Blackthorn.

LOCKTON
REINSURANCE

BEYOND THE BLAST:

CAPITAL MANAGEMENT OF TOMORROW'S TERROR THREATS

- **Exposure**
- **Peril**
- Risk Transfer
- Placement

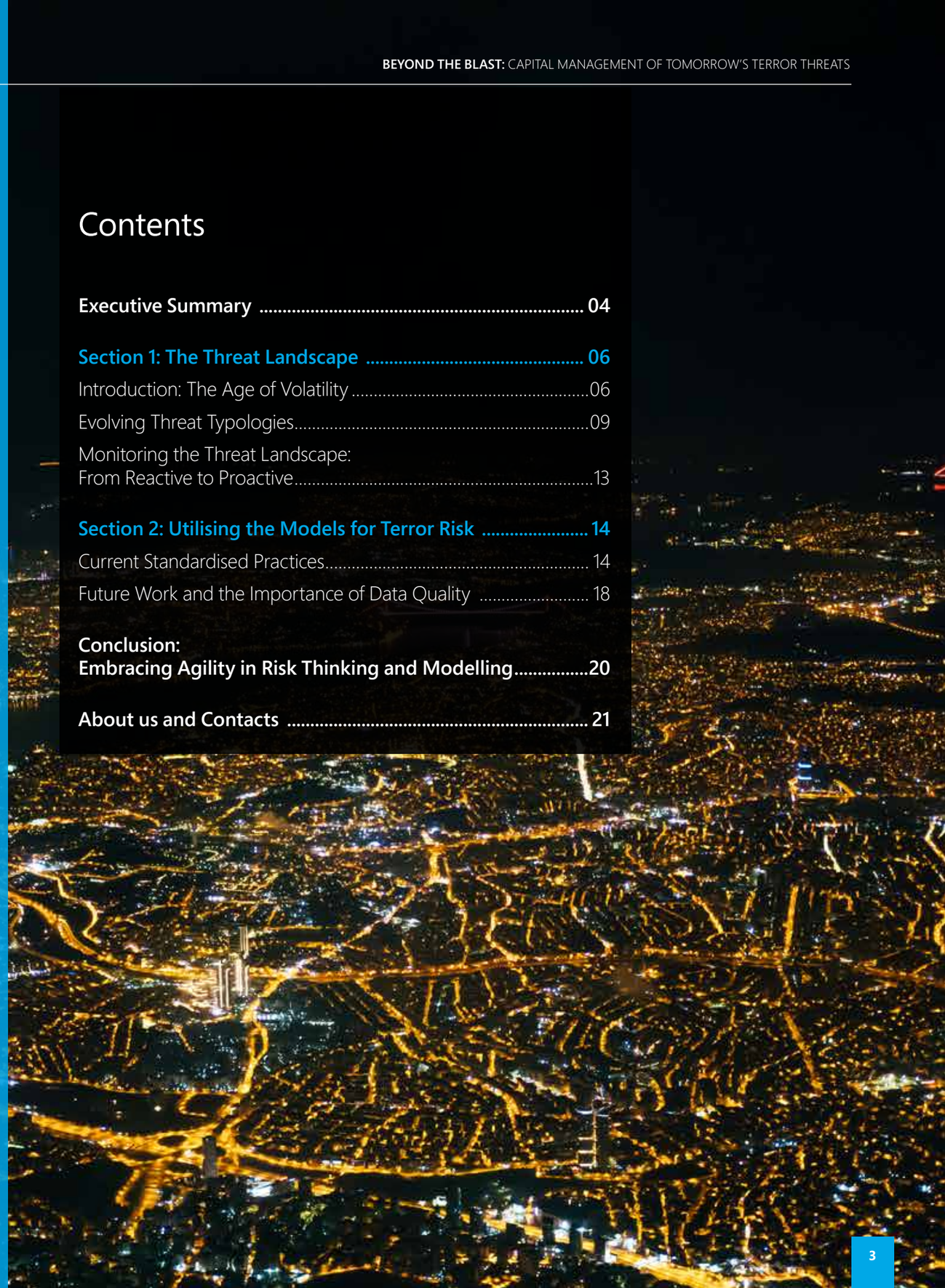
In the last five years, the war, terrorism and political violence (WTPV) insurance sector has experienced exceptional loss activity driven by new realms of geopolitical instability, yet carriers have generated healthy margins and have only been threatened by the constriction of reinsurance. As is often the case in our business, the impact of insurance on economic loss is limited because of capital requirements and the degree to which companies are willing to allow the war and terrorism components to take a greater position within the diversified portfolio.

In this paper, we bring together thought-provoking insights into the threat landscape from Blackthorn with modelling reactions from Lockton Re's lead WTPV modeller, George Wragg. For some time now, the narrative has stated that sophisticated extreme events are unlikely, yet the capital assessment remains without any mitigation by damage ratios. The premise is that, without a more enlightened treatment of event exposure, our conservative view will prevent penetration, pressure prices and threaten margins. The focus is concentrated on the Terror peril: we will follow up on the subject of SRCC and Political Violence at another time.

The intention here is not to escalate the global risk rating but to break down the nature of risk and assess how the reinsurance industry might evaluate today's threat landscape. This brief shows this landscape is reasonably well understood and that with enhanced data capture, capital calculations can be eased and new opportunities can be realised. The industry, otherwise, continues to scratch at the surface of a business class that has delivered 24 years of continuous profit.

> "The industry continues to scratch at the surface of a business class that has delivered 24 years of continuous profit."
>
> Paul Upton,
> Chairman of Specialty Division, Lockton Re

Contents



Executive Summary

Precedent shows that the modern terrorism threat landscape is far from static. Since the attacks of 11 September 2001, the global security environment has evolved continuously, shaped by shifting geopolitical, social and technological factors. While periods of apparent stability in attack types or frequency may create an illusion of predictability, volatility is now the defining feature of the operating context. For organisations engaged in threat and risk assessment, underwriting and claims management, assuming long-term constancy risks operational misalignment, outdated protective measures and, ultimately, major insurance losses. Agility in risk thinking – and in supporting modelling frameworks – is therefore essential.

