research programme into CBRN risk modelling as well as examining the cyber-terrorism issues.<sup>138</sup>

As a final note, the capabilities for mass effect, be it from CBRN or cyber, should be tempered with a sense of perspective. It is estimated that a US citizen’s annual risk of being killed by a terrorist is one in 3.5 million. They are more likely to die in an accident involving a bathtub (nearly one in 1 million), a home appliance (one in 1.5 million) or a deer (one in 2 million).<sup>139</sup>

To quote Professor Joseph Nye of Harvard University: “(Modern-day) terrorism is not World War Three.”<sup>140</sup>

---

<sup>137</sup> King, Boca Raton Newspaper, ‘Former AMI building sold to ACS.’ <https://news.google.com/newspapers?nid=1291&dat=20070518&id=F3BUAAAAIABJ&sjid=Io8DAAAABAJ&pg=6799,960808&hl=en>

<sup>138</sup> Pool Re. ‘New terrorism risk model.’ <https://www.poolre.co.uk/pool-re-announces-new-terrorism-risk-model-partnership-cranfield-university-guy-carpenter-airmic-2016/>

<sup>139</sup> Mueller & Stewart, ‘Thinking Rationally About Terrorism.’ <http://politicalscience.osu.edu/faculty/jmueller/Faexistentialfin.pdf>

<sup>140</sup> Nye. WEF. ‘Has the threat of terrorism in the US been blown out of proportion?’ <https://www.weforum.org/agenda/2016/02/has-the-threat-of-terrorism-in-the-us-been-blown-out-of-proportion/>



**Dr Gordon Woo, PhD, BA**  
**Catastrophist**  
**RMS**

[www.linkedin.com/in/gordon-woo-0176bbb](http://www.linkedin.com/in/gordon-woo-0176bbb)

Gordon Woo specialises in the assessment and management of extreme risks, both natural and man-made. He has focused on terrorism risk since 9/11, and is the chief architect of the RMS terrorism risk model. For his innovative work on terrorism insurance risk, he was named by Treasury & Risk magazine as one of the 100 most influential people in finance in 2004. Since 2009, he has been a regular speaker at courses at the NATO Centre of Excellence for the Defence against Terrorism. In September 2013, as a leading international authority on quantitative terrorism risk assessment, he was called to testify to the US congress on terrorism risk modelling.

He has written widely on terrorism, including for the National Defense University in Washington DC, and has authored of the two books: *The Mathematics of Natural Catastrophes* (Imperial College Press, 1999), and *Calculating Catastrophe* (Imperial College Press, 10th anniversary of 9/11). Dr Woo was a top graduate at Cambridge University, completed his PhD at MIT as a Kennedy Scholar, and was a member of the Harvard Society of Fellows. He is currently an adjunct professor at Singapore's Nanyang Technical University, as well as a visiting professor at University College London.

## **13. ISIS ATTACKS IN PARIS AND SAN BERNARDINO**

### **TERRORISM INSURANCE AS INSURANCE AGAINST THE FAILURE OF COUNTER-TERRORISM**

#### **ABSTRACT**

*Two ISIS terrorist attacks towards the end of 2015 against Paris and San Bernardino, California, shed light on the strategic confrontation between a terrorist organization and the forces of counter-terrorism. For the attack in San Bernardino, a home-grown Jihadi couple, unknown to the US authorities, were able to perpetrate their shooting rampage without their plot being interdicted. For the larger scale more ambitious attack in Paris, three teams of operatives were deployed to attack the Stade-de-France, the Bataclan concert hall, and local bars and cafés. The rationale for the precise targeting and meticulous attack scheduling is explained.*

*ISIS exploited the Syrian refugee crisis to infiltrate several terrorists into Europe, and took advantage of lax Belgian security to despatch four Belgian operatives across into France. The most lethal attack against the Bataclan concert hall was carried out by three French terrorists, combat hardened in Syria. For this attack, ISIS made a strategic decision in using Syrian returnees rather than other radicalized but less trusted French Jihadis. With this risky but operationally effective strategy, all the Bataclan operatives were known to the French authorities, who thus had a good chance of interdicting their attack.*

## COUNTER TERRORISM DEFENCE

Nation states are powerless to stop earthquakes and windstorms; the forces of Nature are greater than those of mankind. However, nation states do have military, intelligence and law enforcement capabilities to stop terrorists before they move towards their targets. Once terrorists are allowed to attack a target, loss mitigation will depend on the site security, and ultimately the local building vulnerability to the specific weapon mode of attack. Measures can be taken to harden targets through entrance screening, hiring extra security guards, security landscaping, blast-proofing of buildings etc., but from a national security perspective, counter-terrorism has failed once terrorists move to attack. If a designated target proves too hard, it can be substituted by one that is softer. There is an abundance of crowded public places that offer potential soft targets for terrorists seeking to maximize casualties.

For a terrorism insurer covering a portfolio of properties within a country, terrorism insurance is essentially insurance against the failure of counter-terrorism. Unless there is some technical deficiency or malfunction in attack execution, there will be a terrorist pay-off if a plot is not interdicted. Insurers therefore need to have a solid understanding and general knowledge of the process of terrorist plot interdiction. Unlike natural hazards, terrorism is subject to state control, the extent of which varies from state to state.

Whereas information about terrorist organizations fills many pages of current affairs journals and hours of media commentary, there is far less information publicly available about plot interdiction. Operational secrecy is the rationale for maintaining confidentiality. If there is some preliminary intelligence about a forthcoming plot, clearly any information leak might jeopardize efforts at stopping the plot, arresting the operatives, and gaining a court conviction. However, once arrests have been made, and the legal process has been duly followed with a court case and subsequent conviction, information can then be made public about the terrorist danger averted. For insurers, this is satisfactory. They do not need plot information in real time. It is not their task or responsibility to stop the next terrorist plot, rather they need to be able to assess the medium term risk. In this respect, the situation is similar to windstorm insurance. State meteorological offices are responsible for forecasting extreme weather in real time. Insurers are concerned with evaluating the medium term risk.

## PLOT INTERDICTION

It is the responsibility of national intelligence and security organizations to interdict terrorist plots. Integrity, professionalism and competence are key to counter-terrorism capability. These virtues may vary quite widely from one country to another. Within its volatile political environment, the Pakistani security agency, ISI, has actively supported Islamist militants, exploiting their guerrilla role in border disputes with India. Accordingly, terrorists in Pakistan have been able to attack at a very high tempo, and Osama bin Laden was able to hide out for years in Abbottabad. Pakistan's neighbour, Afghanistan, is also seriously affected; many Taliban leaders live in and around Quetta, Pakistan. Cross-border movement of terrorists is at the core of the challenge of controlling terrorism, as will be clear in the discussion of the ISIS attacks in Paris on 13th November 2015.

Also important for plot interdiction are resources of staffing, equipment and funding of intelligence and security agencies. Such resources come under pressure during periods of financial austerity, such as experienced over the past eight years within the Eurozone. Alain Winarts, the head of Belgium's domestic intelligence agency from 2006-2014, has complained that his budget was far below the necessary level. The agency had only 600 employees,



covering both operations and analysis, and was in need of at least 120 to 150 more people to function properly.

Elsewhere amongst the western democracies, the Five Eyes Alliance is the world's foremost intelligence cooperative, formed of the Anglophone nations of USA, UK, Canada, Australia and New Zealand. This alliance has a massive annual budget of \$100 billion, and mastery of the internet through the pre-eminent global communications expertise, eavesdropping and code-breaking skills of the American NSA and British GCHQ.

Whereas for a totalitarian state, ruthless anti-libertarian measures can be routinely taken to suppress terrorism, for a democratic state, there is a fine balance between protection of civil liberties and the control of terrorism. Any notable erosion of civil liberties would in itself be perceived as a terrorist gain. However, the safety of its citizens is the first priority of a democracy, and terrorists cannot be allowed to attack at will. Accordingly, stringent counter-terrorism measures are adopted in the western world to interdict significant terrorist plots. Such measures are reinforced after the shock of a terrorist attack, and may be relaxed during episodes of successful plot interdiction with little terrorism loss. Terrorist plots can be interdicted in a number of different ways. These are listed below.