The evolving landscape is being reshaped by five key drivers:

Strategic competition and the state–non-state nexus – proxies and hybrid tactics being used to pursue geopolitical goals.

Political and social polarisation – deepening social and political divisions heightening risks of unrest, lone-actor attacks and extremist violence.

Technological innovations and regulatory gaps – artificial intelligence (AI), social media and additive manufacturing enabling new attack methods.

Climate change – environmental and economic pressures amplifying instability.

Convergence of established risk categories – terrorism, political violence and cyber threats increasingly intersecting.

Together, these dynamics are creating a complex, unpredictable environment that challenges traditional risk assumptions and modelling approaches.

In Western countries, terrorism has notably shifted from centralised, high-sophistication operations to a mix of lower-sophistication lone-actor attacks, state–proxy convergence and technology-enabled threats. While large, coordinated bombings are now less common, accessible technologies such as drones, AI-assisted planning and 3D-printed devices have lowered barriers for both independent actors and state-linked proxies, potentially increasing both the frequency and severity of attacks. With the influence of the above drivers, this evolution expands the spectrum of potential losses and further underscores the need for adaptive, forward-looking modelling approaches.

Among emerging threats, weaponised unmanned aerial vehicles (UAVs), such as drones, represent a critical exposure. Their accessibility, precision and ability to bypass traditional security measures create multi-line risks across property, casualty, business interruption and aviation. Attribution challenges – whether incidents are deemed terrorism, political violence or acts of war – further complicate underwriting and claims management.

To best prepare for this era of volatility, reinsurers should shift from reactive monitoring to proactive adaptation. Establishing systematic trigger thresholds, supported by quantitative and qualitative indicators, enables earlier identification of structural changes in the threat environment and timely recalibration of models. Triggers may include increases in state-linked activity, novel attack methodologies or regulatory shifts affecting dual-use technologies.

The London market standardised method for terrorism risk assessment in reinsurance has long relied on a set of simplified assumptions focused around identifying,

> The capacity to think ahead about emerging threats and their potential convergence is no longer a competitive advantage but an operational necessity for sustainable risk management in this age of volatility.

monitoring and managing exposure concentrations within a prescribed distance. However, in light of the increasingly volatile and complex threat landscape, it has also become even more apparent that conventional measures such as 100% probable maximum loss (PML) may not adequately capture the highly concentrated damage at the point of an attack, reinforcing the need for adaptive, location-sensitive modelling strategies.

In evaluating portfolios against realistic scenarios, it is important to include factors such as coverage type, excess points and data quality. By highlighting how different assumptions, such as variations in bomb size, building height or construction type, affect the view of risk, greater context is given.

Comparison of 250m-radius blast zones using un-PML-ed exposures regularly evaluates potential loss levels greater than 10-tonne bomb scenarios (usually deemed as inconceivable, currently). To achieve more robust analysis and allow efficient output, the market needs to embrace enhanced data capture. In the first instance, this needs to include improved geocoding and policy attachment information. Buyers also need to pay attention to individual policies that drive volatility within their portfolios.

As the market embraces more sophisticated analysis of Terror exposures, carriers need to keep a watchful eye on emerging Realistic Disaster Scenarios (RDSs).

The use of drones, in particular, will create new modelling challenges and will challenge the reinsurance market to provide workable event definitions.

The forces driving volatility show no sign of easing. Strategic competition, technological acceleration, polarisation and climate pressures are continuing to converge, keeping instability as a central characteristic of the global operating environment. For the reinsurance sector, continuous monitoring and proactive assessment of how these trends may intersect to generate new risk scenarios is crucial. The capacity to think ahead about emerging threats and their potential convergence is no longer a competitive advantage but an operational necessity for sustainable risk management in this age of volatility.

SECTION 1: THE THREAT LANDSCAPE

Introduction: The Age of Volatility

Since the 11 September 2001 terrorist attacks in the US, the global threat landscape has undergone a profound transformation in both approaches and methodologies, extending beyond terrorism into a broader spectrum of malicious perils. The operating environment is now widely recognised as increasingly nonlinear in nature, with 'volatile, uncertain, complex and ambiguous' (VUCA) commonly referenced in both security and business circles. Given the almost certain persistence of variation in threat trends going forward, it is essential to consider how this evolving landscape might shape the future manifestation of high-profile acts of terrorism as well as other malicious threats and, importantly, what this means for the reinsurance industry's ability to anticipate and adapt.

For a reinsurance market primarily concerned with major loss events, acknowledging that further change is inevitable raises important questions about the validity of long-standing assumptions around terrorism events that underpin scenario modelling and pricing. As threats continue to evolve and associated impact severity (from an insurance perspective) remains dynamic, traditional processes could become increasingly misaligned with the realities of the risk transfer environment.

In light of these challenges, an overview of the key drivers of change within the malicious risks space provides important context. Recent security incidents illustrate that the landscape is being reshaped by a convergence of complex and interdependent factors:

Strategic competition and the state–non-state nexus

The existing world order faces increasing challenges from revisionist powers[1] such as China, Russia and Iran that seek to reshape global governance, offer alternative economic systems and develop regional spheres of influence. These states employ a range of hybrid methods to destabilise other nations and the political status quo, from political pressure, social engineering and influence to fomenting unrest, targeting critical infrastructure and sponsoring proxy groups, extremists or criminal networks to act in advancement of their strategic objectives – also affording enhanced plausible deniability.

The British Security Service, MI5, has noted that hostile state activity now accounts for approximately 20% of counterterror investigations, a five-fold increase since 2018. This shift introduces new threat actors, methodologies and targets – including the potential for more sophisticated, ambitious or large-scale attacks in the West – that existing models may not fully capture; it could drive a trend towards higher property and infrastructure losses (rather than a focus on human casualties) than in recent years, where hostile actors can inflict strategic economic harm while avoiding the political escalation risks associated with killing civilians.