#### *[a] Informants*

Intelligence agencies infiltrate their agents within terrorist organizations to act as informants. These agents will typically have the same social, religious and cultural background and identity as the terrorists themselves. Some may be reformed extremists, or ex-convicts whose sentences have been reduced on condition of serving as an informant.

Terrorist organizations resist the intrusion and reduce the effectiveness of informants by partitioning their operations within small independent terrorist cells. The damage to a terrorist network by an informant would then be limited, and not compromise the overall organizational structure. Centrally planned attacks are particularly vulnerable to disruption by informants.

#### *[b] Agents Provocateurs*

Intelligence and law enforcement agencies may use their own staff to act as agents provocateurs, who openly solicit expressions of terrorist support, either online or in activist meetings and gatherings. They actively engage with supporters in the planning, preparation and even simulated execution of terrorist acts, with the objective of securing sufficient evidence to convict them of terrorist offences. As a recent example, on New Year's Eve 2015, an FBI sting operation thwarted a lone-wolf ISIS attack in Rochester, New York.

Agents provocateurs are especially effective at curbing the activities of self-starter lone wolves, who are not part of an existing terrorist cell, and lack the expertise and resources to perpetrate their own terrorist attack without assistance from the agent provocateur. Such agents would not be likely to entrap the better trained and experienced terrorists.

#### *[c] Tip-offs*

Observation of suspicious behaviour or activity may result in a tip-off to the police or other authorities from vigilant strangers, or merchants or vendors from whom some unusual purchase of goods or services has been made. In some instances, a tip-off may be made from those who have some acquaintance with the suspect: a neighbour, imam, colleague, friend or even family member may contact the police.



Tip-offs are a valuable crowdsourcing self-organized supplement to professional counter-terrorism efforts. However, they are hit-and-miss and random, and cannot be depended upon to interdict plots. In particular, some of the Paris assailants on 13th November, e.g. Bilal Hadfi, were recognized by those closest to them to be on an irreversible path to increasing radicalization, but family loyalty came before national security.

### *[d] Surveillance of known terrorists*

Known terrorists ought to be kept under active and intensive human and electronic surveillance, so that any recidivist activity that might be linked with future terrorism can be tracked and any potential plot disrupted at an early stage.

Tight border security is important to prevent known terrorists from crossing the border into a target country from a host country that might be a failed state, or one that is a terrorist safe haven. In particular, those on 'no-fly' lists should be excluded from entry by other means.

### *[e] Surveillance of supporters of terrorist organizations*

The biggest challenge for counter-terrorism officials is the threat emerging from within a large population of terrorist organization sympathisers and supporters. Sizeable numbers of them would swamp the resources available for human surveillance. For each suspect, a number of agents would be needed to mount 24 hours personal surveillance. Instead, electronic eavesdropping and communications surveillance are essential to identify links with terrorist cells.

Tracking may require contact chaining, i.e. finding out who are in contact with known or suspected terrorists. The process of tracking communications involves the type of mass collection of communications meta-data disclosed by the NSA whistle-blower Edward Snowden. Following the revelations of Edward Snowden, terrorists have made greater use of encryption and the dark web in their communications. Furthermore, civil libertarians have demanded curbs to indiscriminate state snooping. Updated legislation, and protests from large tech companies, have reined back the authorized powers of the US and UK intelligence agencies in conducting mass surveillance. But an enterprising response to defending national security should be expected from the ever resourceful intelligence community.

## **TOO MANY TERRORISTS SPOIL THE PLOT**

Whatever the mode of plot interdiction, it is clear that the more operatives involved in a plot, the greater is the likelihood that the counter-terrorism services will tag one of them and, through this human portal, gain access to the plot details. A plot can only avoid interdiction if every single one of the operatives manages to avoid any communications that might compromise the plot. The chance of this happening is the product of the individual probabilities, and diminishes progressively as the plot is enlarged. Obviously, lone wolf plots have the smallest communications footprint and the lowest chance of interdiction.

Through terrorist social network analysis, RMS has evaluated the likelihood of a plot being interdicted through the type of systematic and highly intensive electronic surveillance and contact chaining exercised by US and UK intelligence services. This increases with the number of operatives as indicated in Table 1 below:

Table 1: Surveillance interdiction probability as a function of cell size

Cell Size	1	2	3	4	5	6	7	8	9	10
Interdiction Probability	0.26	0.46	0.60	0.70	0.78	0.84	0.88	0.91	0.93	0.95

These probabilities are augmented by random tip-offs, and the activities of informants and agents provocateurs. Highly elaborate ambitious plots capable of inflicting catastrophic insurance loss would typically involve so many operatives as to have a very high likelihood of interdiction. This would be wasteful of terrorist resources and damaging to terrorist morale. Discouragement of Jihadi plots against the US homeland involving double-digit operative numbers has come from Osama bin Laden himself in a message from his Abbottabad hideout: *'For a large operation against the US, pick a number of brothers not to exceed ten.'* The more operatives there are, the greater is the chance that one of them will compromise the terrorist venture: too many terrorists spoil the plot.

## THE SAN BERNARDINO TERRORIST ATTACK OF 2ND DECEMBER 2015

In terrorism risk analysis, it is instructive to introduce the concept of a macro-terror attack. This is a terrorist attack where the number of fatalities attains a threshold of fifty, or where the economic loss exceeds a billion dollars, or where a highly iconic symbolic target is struck. Such attacks require a substantial amount of planning, and a significant logistical burden of human, equipment and financial resources. The terrorist pay-off for the extensive planning involved and the resources committed needs to be substantial. Accordingly, the targeting for macro-terror attacks is focused on major cities with international name recognition, such as Paris on 13th November 2015.

A classic example of focused macro-terrorism targeting is the London transport bombings of 7th July 2005. The key operatives lived in a small provincial town in northeast England. Rather than bomb their home town, they drove several hundred miles south to London to launch their attack during the peak of the morning rush hour to maximize commuter casualties. In all countries of the western alliance since 9/11, the targeting of macro-terror attacks has focused on the principal cities, and can be represented by an evidence-based target tier distribution.

By contrast, so-called micro-terror attacks can, and do occur essentially anywhere. These are less ambitious than macro-terror plots, and often involve a choice of target local to the terrorist home base. The attack logistical burden is lower, with easier reconnaissance and weapon transport. The archetypical attack mode of a macro-terror attack is the vehicle bomb, which has been called 'the terrorist's air force'. Instead of a vehicle bomb, a micro-terror attack often involves the home manufacture of pipe bombs, requiring only small quantities of explosive. In the USA, grenades might potentially be used as an off-the-shelf alternative. They can be purchased, but only with a special tax stamp and FBI background check, which would be a terrorist deterrent. Assault rifles are comparatively easy to purchase, and would be stock weapons of the micro-terrorist arsenal.

Assault rifles and pipe bombs were the weapons used in the micro-terror attack on 2nd December 2015, in [San Bernardino, California](#). Fourteen died and twenty two were seriously injured at a San Bernardino County Department of Health training event and holiday party, held at the Inland Regional Center. One of the victims was Hal Bowman, who once worked at

CREATE, the national Homeland Security terrorism risk center at the University of Southern California. For a micro-terror attack, there is a vast number, literally many tens of thousands, of soft unprotected targets that might be struck. As with other mass shootings, a personal grudge could prioritize the targeting. But this was no ordinary mass shooting. More than one shooter was involved, which is extremely rare.

Anyone who has shared an office with a devout Muslim of Pakistani descent, who has spent time in Saudi Arabia, knows how careful and sensitive one needs to be in discussing Islamist militancy. Just a coffee-break talk about Middle East politics can cause grave personal offence. From his experience at CREATE, where terrorism is studied, Hal Bowman may have appreciated the need for discretion. For if a work colleague happens also to be radicalized, then the level of offence caused by such small talk can trigger a change in psychological state from calmness to anger and even violence. The fact that [Syed Rizwan Farook](#) ultimately took out his rage on his colleagues, and terminally censored what he perceived to be blasphemous and insolent back chat, would not surprise psychologists of terrorism.

### COUNTER-TERRORISM PERSPECTIVE

Terrorism is as much about counter-terrorism as the terrorists themselves. Lone-wolf attacks perpetrated by a single individual are difficult to interdict through electronic surveillance, because very little communication of any kind is needed to plan and prepare for an attack. As exhibited in Table 1, a plot involving two operatives is also hard to stop through electronic surveillance. The amount of electronic communication between operatives is reduced still further if the pair of terrorists happen to be close family. This was the case with the Boston marathon attack Tsarnaev brothers in April 2013; the Charlie Hebdo Paris attack Kouachi brothers in January 2015; and the San Bernardino attack Farook couple in December 2015.

Farook's accomplice was his wife, [Tashfeen Malik](#), another Pakistani with Saudi links. She had professed her Jihadi sympathies online back in 2012, before she married Farook. However, US immigration officials do not regularly check the social media accounts of visa applicants. This has been regarded by the Department of Homeland Security as a violation of free speech and freedom of expression. Ways to include social media reviews in the vetting process are being considered for the future.

The rifles used by the couple were legally purchased in 2011, and subsequently illegally modified to boost their killing power. The buyer was Enrique Marquez, a friend and neighbour of Farook, who allegedly plotted several terrorist attacks with him. But neither of them were terrorist suspects, and the plots were shelved without either coming to counter-terrorism attention. When Farook resumed his terrorist activities with Tashfeen Malik, there would only have been a modest chance of their plot being interdicted through surveillance. No informant could have stopped the attack either, unless Farook's partner had herself been co-opted by counter-terrorism services – a scenario familiar from the East German Stazi era of police state repression, when family members spied on each other.

With luck, there might have been a tip-off from the public. The couple had amassed a large stockpile of weapons, ammunition, and bomb-making equipment in their home. Indeed, unusual garage activity late at night had been spotted by one observant neighbour, but was not reported to the police for fear of being construed as profiling.

From a counter-terrorism perspective, [Syed Rizwan Farook](#) was one of many Muslims who left little trace of their personal radicalization. His colleague, Hal Bowman, with his pioneering CREATE work experience, was not sufficiently concerned about him to tip-off the authorities. On Twitter, Farook followed accounts associated with the Muslim Brotherhood, including the official accounts of the Free Syrian Army and the Syrian Revolution Network, but not the ISIS-affiliated social media feeds that might have attracted notable counter-terrorism interest. His accomplice, [Tashfeen Malik](#), might have been denied her visa, had her social media profile been investigated.

Overall this was a micro-terror plot that, in a free democratic society without tight gun control, always has a reasonable chance of escaping detection. Mass shootings in an office context may potentially result in a substantial workers compensation claim, especially if the death count were compounded by large numbers of long-term injured. But neither the San Bernardino attack, nor the alleged earlier shooting plots by Farook and Marques at Riverside Community College, where they studied, and on the 91 Freeway during afternoon rush hour, would have caused a notably large insurance loss. Like the San Bernardino attack, the putative plots would most likely have been classified as micro-terror attacks.

## THE PARIS TERRORIST ATTACKS OF 13TH NOVEMBER 2015

On 7th January 2015, French liberty itself was attacked by the assassination of the editorial committee of the satirical magazine Charlie Hebdo. At the time, this was the worst terrorist attack in France for half a century. This was superseded ten months later on 13th November, when 130 died in Paris from another deadly terrorist attack by ISIS. Most of the victims were at the Bataclan concert hall, where they were being entertained by the American band: Eagles of Death Metal. When the three terrorists stormed in past the unarmed security staff, the band were playing their hit number 'Kiss the Devil'. Some in the audience responded with a devil's horn hand gesture. Charlie Hebdo, champions of democratic freedom of expression, and opponents of religious fascism, noted wryly from tragic experience in January: *'Invoke his name, and he will come'*.

Two longstanding security fears became deadly reality in the terrorist attacks on Paris on the evening of 13th November. The first is of European Jihadi support for ISIS blowing back to strike Paris or London. The second is of a coordinated mass gun attack as struck Mumbai seven years previously, in November 2008. The reason why this attack had not happened before is because of the great success of the western security services in stopping terrorist plots. Reviewing the catalogue of terrorist plots against the western alliance since 9/11, more plots have actually been stopped than might have been expected. Citizens of the western alliance have been lucky. The director-general of the British security service, Andrew Parker, has urged a strengthening of surveillance powers, (weakened after the Snowden revelations), so as to counter the ISIS threat.

The raison d'être of ISIS is to establish an Islamic State within the borders of Syria and Iraq where the governments in Damascus and Baghdad have left many Sunni Muslims resentful of being disenfranchised. To the politically excluded it offers marginalized Iraqi Sunnis an alternative to Shia rule in Baghdad; to dispossessed Syrians an alternative to the sectarian repression of President Assad; and to Muslims treated as second class citizens in Europe the prospect of a new life in the caliphate.

Since July 2014, ISIS has published a magazine that aims to establish the legitimacy of its caliphate, and to encourage migration. The name of the magazine is Dabiq, which is a small town in northern Syria mentioned in a saying of the Prophet (hadith) about Armageddon. ISIS believes Dabiq is where Muslim and infidel forces will eventually face each other. After the infidel forces are defeated, the apocalypse will begin. Muslim migration to the new Islamic state is partly driven by the pull of being on the cusp of history.

ISIS has threatened that foreign powers that seek to thwart their caliphate ambition through military intervention will be targeted for terrorist attack. For Russia, a major Moscow public transportation plot and the bombing of a Russian passenger aircraft over Sinai were the beginning in October 2015. Following the loss of 224 lives, almost all Russian air passengers and crew, more attacks were anticipated against the 'crusader' countries intervening in Syria and Iraq. Less than a fortnight later, the justification for attacks was expressed directly in a terrorist declaration at the Bataclan: *'We are the soldiers of the Caliphate. It is all Hollande's fault. You attacked our women and children in Syria. We are defending ourselves by attacking the women and children in France.'*

### TARGET SELECTION

Macro-terrorism targeting is deliberate and purposeful. This principle is affirmed by the ISIS communiqué: *A group of believers from the soldiers of the Caliphate set out targeting the capital of perversion, the lead carrier of the cross in Europe — Paris. Eight brothers equipped with explosive belts and assault rifles attacked targets in the heart of the capital of France, which had been precisely chosen in advance. These targets included the Stade de France stadium during a soccer match between the teams of Germany and France, both of which are crusader nations.*

The primary target was the Stade-de-France, where President Hollande was attending a friendly soccer match between France and Germany. Terrorism against international soccer matches in France has been plotted since the 1998 FIFA World Cup in France, and there are now security fears for the forthcoming UEFA EURO 2016 tournament. Based on terrorist plot intelligence, a friendly match between Netherlands and Germany in Hannover scheduled for 17th November 2015 was cancelled.

There was high security at the Stade-de-France on 13th November 2015, with 150 security guards specially deployed. Fortunately, one of these guards spotted somebody trying to enter by tailing a ticket-holder. He was prevented from entering the stadium. He was a Syrian arrival on the refugee route via Turkey and the Greek island of Leros. A fellow Syrian traveller was the second suicide bomber, and the third was Bilal Hadfi, who had journeyed from Belgium to Syria in early 2015. The terrorist plan was for the first bomber to detonate his suicide vest inside the stadium, and for the other two to kill spectators as they rushed out of the stadium in panic. Due to the vigilance and professionalism of the security guard, (a devout Muslim himself), the death toll was limited to a single Portuguese fan. Although there were some serious injuries, including a scarf-vendor and his wife hit by shrapnel from the third suicide vest, a major loss had been averted. The timings of the detonations might have been altered to cause more carnage, but they were fixed with the objective of drawing first responders away from the Bataclan.

A key principle of terrorist modus operandi is target substitution. The Russian Metrojet 9268 brought down over Sinai several weeks earlier on 31st October 2015 was a substitute for a plane from the US-led western coalition, because the Russian plane security was more easily



compromised at Sharm-el Sheikh airport. Because of high security, an attack on the Stade-de-France was ambitious, but not very likely to be successful. Had this been the only target, ISIS would not have gained the media coverage desperately sought to sustain recruitment. 'Half of Jihad is media' is a driving slogan of their attack strategy.