Real-world example

Israeli Embassy plot: In May 2025, UK police arrested five individuals – primarily Iranian nationals – suspected of planning an attack on the Israeli Embassy in London. Officials suspected the involvement of Iran's Islamic Revolutionary Guard Corps (IRGC) covert Unit 840. Had the plot been successful, it likely would have triggered terrorism insurance claims for structural damage, tenant relocations and business interruption.

Political and social polarisation

Political and social polarisation in Western countries has intensified, creating conditions that amplify extremist messaging. This results in an elevated risk environment characterised by multiple unpredictable domestic flashpoints ranging from civil unrest to lone-actor terrorism and coordinated extremist violence, all of which could materially increase threat volatility and potential insured losses as well as complicate risk modelling.

Real-world example

US Capitol attack: In January 2021, political polarisation and extremist mobilisation culminated in the storming of the US Capitol, resulting in multiple fatalities, over 140 injuries and over US$30 million in property damage. The incident showed how sudden flashpoints of domestic polarisation can escalate into mass extremist violence, with the potential – had commercial assets been targeted – to generate insured losses in the hundreds of millions across property, liability and business interruption lines.

Technological innovations and regulatory gaps

The rapid development and democratisation of transformative technologies such as social media, AI and additive manufacturing[2] not only create new categories of exposure but also alter established risk profiles in ways that may be complex to model and highly uncertain in their accumulation potential. Such advancements are outstripping regulatory frameworks' ability to provide effective governance against malicious applications and lowering barriers to operational expertise, affording opportunities for malicious actors to enhance their capabilities.[3] While the growth of such technologies does not directly give rise to increased property damage, expanding the abilities of would-be lone actors and organised groups has the potential to escalate the frequency of medium-sized loss events through magnifying possible attack scale and severity.

Real-world example

Las Vegas AI-assisted bomb plot: In late 2024, a man in Las Vegas allegedly used an AI chatbot to calculate explosive quantities, source materials and plan a truck bombing on 1 January 2025. The attack injured bystanders but caused limited structural damage, partly because the homemade device only partially detonated. However, had more powerful or effectively constructed explosives been used, insured losses could have reached hundreds of millions across property, business interruption, liability and casualty lines.

[1] States that seek to fundamentally alter the prevailing international order.

[2] Additive manufacturing ('3D-printing') is a dual-use technology that enables rapid prototyping and customisation while allowing weapons or components to be produced outside regulated supply chains. While predominantly utilised to fabricate firearms, it is also increasingly being used to customise UAVs, a development that could enable more sophisticated, high-profile drone attacks with greater loss potential.

[3] For terrorist purposes, this might include automated attack planning (including facilitating the design of biological or chemical weapons), enhanced hostile reconnaissance and the generation and dissemination of propaganda or misinformation (potentially amplifying wider civil unrest).

Climate change

Climate change exacerbates existing vulnerabilities and creates new sources of volatility in the threat landscape. Environmental pressures can drive resource scarcity, population displacement and economic disruption, which can heighten the risk of social unrest, political violence and conflict. This interconnectedness amplifies accumulation potential and complicates efforts to model correlations between terrorism, strikes, riots and civil commotion (SRCC), natural catastrophe and other lines of exposure.

Real-world example

Climate change–linked extremist violence: Recent years have seen a global uptick in 'eco-fascist' violence motivated by perceived threats from overpopulation, environmental degradation and resource scarcity, such as the 2019 mass shootings in Christchurch, New Zealand and El Paso, Texas. While physical insured losses are relatively limited, climate-driven grievances act as a force multiplier, increasing the likelihood of triggering broader social unrest and politically motivated violence that intersect with other insurance lines.

Convergence of established risk categories

Geopolitical competition, conventional conflict, sub-state violence and information warfare are increasingly interwoven, producing hybrid threats that strain categorisation frameworks. This convergence further complicates coverage certainty as terrorism, political violence and civil unrest can interact unpredictably, creating exposure to a broader range of targets and amplifying accumulation potential across multiple insurance lines. Insurers now face the challenge of modelling overlapping perils where a single event – that might comprise sabotage, cyber disruption and physical violence, for example – may simultaneously trigger claims under terrorism, SRCC, cyber and property policies, complicating risk aggregation and allocation of capital.

Real-world example

South Africa riots: In 2021, mass rioting, looting, arson and violence triggered by political grievances swept through South Africa. The unrest resulted in insured losses exceeding US$2 billion, with extensive property and business interruption. The unrest blurred lines between opportunistic disorder and organised sabotage, sparking debate over whether it should be classified as SRCC, political violence or terrorism – a distinction with major insurance implications.

Evolving Threat Typologies

Underpinned by a combination of the above drivers, the terrorism landscape in the West has transformed over the past two decades from predominantly complex operations to lower-sophistication attacks. We have witnessed three broad phases:

1. Historically

Historically, high-profile terrorist activity was associated with centralised organisations such as Al-Qaeda, Basque nationalist and far-left separatist organisation Euskadi Ta Askatasuna (ETA) and factions of the Irish Republican Army (IRA) that conducted sophisticated, larger-scale and higher-severity operations requiring extensive planning, coordination, financing and specialised expertise. The 9/11 attacks exemplified this resource-intensive, internationally coordinated approach. It was also during this phase, in the early 1990s, that the Lloyd's RDS framework was introduced, which included a 2-tonne urban bomb scenario that syndicates are still required to stress-test their portfolios against today.

2. Post-9/11

Post-9/11, as the 'Global War on Terrorism' developed, counterterrorism pressure shifted attack tactics more towards small, decentralised cells and ideologically inspired but largely undirected individuals conducting less-sophisticated, lower-severity attacks utilising vehicles, knives and other simple methodologies. Internet proliferation facilitated this phenomenon, rendering prevention significantly more challenging. Additionally, while Islamist extremism remained the primary ideological concern globally, Western countries also saw notable increases in far-right extremist violence.