One of the benefits of a multi-target attack strategy is that if one attack fails, others may succeed. The second main target was the Bataclan, No. 50 Boulevard Voltaire in the 11th arrondissement of Paris. One of the most illustrious historical concert venues in Paris, for forty years until September 2015, this concert hall was owned by two Jewish brothers. For this, the Bataclan had been targeted several times; terrorists have a habit of re-visiting sites of previous plots. In 2004, an Israeli hip-hop duo performed there despite threats, but in 2006, a return show had to be cancelled. In 2007 and 2008, the Bataclan received threats over hosting events for Jewish organizations, such as the Israeli frontier police. In 2011, a Belgian man confessed to planning an attack against the Bataclan. If any further anti-zionist motivation were needed by the terrorists for attacking the Bataclan, the band 'Eagles of Death Metal' had themselves played in Israel in July 2015, in defiance of a pro-Palestinian boycott.

For the assault on the Bataclan on 13th November 2015, a team of three French operatives were selected: Sami Amimour, Ismael Mostefai and Fouad Mohamed-Aggad. Amimour was known to be a terrorist, the other two were known to be radicalized. All three were known to have been to Syria. They killed ninety in the audience of more than a thousand. They called out for the American band; but all the band escaped. The terrorists were specifically looking to assassinate the lead singer, Jesse Hughes, who is nicknamed 'the devil'. Ironically, he is a strong supporter of US gun ownership.

A glance at the Bataclan concert hall billing for November 2015 shows Michael Schenkar on 1st and 3rd; Hannah Lou Clark and K's Choice on 4th; Piano Opera on 7th; Young Thug on 10th; and St. Germain on 12th. Music is anathema to Islamist extremists, but none of these acts would have been nearly as compulsive a target as the Eagles of Death Metal concert – the first gig of their French tour. Indeed, this concert was explicitly described in the ISIS communiqué as a festival of perversion.

Even without the international game that fateful Friday evening at Stade-de-France, the appearance of this particular band at a noted terrorist target venue might well have pressed French counter-terrorism officers to go on high alert. At the least, the Bataclan security should have been stepped up to a far higher level.

Synchronous events are particularly attractive for terrorism strategy. This is because security is typically heightened after a successful attack. Thus if the Eagles of Death Metal concert had been scheduled for the following day, Saturday 14th November, the suicide bomb attack at Stade-de-France the previous night would have automatically raised security at all major public venues in Paris, including the Bataclan. As it so happened, when the 2015 Paris sports and music calendars were overlaid, both events were scheduled for exactly the same evening – and at the same hour. This turned out to be a coincidence too good for ISIS to pass up. But with these being very attractive honey-pot targets, why would ISIS complicate a double attack plot by including any other targets, especially those not in the same league of name recognition? This requires analysis and explanation.

Gilles Kepel, a French authority on militant Islam, has quoted the Jewish Dutch 17th century philosopher Spinoza: *'In order to preserve in political science the freedom of spirit to which*

*we have become accustomed in mathematics, I have been careful not to ridicule human behaviour, neither to deplore nor to condemn, but to understand.'*

The ISIS terrorist attacks in Paris were deplorable and condemnable - but also understandable. The latter is key for terrorism risk assessment. The more that can be understood of the past, the more that should be understandable about future threats.

Apart from partly being a Jewish quarter, with many Jewish-owned stores, the area around the Boulevard Voltaire is noted for the liberal lifestyle that is so despised by ISIS as decadent. Although not a posh part of town, it is a trendy *bourgeois-bohème* (*bo-bo*) area with a high density of bars and cafés. In the Parisian annals of terrorism, there have been a few attacks on public restaurants. The most notable was an attack on 9th August 1982 by the Palestinian Abu Nidal Organization on a Jewish restaurant, Chez Jo Goldenberg, in the Marais district, where Jews who arrived from Eastern Europe lived. Two assailants threw a grenade into the dining room, then rushed in and fired machine guns, killing six patrons.

There is no shortage of Kosher restaurants around the Boulevard Voltaire. But none of these were targeted on 13th November 2015. Nor were any Kosher supermarkets struck, as Amedy Coulibaly had done on 9th January 2015 soon after the Charlie Hebdo attack. Instead, a series of bars and cafés were attacked in a sequence which is explainable in terms of the overall logistics of the attack scheduling, as elucidated in the next section.

Fifteen died at Le Carillon and across the street at Le Petit Cambodge, where their patrons often dined. Also there was a heavy death toll of nineteen at La Belle Equipe, a popular bistro opened at the end of 2014. Besides these 34 fatalities, 5 died in shooting at La Café Bonne Bière and across the street at La Casa Nostra.

Ibrahim Abdeslam terminated the shooting spree at Le Comptoir Voltaire, on the Boulevard Voltaire, by detonating his suicide vest, seriously injuring a waitress and some patrons, but managing to kill only himself. This café location is shown with all the others on Figure 1 below. The event timings are also indicated. These are significant for understanding the logic of the overall operational strategy. With just a few minutes shooting time allotted at each bar or café, and several minutes average drive time to reach the next location, there was only time for three geographically separate locations to be attacked before the final suicide vest detonation at Le Comptoir Voltaire at 9.40pm.

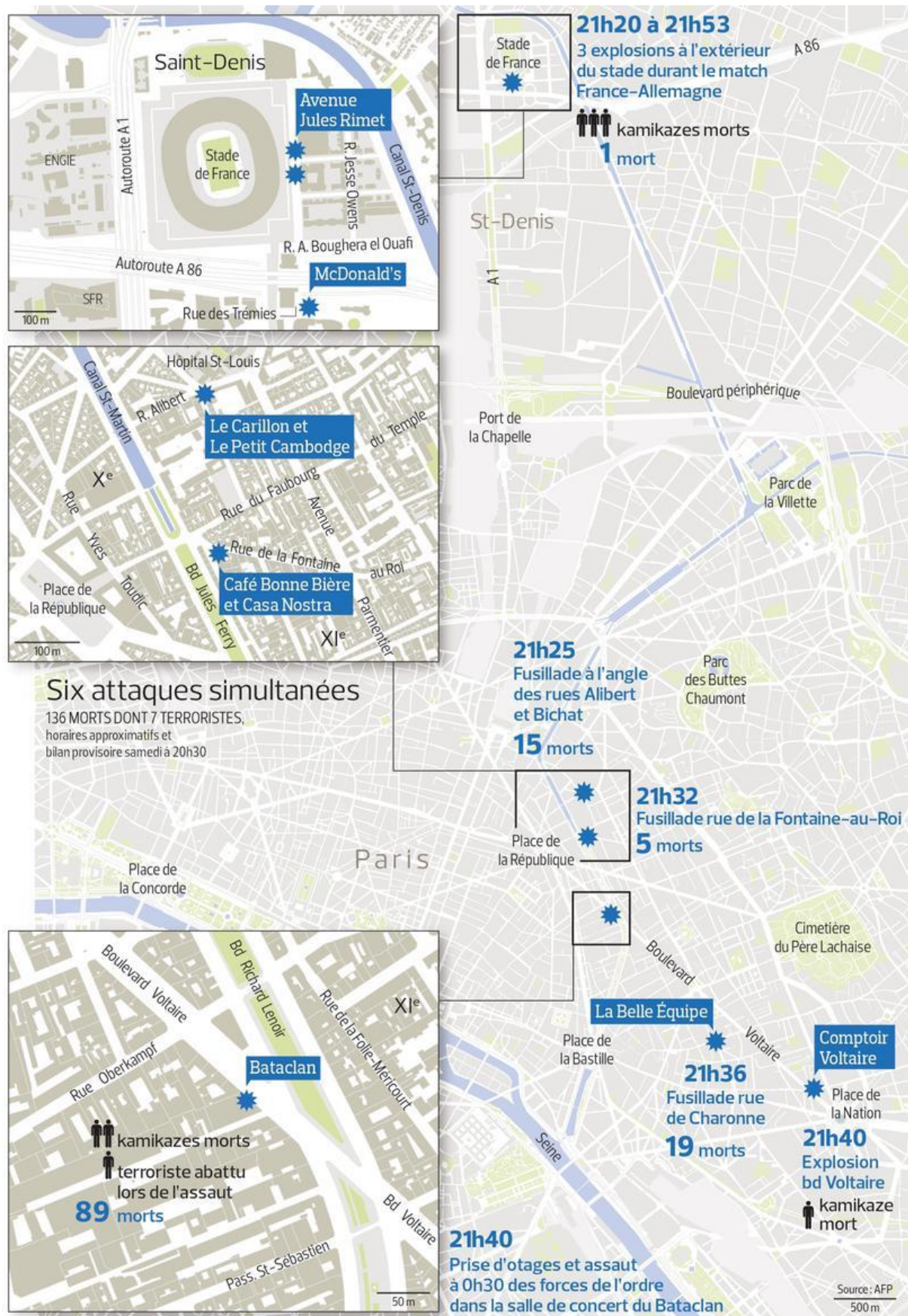


Figure 1: Paris attack chronology [Source AFP; reproduced in Le Figaro: 14/11/2015]

### 3.2 Precision attack scheduling



The ISIS attack communiqué describes the targets as being chosen in minute detail. This would not be apparent by considering each individual bar and café. Prurient Islamist sensibilities might have been offended by La Belle Equipe, managed by four girls, or Le Carillon, which was highly recommended as a dive bar. But Paris is the historical home of the restaurant, with some of the world's finest and most exclusive restaurants. None of the targets were known except to the local '*bobos*'. Out of all the many thousands of eateries in Paris, why would an ordinary Italian pizza outlet like La Casa Nostra be shot at? Le Petit Cambodge had a young and trendy clientele, but was no fine-dining Michelin star establishment. Why was this ethnic restaurant attacked?

The ISIS communiqué makes no mention of the decadence of the bars and cafés that were attacked. The rationale for target selection was not based on decadence or other attribute an Islamist would condemn, but rather on the intricate spatial-temporal logistics of attack scheduling. The Bataclan assailants would have about fifteen minutes of free shooting without armed response, unless some police happened to be in the vicinity at the time. A brief drive-by shooting spree around the Boulevard Voltaire was precisely scheduled before the Bataclan assault as a deceptive diversion to cause local chaos all around the general neighbourhood of the Bataclan, and draw police and emergency services away from there. This was a classic play out of Sun Tsu's Art of War: '*All warfare is based on deception*'.

The timing of this strategic smokescreen was meticulously synchronized with the precision of a pyrotechnic display, and did not allow for dallying to shoot more patrons inside restaurants, or despatch the wounded on the terrasses, or even to shoot at more drinkers and diners, or pedestrians. The logistical factors that dictated the selection of bar and café targets were as follows:

- Attacking on side streets to minimize the chance of prompt police intervention.
- Attacking at or near crossroads to ensure an unblocked getaway.
- Attacking places known to be crowded on a Friday evening.
- Attacking people outside on terrasses to minimize shooting time.
- Attacking adjacent pairs of restaurants to maximize target opportunity at each stop.
- Attacking restaurants both north and south of the Bataclan, to absorb capacity of the local emergency response, and to cause traffic congestion.
- Attacking away from the vicinity of the Bataclan, to avoid a security alert there.
- Ending the shooting spree with a suicide bombing on the Boulevard Voltaire, synchronized with the Bataclan assault, to distract and delay the emergency response.

The choice and sequence of bar and café targets can be posed as a mathematical problem familiar in operational research. What is the optimal route, complying with these eight logistical factors, which could be traversed within the tight operational time window of about fifteen minutes, after which an encounter with armed police would be expected? The terrorists found a viable shooting solution: striking two pairs of targets north of the Bataclan in two stops, then driving southeast on Avenue Parmentier to reach La Belle Equipe. The specified constraints do not quite uniquely determine the designated targets. But they reduce the range of possible Parisian street targets from more than 10,000 to just a few. Actual driving reconnaissance of the short-list would have narrowed down the choice to an optimal sequence of bars and cafés which could all be targeted within the set tight operational schedule, with alternative getaway options if a street were blocked. The importance of having alternative exits was clear from the January attack on Charlie Hebdo; the assailants' vehicle was blocked in by a police car and they had to shoot their way out.

After the Stade-de-France, the primary target in central Paris was evidently the Bataclan, both because of the venue and the band on the playbill. The impact on selected bars and cafés around it might be interpreted as collateral damage at a micro-terror level. It is extremely unlikely that any of these small eating and drinking establishments would have been primary terrorist targets, but they fell within the extended spatial footprint of the macro-terror shooting attack on the Bataclan. The possibility of small businesses suffering collateral loss as secondary targets in this indirect manner should be recognized by terrorism insurers.

The need to keep rigidly to the precise strategic scheduling meant that the toll of deaths and injuries in local bars and cafés was lighter than it might otherwise have been. At 9.25pm, the shooting started at Le Carillon and Le Petit Cambodge, at the crossroads junction of Rue Bichat and Rue Alibert, as shown in Figure 2.

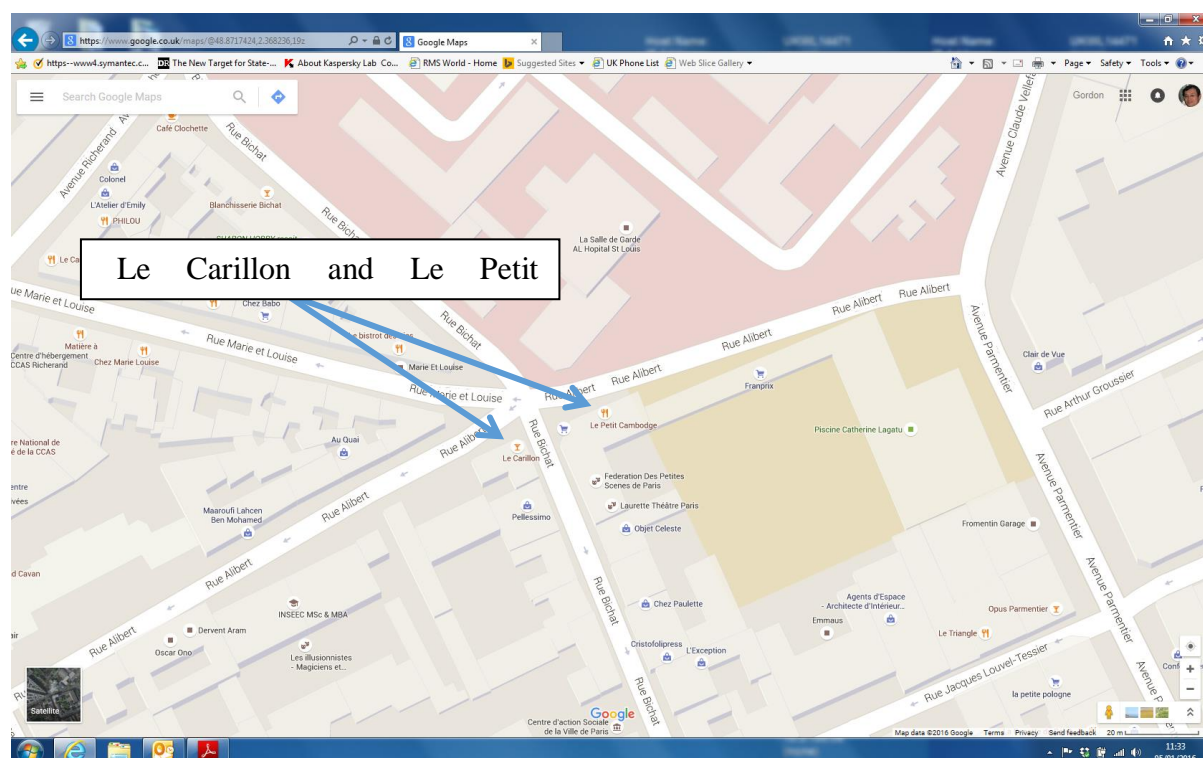


Figure 2: Crossroads attack on Le Carillon and Le Petit Cambodge

A few streets away at 9.32pm, La Café Bonne Bière and La Casa Nostra were struck at the junction of Rue du Faubourg du Temple and Rue de la Fontaine au Roi. Several of the seriously wounded might have survived if the emergency medical response had been better equipped; stretching critical care facilities was a strategic aim of the attack strategy. At La Cosa Nostra, Salah Abdeslam was caught on CCTV shooting at patrons, but left when his AK47 misfired. Driving a few kilometres southeast, past the Bataclan, at 9.36pm the shooters next targeted La Belle Equipe on Rue de Charonne at the junction with Rue Faidherbe. The front seat passenger got out and did the shooting, the driver provided cover with his AK47. There were also casualties at the adjacent Sushi Maki Japanese restaurant.