3. Currently

Currently, while many characteristics of the previous phase persist, terrorism (and, similarly, political violence), is increasingly shaped by an interplay of state involvement and technological innovation. Rather than overtly sponsoring large organisations, hostile states today more often leverage proxies, cyber-enabled operations and disinformation campaigns, further blurring the boundaries between terrorism, political violence and hybrid warfare.[4] Simultaneously, accessible technologies such as drones, 3D-printed weapons and AI are reducing barriers to entry for attack planning and effectiveness, as well as expanding the range and scalability of threat scenarios involving both state-backed and independent actors. Together, these dynamics create a more volatile and unpredictable environment than in previous eras.

Indeed, a 2025 study by the International Centre for Counter-Terrorism reported that more improvised explosive device (IED) attacks, attempted attacks or foiled plots occurred in the US in 2024 than in any other year since 2009, with three times as many cases as in 2023. The most common form was person-borne IEDs, primarily targeting crowded spaces, critical infrastructure and government buildings. While 80% of the incidents were thwarted by intelligence and law enforcement, the remainder either failed due to technical mistakes or were successful. This resurgence underscores that while large, centrally coordinated bombings have become rarer, IED use nevertheless remains a persistent and adaptive threat. Furthermore, cuts to US domestic counterextremism funding in early 2025 risk undermining interception capabilities and allowing the elevated level of IED use to continue or worsen. Importantly for reinsurers, even small-scale IED incidents can produce liability, casualty and business interruption losses that add up over time, especially if elevated frequency persists.

[4] A strategy that blends conventional military force with nonmilitary tactics such as cyberattacks, disinformation, economic pressure and proxy forces to weaken an opponent while avoiding open war.

While this report focuses on threats to Western countries and major urban centres, it is important to highlight that both key drivers of change and dominant threat typologies vary across regions; localised conflict spillovers, resource scarcity or insurgent dynamics may shape the operating landscape differently in Africa, the Middle East or South Asia than in Europe or North America. Although this geographical variance does not alter the core conclusion – that the threat environment is evolving in ways that complicate modelling – it reinforces the need for flexible, context-specific monitoring and scenario analysis (explored further in the 'Monitoring the Threat Landscape: From Reactive to Proactive' section on page 13).

What current (and future) developments mean for reinsurance

For reinsurers, the significance of the above shifts is not only in the headline evolution from complex international plots to simpler lone-actor attacks but also in how more subtle developments reshape the mechanics of loss over time. As highlighted, the adoption of emerging technologies, repurposing of non-terrorist methodologies for extremist purposes and blurring of traditional boundaries between perils all complicate risk classification, accumulation management and coverage interpretation. The result is a greater potential for systemic insured losses and heightened uncertainty in modelling, requiring a more agile and adaptive process (explored further in Section 2 of the report).

For brokers, the convergence of risk categories also strengthens the case for combined terrorism / political violence / war solutions, while for insureds, it means greater clarity is needed on how policies respond to 'grey zone' violence.[5] Insureds should further assess whether political, social or commercial connections increase their exposure to targeting within the continually evolving threat landscape.

In addition, it is important for the insurance market to keep abreast of developments that might lead to notable future evolution in threat tactics and methodologies, such as advances in drone usage and capabilities.

Unmanned aerial vehicles (drones)

In conventional warfare, UAVs have become both widespread and increasingly lethal. Defence news reporting from 2025 confirms that drone attacks now cause more than 70% of combat casualties in Ukraine, with the conflict acting as an incubator for rapid innovation. However, the threat is not confined to battlefields: In 2024, the Danish Institute for International Studies estimated that over 65 non-state armed groups had drone capabilities, and this proliferation has already produced major attacks such as a 2023 strike in Homs, Syria, which killed more than 100 people.

From a counterterrorism perspective, perhaps the most concerning development is how easily commercially available drones – including heavy-lift models – can be adapted and weaponised with components readily purchased online. This places effective aerial attack capabilities within reach of lone actors or small groups with only modest resources and technical knowledge. Furthermore, unlike ground vehicles, drones can bypass many security perimeters and target critical vulnerabilities (those with the greatest potential to cause widespread business disruption) with precision, potentially amplifying attack severity and associated losses.

> "For reinsurers, weaponised drones represent a multi-line exposure across property, mass-casualty liability, business interruption, event cancellation and aviation."

For reinsurers, weaponised drones also represent a multi-line exposure across property, mass-casualty liability, business interruption, event cancellation and aviation. The 2018 drone sightings at London Gatwick Airport that suspended over 1,000 flights and caused insured losses in the tens of millions of pounds also underscored the challenge of attribution. Authorities could not determine whether the disruption stemmed from terrorism, eco-activism, mischief or even state-linked interference. This uncertainty illustrates how drones can blur multiple coverage boundaries at once – between malicious mischief and terrorism or between terrorism and acts of war when state proxies, insurgents or ideologically motivated individuals might deploy similar technologies – raising the prospect of complex and prolonged disputes.

Looking ahead, the rapid spread of drone technology heightens the risk of high-severity urban attacks and makes proactive scenario analysis and stress-testing essential to ensure models capture the scale of potential impacts.

Contemporary Realistic Disaster Scenarios

While a low-sophistication, casualty-focused vehicle or knife attack remains the most likely terrorism scenario in Western countries, and the routinely modelled 2,000kg TNT NEQ[6] vehicle-borne IED remains the most credible 'worst-case' scenario (where extensive property damage and operating disruption are more likely), the evolving threat environment necessitates a review of other emerging, potentially high-severity scenarios to better inform contemporary risk modelling. For the reinsurance market focused on both accumulation and high cost 'tail events', recent developments in drone capability and utilisation warrant further exploration.

The following RDS is predicated on recent technological developments as a plausible scenario for reinsurers to be aware of and that can be used to guide proactive threat monitoring. However, it should not be seen as a prediction of how high-impact terrorist activity will evolve in the future.

[5]Activity that captures state-linked hostility conducted below the threshold of open state-on-state conflict (including using non-state proxies), intended to coerce, disrupt or erode a government's operational capacity.

[6]A measure of explosive power based on an equivalence to the net explosive quantity of TNT high explosive.

Contemporary RDS

A contemporary high-impact RDS might entail multiple explosives-laden drones, controlled individually or in a networked swarm[7], attacking high-value assets such as a data centre or network transformers at their most critical/vulnerable points. The resulting combined property damage and business interruption could cascade across multiple business lines, with losses potentially reaching hundreds of millions of pounds.

Even for attacks prioritising casualties over structural damage or business disruption, coordinated multi-drone attacks with explosives or incendiary devices on stadiums, festivals or other large-scale events, for example, could generate high property losses and significant business interruption (including future event cancellations) into the tens of millions.

Importantly, the potential for multiple simultaneous drone detonations calls for more nuanced analysis in modelling, as discussed further in Section 2. It could render both the currently used 250m-radius standard blast zone more limited in its applicability and the 2,000kg credible worst-case scenario obsolete, because for the adversary, there are less risky and more impactful approaches. Drones can be made covertly using individual customisation and/or additive manufacturing, thereby circumventing laws and reducing the likelihood of law enforcement apprehension. Advances in AI also mean that active control is not required and attacks can be reconnoitred and rehearsed.

Additionally, in light of these evolving threats, it has also become increasingly clear that conventional measures such as 100% PML may not adequately capture the highly concentrated damage near the point of attack, reinforcing the need for adaptive, location-sensitive modelling strategies.

However, while attacks involving simultaneous drone detonations are now possible, it should be noted that in Western countries, multiple robust mitigations are in place that should prevent the most extreme iterations of such attacks. For example, regulations on the purchase of certain explosives precursors or certain quantities of such materials exist in many countries.

[7] The largest swarm of drones acting in unison to date included 10,197 devices for a light show in the Chinese city of Shenzhen in 2024, demonstrating that the technology for massed, coordinated drone activity now exists.

Monitoring the Threat Landscape: From Reactive to Proactive

Simply presupposing that future events will mirror the past can be dangerous in an increasingly nonlinear world. As highlighted, threats are increasingly interconnected and mutually amplifying – from cyberattacks that cascade into physical infrastructure failures to climate events that exacerbate social unrest and political violence. For reinsurers, the challenge lies in identifying fundamental changes that could alter core modelling assumptions before significant losses materialise.

Establishing trigger thresholds

Readiness for future volatility requires systematic monitoring (horizon scanning) for weak signals or early indicators of change. These signals can be both qualitative and quantitative, and when they reach a defined threshold (to be determined internally), they should trigger a reassessment of risk models, underwriting assumptions and accumulation strategies.

By proactively tracking these types of indicators, reinsurers can anticipate shifts in the threat landscape, adjust risk models in advance and ensure that policies, limits and coverage structures remain aligned with emerging exposures.

Indicators could include:

QUANTITATIVE

- A sustained increase in state-linked threat investigations, espionage or proxy activity above historical baselines (e.g. a surge in UK counterterror investigations noted by MI5). While a lot of this information might be classified, the UK government has outlets such as the National Protective Security Authority who release unclassified information into the public domain.
- A measurable rise in the number of terrorist or politically motivated incidents employing novel methodologies (e.g. drone strikes, AI-assisted attack planning or additive manufacturing) within a defined timeframe.
- Critical infrastructure attacks with suspected or confirmed state or proxy involvement exceeding historical frequency or severity.

QUALITATIVE

- Confirmed deployment of advanced technologies (e.g. AI, drones or 3D-printed weapons) in operational planning and/or attacks.
- Evidence of new forms of state–non-state collaboration, including sponsorship of proxies, criminal networks or unaffiliated individuals to achieve strategic objectives abroad.
- Escalating societal tensions, polarisation or identity-driven grievances in a region, which could create flashpoints for civil unrest or politically motivated violence.
- New regulatory restrictions or relaxations on dual-use technologies, which may affect the availability or sophistication of tools used in attacks or prompt actors to adapt tactics in unexpected ways.

Note: Region-specific triggers could be added or refined as required to reflect local threat trends, social dynamics or geopolitical developments that may materially affect exposure in particular markets.

SECTION 2: Utilising the Models for Terror

Current Standardised Practices

The London market standardised method for terrorism risk assessment in reinsurance has long relied on a set of simplified assumptions focused around identifying, monitoring and managing exposure concentrations within a prescribed distance. The fully exposed limit is then assessed at this chosen radius, which is dependent on a client's risk appetite (typically a 250m radius). While this approach has served as a useful tool for benchmarking and assessing portfolios, the simplistic nature is now increasingly questioned considering today's evolving threat landscape (as described by Blackthorn), improved modelling capabilities and increasingly available data.

The 100% PML standard practice was largely developed in response to high-profile events such as the 9/11 attacks and incidents in London (7/7 bombings 2005) and Mumbai (2006). Regulatory requirements and market pressure drove reinsurers to define exposure limits quickly and conservatively. As a result, metrics such as 100% PML by distance and city accumulations became widely adopted.

This practice aims to answer the basic question: Where are the peak exposures across my portfolio? Which is used as a proxy to answer the real question: What would it cost if a significant event occurred? But the simplicity of this approach has its limitations.

The approach assumes a uniform maximum damage for all assets within a given radius. While this offers a conservative loss scenario (depending on the current threat landscape), it fails to capture crucial factors such as varying building vulnerability, differences in the cityscape or the spatial variation of damage intensity. The 100% PML approach also overlooks the probabilistic nature of terror events, where frequency and severity are highly uncertain and difficult to quantify.

Probabilistic models have long been a cornerstone in natural catastrophe risk assessment, but their role in

> "Total exposed risk can present an inaccurate view of potential loss, especially when key characteristics are ignored."

Terror modelling is limited. There are multiple probabilistic models available, but their accuracy and reliability are often questioned. One major challenge is estimating event frequency. Unlike natural disasters, terrorism is human driven with no predictable patterns or return periods.