At 9.40pm, Ibrahim Abdeslam ended the shooting spree at Le Comptoir Voltaire, situated at the other end of the Boulevard Voltaire from the Bataclan. This final café attack was synchronized with the start of the assault on the Bataclan to surprise and confuse the first responders. As it happened, the fire and the SAMU emergency medical service had a terrorism training exercise that morning.



There were still five AK47 magazines left, after eleven had been used in the firing of hundreds of bullets. But by this time, the chance of armed police response was high, so rather than continuing shooting until the very end, Ibrahim Abdeslam detonated his suicide vest. According to the ISIS communiqué, another suicide vest detonation in the 18th arrondissement, perhaps around Montmartre, seems to have been planned for the north of Paris. But Ibrahim's brother, Salah, deviated from the attack plan and abandoned his car in Place Albert Kahn in the 18th arrondissement. He phoned local friends from Molenbeek to pick him up and drive him back to Belgium.

According to police sources, all the terrorist shootings at the Bataclan took place before 10pm. To have saved more lives, the police response would have had to have been swifter. But any local police would have drawn to the bars and cafés attacked. It was only just before 10pm that a brave commissioner from the BAC (Brigades-Anti-Criminalité) arrived at the Bataclan and managed to shoot one of the terrorists, even though he was not equipped to deal with criminals armed with assault rifles.

At about 10.15pm an elite team appeared on the scene from the BRI (Brigades de Recherche et d'Intervention) to relieve the BAC. BRI is a special unit of the Paris police department, intervening only within and around the capital. They are expertly trained for stakeouts and surveillance. The BRI chief, Christoph Molmy, had been notified of the Stade-de-France suicide bombings and the attack on a bar in Rue de Charonne, and immediately mobilized his fifteen-man Rapid Intervention Force. They gathered at their landmark Paris office at 36, Quai des Orfèvres, before driving several kilometres to the Bataclan.

The security guard who stopped the first suicide bomber from entering the Stade-de-France was praised for saving France. The mitigating impact of his vigilance is all the greater in the context of the overall attack plan. For terrorism risk estimation, it is salutary to contemplate the counterfactual scenario where the first suicide bomber succeeded in entering the stadium. After the first bomb explosion at 9.20pm, there would have been a number of severe casualties, and panic leading to a disorganized exodus of 80,000 from the stadium. A subsequent explosion at 9.30pm would have struck exiting spectators. A major police alert would have been raised, sweeping in armed response from BAC and BRI. A further bomb explosion at 9.53pm would have raised the alarm level and increased the sense of uncertainty and dread around Stade-de-France yet further. The initiation of the Bataclan attack at 9.40pm might then have taken advantage of the extra time available to shoot even larger numbers of the sell-out audience before the armed police intervention. The overall death toll might then have been a catastrophic multiple of the actual number.

### CHOICE OF WEAPONRY

The two stock terrorist weapons for maximizing casualties in crowded public spaces are improvised explosive devices and assault rifles. Both were deployed in Paris. The eight operatives each wore a suicide vest containing triacetone triperoxide (TATP) explosives. TATP is highly volatile, and the blast impact is variable. At the Stade-de-France, only one bystander was killed, even though three suicide vests were detonated. Salah Abdeslam's unused suicide vest was found discarded in a dustbin in Montrouge. The bomb-maker was identified quickly as Mohammed Khoualed from Roubaix in northern France.

More reliable than an Improvised Explosive Device is the AK47. It was this weapon that caused almost all the casualties. There were 130 fatalities and more than 350 injured. As is common

with terrorist attacks in crowded public places, the young and middle-aged were the main victims. Of the dead, 25% were in the age range of 35-39; 20% were in the age range of 30-34, and also 25-29. About 10% were in the age range of 20-24 and also 40-44.

Outside international arms dealers, it is not widely known that, since the Napoleonic era, Belgium has been a centre for weaponry. When it comes to re-modelling of light military weapons, Belgium has the 'savoir-faire'. One-third of EU small arms sales to the Middle East and North Africa come from Belgium. Large quantities of re-modelled AK47s from Yugoslavia are on the Belgian market, and have been used for both criminal and terrorism purposes. The transport of such weapons across continental Europe is facilitated by the Schengen area agreement, which removes border checks within the European Union. The ready supply of weapons makes Brussels a European terrorist arms bazaar and supermarket. Ayoub El Khazzani was armed with a re-modelled AK47 when he attempted to shoot passengers on the Thalys train from Brussels to Paris on 21st August 2015.

## **FAILURE OF BELGIAN AND FRENCH COUNTER-TERRORISM**

Since 9/11, there have only been two major successful macro-terror attacks against the Five Eyes Alliance of USA, UK, Canada, Australia and New Zealand. These were the London transport bombing of 7th July 2005 and the Boston marathon bombing of 15th April 2013. Through the technical excellence and international coverage of counter-terrorism surveillance, dozens of terrorist plots against the Five Eyes Alliance have been interdicted since 9/11. As disclosed by the NSA whistle-blower Edward Snowden, suppression of terrorist plots is expedited by the covert process of contact chaining: if any conspirator contacts somebody who is in contact with a known terrorist, the conspirator will be placed under communications surveillance. The larger a conspiracy, the greater is the chance that one of the conspirators will be under communications watch. Accordingly, due to oppressive covert surveillance, a high proportion of the plots against USA and UK have been lone-wolf plots.

The fact that so many plots have been foiled owes much to the capability and professionalism of the American and British security services, and also to an element of luck when the police are tipped off about suspicious behaviour or randomly search a car or property. For both the 2005 London and 2013 Boston bombings, at least one of the terrorists was known to the security services, but none was a proven terrorist. There was some failure of counter-terrorism, but not on the scale that allowed three teams of three terrorists to attack at will across Paris on the November evening of Friday 13th – the day when counter-terrorism luck ran out.

Two months earlier, on 11th August, a French supporter of ISIS, Reda Hame, was stopped on his return from Syria and detained for plotting a mass-casualty attack on a concert hall. In September, French officials were actually warned of an imminent attack by their American counterparts, who have superior international communications intercept and electronic eavesdropping capabilities. But they were blindsided by the attack being plotted across the border in Belgium, which is a country lacking an intelligence culture. At the highest level of the domestic intelligence agency (Sûreté de l'État), it is recognized that there is a lack of interest or even mistrust against the intelligence service among politicians and the public. This negative situation has been aggravated by Edward Snowden's disclosure that GCHQ hacked into Belgacom, Belgium's largest telecommunications provider, to install spying malware allowing GCHQ to tap Belgian phone calls.

The 13th November Paris attack was planned from the run-down Molenbeek immigrant district of Brussels, with 30% unemployment, notorious for being the Jihadi capital of Europe and

weapons trafficking centre. The mastermind was Abdelhamid Abaaoud (aka Abu Omar Al Belgiki), a Moroccan-Belgian, who was a self-confessed terrorist, well known for his involvement in a number of terrorist plots. In his absence, he was sentenced to 20 years by a Belgian court. Even if terrorists are elusive, and their whereabouts uncertain, surveillance can be undertaken of their communications. In January 2015, Abaaoud's cell phone was reportedly traced to Greece from calls made to Jihadi contacts in Belgium.

No terrorist plot of any complexity can be planned and executed without a substantial amount of electronic communication. Regrettably, Belgian capability in communications surveillance has been limited, even primitive. Before 2010, the domestic security agency was legally unable to use standard intelligence gathering methods such as bugging, video surveillance, phone taps and computer hacking. Only with the passage of a new law in 2010 were these basic intelligence-gathering techniques allowed.

To make security even more challenging, Belgium has highly fragmented administrative systems. In Autumn 2013, three Jihadi training camps were identified in the Ardennes by the Belgian intelligence service. However, this information was not transmitted to the local police. Brussels itself has six policing zones, which impedes information exchange. To compound the cross-border counter-terrorism dysfunction, the French internal security service, *General Directorate for Internal Security (DGSI)*, did not share its extensive list of Jihadis in Syria with its Belgian counterpart.

Belgium has provided a comparatively safe haven for terrorists within Europe. A Belgian lapse in counter-terrorism might only have repercussions within its borders, except for the Schengen agreement. Belgian terrorists could drive the 150 miles from Molenbeek to Paris as if the French border did not exist. The superior French counter-terrorism capability was negated by the Belgian terrorist threat source. To deter Belgian terrorists from striking France again, President Hollande of France has called for major security reforms that will stretch the interpretation of the Schengen agreement.

Within the context of US Homeland Security, the national fragmentation of continental European security would be as if both the National Security Agency and the Federal Bureau of Investigation were abolished, and each state of the union had its own separate security and law enforcement detective agency. The smaller states would have far less resources for their own state agencies. Through inter-state freedom of movement, this would diminish security in the larger states, where the US terrorist targets are mostly concentrated. The prospect of heavily armed terrorists based in rural Vermont crossing over at will into New York State and towards Manhattan would alarm and could surprise the New York Police Department, and contract the US terrorism insurance market.

### NETWORK OF OPERATIVES

According to the ISIS communiqué, eight brothers wrapped in explosives belts, and armed with machine rifles, targeted sites in the heart of the capital of France. Their leader, Abdelhamid Abaaoud, was present in Paris to oversee the attacks, and is believed to have participated in the bar and café shootings. Abaaoud's fingerprints were on an AK47 in the black Seat Leon shooters' car abandoned in Montreuil. It is known from CCTV that he took the metro back into Paris from Montreuil, where the car used for the bar and café shootings was found. He was a notorious Belgian terrorist, one of 500 jihadists for Syria and Iraq to have emerged from a Belgian population of only 11 million — the highest figure per capita in the

European Union, and twice as high as France. He was summarily brought to justice during a police raid in Rue Corbillon, Saint-Denis, a few days later.

The Paris terrorist attack force was comprised of three teams tasked with striking the Stade-de-France; the Bataclan concert hall; and neighbouring bars and restaurants. At the Stade-de-France, two operatives were brought in from Syria via the refugee trail from Turkey to Greece. They were accomplices to Bilal Hadfi, who was the last of the three to detonate his suicide vest. Bilal Hadfi, a French national, living in Molenbeek, had openly posted his Jihadi sentiments on Facebook in June. Like his two accomplices, he had a Syrian connection. After his departure for Syria early in 2015, Belgium issued an international arrest warrant for him.

Molenbeek was the Belgian base for the bar and café shooting team, which comprised the Abdeslam brothers, Ibrahim and Salah, and Abdelhamid Abaaoud. The inclusion of a Molenbeek friend in the Stade-de-France team was important for Abaaoud's control of the attack plan. Bilal Hadfi was in phone contact with Abaaoud for much of the forty minutes before the first suicide bomb detonation.

Molenbeek is the source of the highest concentration of jihadi foreign fighters in Europe. In 2001, it was in Molenbeek where the assassins of Afghanistan's anti-Taliban commander Ahmad Shah Massoud had stayed. It was also a haven for Hassan El Haski, one of the masterminds of the 2004 Madrid train bombings. Mehdi Nemmouche, the principal suspect in the Jewish Museum attack in Brussels in May 2014, also stayed there. Ayoub El Khazzani, the shooter in August 2015 on a Paris-bound Thalys train from Amsterdam, stayed in Molenbeek with his sister before boarding the train in Brussels. His re-modelled AK47 jammed, and he was overpowered by several passengers. Otherwise his rampage might have been so deadly that the export of terrorism from Molenbeek to Paris could then have been placed under tight control.

The third 3-man attack team was entirely French. First, there was Sami Amimour, a noted French terrorist, who defaulted on his weekly obligation to report to a police station, and was under international arrest warrant. Secondly, there was Ismael Mostefai, who was marked by French authorities as being radicalized, and whom the Turkish authorities had warned the French about, whilst travelling to Syria. The third was another Syrian veteran Fouad Mohamed-Aggad. At the end of 2013, Fouad Mohamed-Aggad travelled to Syria with his brother Karim, and a group of friends from Strasbourg. Most were arrested in Spring 2014 when they returned to France. But he stayed in Syria, not wishing to go to prison in France. He made his final return to France for the Bataclan attack.

The Paris attacks were planned across the border in Belgium, which has an inferior capability in counter-terrorism surveillance, and where weaponry is a thriving business sector. Without any border checks between France and Belgium, because of the Schengen area agreement, Molenbeek terrorism could be covertly exported to France. Furthermore, the two suicide-bomber Syrian operatives swept in to western Europe with a tide of destitute refugees via the porous Greek island border with Turkey. This Syrian duo along with the Molenbeek terrorist quartet were not only trusted and dependable ISIS operatives, but they also had a comparatively low counter-terrorism profile in France.

Thus the effective number of plot operatives potentially visible to DGSI was reduced from nine to just three: the Bataclan terrorist trio. But it was this French trio who were responsible for the bulk of the carnage on 13th November. The Stade-de-France suicide bombings essentially

failed, with just one passer-by killed. Furthermore, when considered purely on their own, the bar and café shootings amounted to a Belgian micro sub-attack diversion for the police and emergency services, with lesser value property targets than for a macro-terror attack.

### **BATACLAN TERRORIST TEAM SELECTION**

At about 10%, France has the highest proportion of Muslims in the population of any western European country. Amongst French Muslims, there is substantial minority support for ISIS. There may be as many as 20,000 who hold radical Islamist views, and who might be a threat to French national security. According to Prime Minister Manuel Valls, intelligence services have files on 10,500 individuals who have been radicalized to a greater or lesser extent. Of these, as many as 7,000 are on a severe terror watch list. About a thousand French nationals have travelled to Syria and Iraq to fight with ISIS. Of these, about 150 have died and will never return.

The Bataclan attack team might have been drawn from the ample reserves of radicalized French Muslims, with little or no counter-terrorism profile, and who had never visited Syria. There would have been clear security advantages, but there would have been doubts about their combat capability, dependability and trustworthiness. By contrast, Syrian veterans would have been trained, battle-hardened, and have already demonstrated their commitment. The trade-off between operational secrecy and effectiveness was decided by ISIS in favour of the deployment of Syrian returnees. All three of the Bataclan shooters were not only French but also well known to DSGI as Syrian fighters.

The eight hundred surviving French ISIS combatants might well have been prioritized for communications surveillance, given their combat suitability as team members for an ISIS attack in France. There must have been a substantial amount of electronic communication between the Bataclan trio. It is known that on the evening of 13th November they received tweet messages sent from an ISIS tweet account @op\_is90. Electronic surveillance might have picked up some of this communication. It is confirmed that before the 13th November attacks, encrypted messages were sent by terrorists via WhatsApp and Telegram App. But even if communications were encrypted, the meta-data on the communications might have raised the French counter-terrorism alert.

Notwithstanding civil liberties restrictions on eavesdropping on communications in France, a significant percentage of known French ISIS combatants can be intensively surveilled. Given the size of DSGI, with several thousand officers, it seems realistically plausible that tight surveillance could be maintained over at least several hundred Syria returnees, which is approximately a quarter of the number of French Jihadis who survived fighting for ISIS. Even if only one quarter of known French ISIS combatants were electronically tracked by DSGI, there would then have been about a 60% chance that the plot would have been compromised through one of the three operatives being detected before moving towards the Bataclan. ISIS pushed their luck with using three operatives all of whom were known already to the French counter-terrorism services, rather than using 'clean skin' radicalized individuals with no Syrian combat experience.