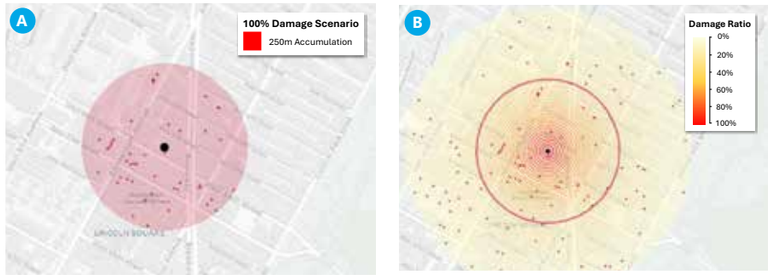
Whilst there is value in simplicity using the 100% PML approach, it is important to recognise the limitations. Total exposed risk can present an inaccurate view of potential loss, especially when key characteristics are ignored.

Evaluating portfolios against realistic scenarios is important for including factors such as coverage type, excess points and data quality. By highlighting how different assumptions, such as variations in bomb size, building height or construction type, affect the view of risk, greater context is given. This approach gives greater insight and deeper understanding to the extent of portfolio exposure and how these shift under more realistic scenarios.

Issues looking at exposed limits by radius

Accumulation analysis is typically conducted across a portfolio to identify high-exposure areas. Terror model vendors support this by allowing users to estimate exposure by applying financial layers across a predefined grid within a set radius (e.g. 250m).

The standardised 100% PML approach overlooks critical factors such as building vulnerability – treating all structures equally, regardless of their resilience (e.g. steel



C

Location ID	Sum Insured	Damage Ratio		Ground Up Loss	
		250 Meter Accumulation	Bomb Blast Scenario	250 Meter Accumulation	Bomb Blast Scenario
153701	39,839,322	100%	5%	39,839,322	1,991,966
66220	24,239,936	100%	50%	24,239,936	12,119,968
14150	1,776,812	100%	25%	1,776,812	444,203
75447	33,638,235	0%	40%	-	13,455,294
10835	74,503,536	0%	0.01%	-	3,725
23615	20,743,351	0%	60%	-	12,446,010
4708	36,947,751	100%	0.10%	36,947,751	36,948
5643	1,000,000	100%	0.10%	1,000,000	100,000
			TOTAL	103,803,822	40,598,115

Figure 1:
A. 250m 100% PML example in New York. Zone designated by an accumulation analysis which aims to find the peak areas of exposure at a set distance. Uniform 100% damage across the red area.

B. A hypothetical bomb blast - point of detonation set to the same coordinate as the 100% 250m PML. Distance of damage is further than the 250m but the damage ratio decreases exponentially as the stand off distance increase.

C. Locations affected for each scenario for the same coordinate along with the estimated mean loss. Damage ratios are overall much lower on average compared to the 250m accumulation. But more locations are effected due to the larger, but less severe damage rings.

high-rises vs. masonry low-rises). In dense urban areas, this can distort risk estimates. Moreover, blast wave behaviour varies with city layout; high-rise buildings can shield or channel pressure differently. As such, a fixed-radius approach may not suit all cities. New York's density, for example, differs significantly from London's.

Treating all coverages as being fully exhausted is also problematic and could overestimate or underestimate the loss depending on the portfolio. Content loss would typically start once a certain building damage threshold is exceeded, while business interruption is likely to occur farther out than the point of detonation. The makeup of a portfolio will impact the effect this could have on eventual loss.

Full exhaustion also masks any effect of attachment points. Two policies with a $100m limit, but with different excess points of $50m and $200m, produce the same exposed risk using the 100% PML approach. The latter policy would be less likely to incur a loss, particularly if the asset is located on the edge of the accumulation zone.

Lastly, using a uniform 250m blast zone globally for terrorism accumulation modelling ignores the real-world variability in threat levels across regions. The 250m radius was initially derived from a 2-tonne bomb which, in the context of the current threat landscape, may not be appropriate and will differ by country, city and state.

Using deterministic scenarios alongside the 100% PML analysis offers deeper insight and accounts for additional risk factors. Sensitivity analysis around data quality and attachment points can further increase understanding. As seen in Figure 1, the loss distribution for a 2-tonne bomb scenario is dramatically lower than the 250m 100% PML option. Factors such as location spread and more robust building codes could explain this mismatch.

Utilising the model what-if scenarios

The vendor models have developed a set of deterministic attack scenarios aimed at recreating 'what if' situations across a portfolio. Damage is prescribed as a set of concentric circles emanating from a blast centroid, with damage declining sharply with distance depending on bomb size. These damage ratios are based on a combination of real-world events, engineering studies and computational fluid dynamics (CFD) model outputs.

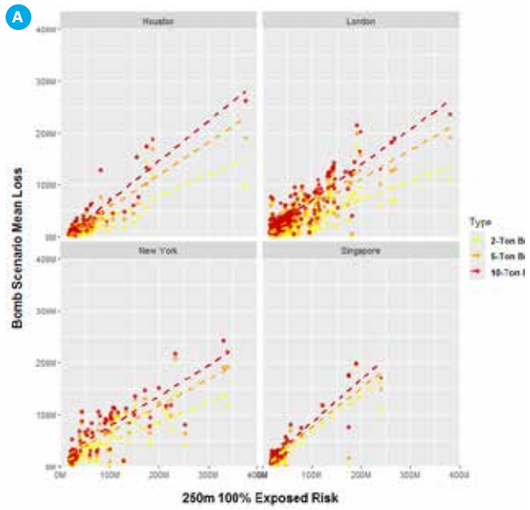
To demonstrate the difference between the traditional 250m accumulation analysis and realistic scenarios, peak exposure can be identified using the standardised 100% PML analysis, and the various terror scenarios can be run at the centroid locations. Figure 2 shows that for this specific portfolio, the total exposed risk is rarely higher than the deterministic events.

A 10-tonne bomb is often used as a worst-case deterministic scenario and is considered inconceivable, particularly in Western countries. Assembling, transporting and delivering such a bomb undetected is exceptionally difficult given modern surveillance, border controls and intelligence. The 10-tonne bomb can be used as a stress-test accumulation but is seen to be overly conservative. The more realistic 2-tonne bomb, which has some historical analogues (Beirut 1983 and Oklahoma City 1995), typically models much lower than the 250m exposed risk for this portfolio, although this can differ by city and data quality. As seen from the graph, the bomb scenarios for the largest 100% PML accumulations do not exceed the potential loss, suggesting that the 100% PML analysis is overestimating potential loss.

Building characteristics

While deterministic scenarios may affect more locations, since medium to large bombs impact areas beyond 250m, damage decreases exponentially with distance from the blast. For portfolios with low location concentration, mean losses are typically lower than the exposed risk. As noted, models incorporate limited building characteristics, which influence damage and loss. High-quality, complete data improves the accuracy of terror scenario estimates. However, large terror portfolios often suffer from poor data quality due to reliance on standard accumulation metrics that overlook key factors.

A



B

City	100% 250 meter	Aircraft Impact	1 Tonne Bomb	2 Tonne Bomb	5 Tonne Bomb	10 Tonne Bomb
Houston	375,890,101	135,263,867	118,335,257	154,302,969	190,339,536	262,024,856
London	381,906,181	138,696,852	142,702,765	171,675,597	199,070,345	236,298,619
Singapore	240,216,459	195,467,829	194,398,757	195,615,984	196,448,102	197,588,950
New York	338,616,261	195,830,608	136,590,766	140,033,097	207,101,250	241,858,528
Max Loss	381,906,181	195,830,608	194,398,757	195,615,984	207,101,250	262,024,856

Figure 2:
A. Compares top 250m 100% PML scenarios with varying deterministic model scenarios at the same centroid. The white dotted line indicates perfect correlation—points above show higher deterministic losses; below, lower.
B. Displays top city accumulations by bomb scenario and the overall maximum across cities.

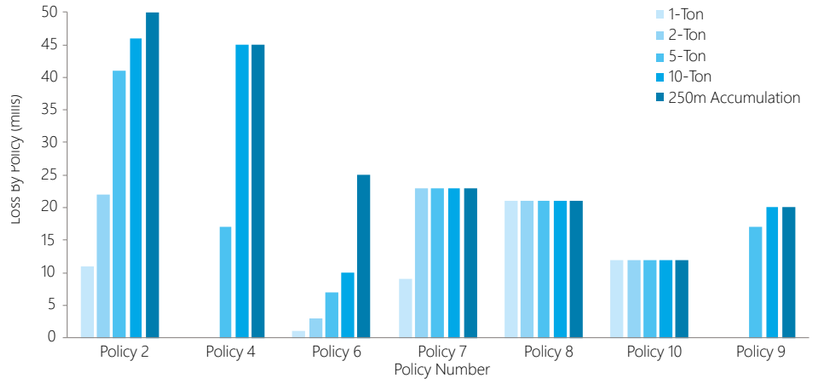


Figure 3: potential loss to each policy for the top 250m 100% PML and vendor model deterministic events. Policies with higher attachment points begin to take loss once the threshold is exceeded and caps at the limits. As severity decreases, some policies may receive no loss as this attachment point is not exceeded (see policy 4).

To compensate, models apply broad assumptions based on regional economic data when building details are missing. Though not ideal, these assumptions reflect regional construction standards where possible.

Assumptions on blast wave behaviour, accounting for building density and shielding effects, have been developed for select US cities. Though simplified compared to full CFD models, they offer useful approximations. More realistic damage estimates rather than flat 100% factors enable better assessment of attachment points. Locations with high attachment points at medium distances may not significantly impact loss, even within 250m. The bomb size used in modelling can vary based on risk appetite and region.

Attachment points

This approach adds insight by illustrating how losses shift with changes to attachment points, revealing portfolio sensitivity in high-risk areas. Stricter underwriting, such as higher attachment points in key urban postcodes, can be tested and benchmarked against peers by aligning layers or converting primary to excess, helping quantify the impact of higher limits across bomb scenarios.

As shown in Figure 3, deterministic scenarios help identify loss-driving policies that often differ from those highlighted in a 100% PML view. In realistic attacks, centrally located risks dominate, whereas the 100% PML approach captures high-value assets within a broad radius. Recognising this difference is crucial for reinsurers assessing true exposure and maximum limits.

> "Failing to identify which policies drive losses across multiple deterministic terrorism scenarios across a portfolio can have significant consequences for buyers."

Failing to identify which policies drive losses across multiple deterministic terrorism scenarios across a portfolio can have significant consequences for buyers. Without this insight, companies risk purchasing facultative reinsurance for policies that contribute little to actual losses, while neglecting coverage for those that are truly vulnerable. Similarly, setting attachment points without a clear understanding of how losses distribute across scenarios may lead to layers being either underutilised or frequently breached, resulting in unexpected volatility and net losses. Overlooking scenario loss drivers impairs effective aggregation management, particularly in high-risk urban zones where clustering of exposures can magnify losses.

Future Work and the Importance of Data Quality

Capturing the hazard

There has been a recent push in the market to assess the impact of a realistic Terror event in a more detailed way, with outputs from CFD models often referenced. CFDs can provide detailed blast footprint estimates, accounting for the building scape and surrounding topography. These simulations are computationally intensive and time-consuming, often taking hours for a single run. This makes CFD impractical for the large portfolios typical in reinsurance, where identifying peak concentration and accumulation risk quickly across an entire portfolio is critical. While there is promising work in applying AI to generate CFD-like blast footprints rapidly, these techniques remain in the preliminary stages. The data requirements needed to achieve this level of granularity are also lacking.

Data issues – geocoding

Data quality remains a key challenge in terrorism risk modelling. Inaccuracies in geocoding, incomplete building details and limited exposure data can significantly reduce model accuracy, especially given the highly localised nature of blasts, where a few meters can change damage severity. Even street-level geocoding can cause major positional errors (Figure 4, left). As models become more detailed (e.g. CFD), building data is needed not just for insured assets but for all nearby structures, as this influences damage (Figure 4, right).