### **CONCLUSIONS**

After the October 1984 Brighton bombing which came very close to assassinating the UK prime minister, Margaret Thatcher, the IRA famously taunted: *'We only have to be lucky once, you will have to be lucky always'*. Both Belgium and France have been lucky to have interdicted



as many terrorist plots as they have since 9/11. But the Paris attacks on 13th November 2015 exposed gaping weaknesses in European border security, and were a major joint failure of Belgian and French counter-terrorism.

The terrorists too were lucky to get away with deploying so many Belgian and French operatives known to the authorities, without their ambitious brazen plot being interdicted. On 13th November, ISIS boldly fielded four operatives known to the Belgian authorities, and three known to the French authorities. Just two Syrian suicide bombers were additional to the Belgian and French operational team.

In 2006, Al Qaeda plotted to bring down seven transatlantic aircraft using liquid explosives, in what chief strategist Ayman Al Zawahiri boasted would be the biggest multiple terrorism strike since 9/11. This was interdicted through the combined capabilities of the UK and US counter-terrorism forces. Had this plot originated in Molenbeek, Belgium, rather than Walthamstow, England, and targeted flights departing from Paris rather than London, the outcome might have been very different.

After the terrorist attacks in Paris, western intelligence services stepped up their surveillance. They intercepted communications between Abdelhamid Abaaoud and Islamic State leadership in Syria. Furthermore, through discovery of a cell phone near the Bataclan with contact details for Hasna Aitboulahcen, the cousin of Abaaoud, a planned second Paris attack phase at La Défense was completely disrupted, and the operatives killed, including Abaaoud himself.

The European Union does not function as a police state such as the former East Germany, where all suspected dissidents were under oppressive surveillance by the feared Stazi. Track cannot be kept of all ISIS supporters. Strategic thinking could prioritize surveillance resources, in particular in respect of Syrian returnees. Those with Syrian experience are trained, have shown commitment, and can be trusted. By contrast, those who are radicalized but have not taken the initiative to fight in Syria may not be as reliable, neither in terms of technical capability, nor in terms of being able to maintain tight plot secrecy.

Individual countries within the Schengen zone, like Sweden and Denmark, are reinstating their own border controls to protect against illegal migration through porous European external borders. As an immediate response to the counter-terrorism failures, new measures to tighten European border security are to be introduced. One is the creation of a standing European border force and coastguard to take control of external frontiers. Another is the creation of a European passenger name record system for air passengers entering or leaving the European Union.

Furthermore, the European Commission will adopt a European Agenda on Security which will reorient the EU's internal security to meet the challenges posed by current criminal and terrorist threats. This will strengthen cooperation between Europol and other European agencies and threat assessment bodies, notably EU INTCEN (European Intelligence and Situation Centre). It will also reinforce the exchange of information at EU and international level on illegal firearms. Until these measures take effect, the terrorism risk in continental Europe will remain significant. Assistance from UK should be valuable.

Lord Carlile, overseer of UK counter-terrorism legislation has commented to Newsweek: *'The security services in Belgium are nothing like as good as the French security services. Plainly, what is needed is cooperation within the EU to ensure security services and*

*intelligence agencies are on the same page about threats to shared security. It is vitally important that the Belgian government reassures security services and police in the rest of Europe that it has the capacities to deal with similar plots. If not, they should be willing to accept our assistance. I would suggest the UK security services have demonstrated themselves to be superbly competent to assist.'*

These countries of the Five Eyes Alliance collectively have superior intelligence, eavesdropping and decryption capabilities than exist in the Eurozone, and USA and UK assume more sweeping surveillance powers, and far-reaching objectives. For example, GCHQ states an ambition to exploit any phone, anywhere, any time. Crucially, with long coastal national boundaries, border security is far tighter in the English-speaking western democracies than within the Schengen zone where most land borders can be crossed without challenge.

The barrier to entry into USA, UK and Australia is very much harder. But the intent to attack these countries is clear. The ISIS communiqué ended with a stark threat: *This attack is just the start of the storm, and a warning to those wishing to contemplate and draw lessons.* Abdelhamid Abaaoud is believed to have visited UK in August 2015, using a false passport. On his cell phone, there were pictures of the Birmingham Bullring, the city's most popular tourist venue. Shopping malls like this and Les Quatre Temps in La Défense are prime targets for terrorist armed assaults. A number of radicalized Muslim youths from Birmingham are known to have joined IS in Syria. The highest ranking of these was Junaid Hussain, leader of ISIS's cyber caliphate wing. He was killed in an air strike in August 2015.

For ISIS to perpetrate a major multi-pronged terrorist attack within UK, USA or Australia, they would need to push their luck much further than they did in Paris. Already a number of ISIS plots in UK have been interdicted. This should give insurers confidence in the capabilities of the Five Eyes Alliance to deal with the evolving ISIS threat. Insurers need to keep faith with the security services of the countries in which they have terrorism risk exposure. The terrorism threat is persistent and opportunist; always seeking to exploit any weaknesses in security and deficiencies in intelligence gathering. Ultimately, it is the occasional counter-terrorism failure to interdict a macro-terror plot that insurers are providing coverage for.

### LESSONS FOR TERRORISM INSURERS

In a bygone 20th century terrorist threat era, the IRA provided bomb warnings to avoid civilian casualties that would have alienated their Catholic support base in Ireland. A high percentage of warnings were hoax calls intended to cause economic dislocation. Causing economic loss and massive property damage were the significant impacts that the IRA leveraged with their bombing campaigns, rather than a high toll of civilian deaths and injuries.

With Islamist militants, especially ISIS, killing infidels is not just acceptable, it is their principal desire and objective, rather than inflicting property loss. (Ayman al Zawahiri, the Al Qaeda leader, commented that the economic cost of ever tighter homeland security was in itself a severe economic burden inflicted by militant Islam.) On 2nd November 2011, the Charlie Hebdo office in Paris was petrol-bombed by a Molotov Cocktail at 1am, the day after it had named the Prophet Mohammed as its editor-in-chief for the week's issue. The local impact of this property damage and business disruption was as nothing compared with the shock and horror that resonated around the world at the assassination of the Charlie Hebdo committee on 7th January 2015.

Insurers should always seek to learn new lessons from events that occur. It is well appreciated from international experience of terrorism that lethal micro-terror armed attacks against occupants of small businesses, (such as shops, restaurants and offices), can occur essentially anywhere. The San Bernardino attack on 2nd December 2015 killed fourteen workers attending a small nondescript office party in a town with a population of two hundred thousand.

A new lesson from the Paris attacks of 13th November 2015 is that there can be noteworthy micro-terror collateral loss within the overall footprint of a macro-terror strike. Irrespective of the specific weapon attack mode used at the Bataclan concert hall, (whether armed suicide attack; back-pack, vehicle or incendiary bomb), there was an operational rationale for ancillary small arms attacks nearby. These would divert any police who happened to be nearby, to ensure the Bataclan assailants would have fifteen minutes of unanswered shooting.

Establishing such a secondary micro-terror smokescreen around a primary terrorist target comes at a price to a terrorist organization. More operatives are required to go on a local shooting rampage. Increasing the number of operatives inevitably increases the likelihood of plot interdiction. In the case of the Paris attacks, the security price was low: the shooting team acquired weapons easily in Belgium, rented cars with Belgian number plates, drove across the open Belgian border from Molenbeek, and were almost invisible to the French counter-terrorism authorities. Outside the Schengen zone, foreign terrorists would be harder to infiltrate, but the threat of ancillary small arms attacks within a macro-terror footprint remains a prospect within the western alliance that needs to be considered by terrorism insurers.

Whereas the effect on a scenario estimate of Probable Maximum Loss may not be so significant, it should alert terrorism underwriters to the coverage requirements of small businesses. Insurers have long known that collateral damage to small businesses may arise within the blast radius of a nearby vehicle bomb targeted at an attractive target. The extent of the blast radius depends on the explosive yield of the vehicle bomb.

But any macro-terror attack may generate an extended footprint of intermittent collateral loss. As demonstrated by the Paris shootings of 13th November 2015, this footprint may stretch for several miles. Given the high density of attractive terrorist targets within an urban environment, a corollary is that all small businesses would be advised to have some terrorism coverage for the contingency that they happen to be attacked along with a large corporation or similar principal terrorist target.