To improve model reliability ahead of adopting advanced tools such as CFD or AI-based simulations, two data priorities must be addressed: geocoding accuracy and building attribute completeness. Precise building-level geocoding is essential, as small errors can shift properties between high and low damage zones. Improving geocoding is also more cost-effective and impactful than relying on complex loss scenarios, which remain highly sensitive to location and blast proximity. Geocoding accuracy can be enhanced by implementing higher data collection standards at the source, leveraging region-specific geocoding services that specialise in accurate building-level placement and conducting manual validation in areas of high risk or exposure. These portfolios are often large, but focusing on areas of high risk or exposure can be beneficial at a low cost.

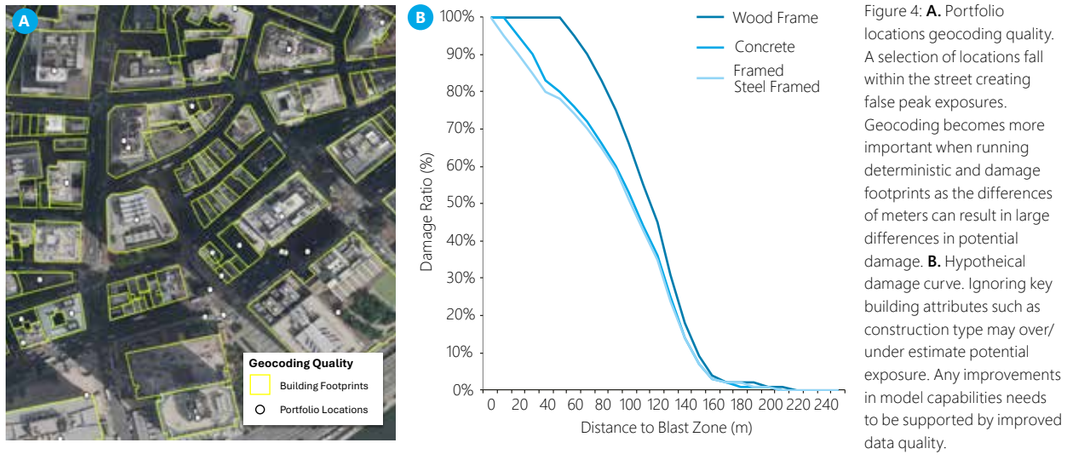


Figure 4: **A.** Portfolio locations geocoding quality. A selection of locations fall within the street creating false peak exposures. Geocoding becomes more important when running deterministic and damage footprints as the differences of meters can result in large differences in potential damage. **B.** Hypotheical damage curve. Ignoring key building attributes such as construction type may over/under estimate potential exposure. Any improvements in model capabilities needs to be supported by improved data quality.

Data issues – building characteristics

Improving building attribute data is equally essential. Current models often rely on broad assumptions due to missing details such as construction type, occupancy and number of stories. For future CFD analysis, it's not enough to know only the insured structures; every building within the blast zone must be included in a detailed 3D urban model to accurately capture shielding and blast dynamics.

Addressing internal data quality is the most effective first step. Investing in complete, high-quality exposure data with accurate geocoding and building-level details not only enables advanced modelling but also brings immediate benefits: more realistic loss estimates, better reinsurance efficiency, improved aggregation management and clearer differentiation of terrorism risk across portfolios. Data quality improvements can be achieved by requesting more information from the insureds and maintaining this data or using third-party datasets to enrich building characteristics. Again, focusing on areas of high risk or exposure will provide the greatest returns on accuracy at the lowest cost.

Emerging Realistic Disaster Scenarios

The current Terror models have focused on historical attack patterns such as vehicle-borne conventional explosives and aircraft explosions. However, the threat landscape is continually shifting and Blackthorn laid out new and emerging technologies, particularly drones, AI and unmanned systems, which are introducing novel attack scenarios that current models have not yet incorporated into their framework. Modern threat actors can exploit commercially available drones for targeted attacks, enabling remote, mobile and low-cost operations that bypass traditional security barriers. These attacks can be highly localised and targeted, with attackers able to select specific points of vulnerability – such as fuel tanks, structural joints or ventilation systems – to maximise impact from a minimal payload. As a result, smaller explosive quantities could potentially generate disproportionately large damage, especially when critical or fragile components are targeted.

Beyond single drone strikes, there is a threat of swarm attacks, where multiple drones operate in coordination. This presents a complex challenge with specific event definitions required to cater to very different loss patterns. These scenarios could overwhelm security systems, deliver simultaneous hits across various locations or create cascading failures in critical infrastructure. This type of attack mode defies the logic of traditional modelling approaches and demands a framework that accounts for movement, precision targeting, sequencing and potentially multiperil outcomes.

Models need to incorporate these new threats, and pressure from the market will promote future model development proactively, rather than retrospectively. In the meantime, measuring combined accumulation zones across a major urban area can act as a proxy for a swarm drone attack. Certain coverages, especially Business Interruption (BI), Contingent BI and Cyber may be far more severely impacted. For example, a drone attack on a data centre could result in minimal physical damage but trigger extensive BI losses due to service outages, downtime and knock-on effects across dependent systems and infrastructure. This evolving threat highlights the importance of revisiting sub limits and coverage definitions. As drone capabilities evolve, so must the insurance industry's approach to aggregation, risk modelling and coverage design. Assessing fully exposed coverage limits for each policy which falls in a blast zone could help assess this.

Recommendations

Ongoing trends in the evolution of the threat landscape show no sign of abating. Strategic competition is intensifying rather than stabilising, technological development continues at a rapid pace, political polarisation appears to be deepening and climate pressures are mounting. The convergence of these factors suggests that volatility is not a temporary condition to be weathered but a fundamental characteristic of the contemporary operating environment. For the reinsurance industry, this reality necessitates continuous monitoring of threat developments and proactive analysis of how these various factors might intersect to create new risk scenarios. The capacity to think ahead about emerging threats and their potential convergence is no longer a competitive advantage but an operational necessity for sustainable risk management in this age of volatility.

Deterministic Terror models, which simulate realistic 'what-if' bombing scenarios based on blast radius and damage gradients, offer a more accurate and nuanced view of portfolio risk compared to a traditional 100% PML approach. Ultimately, leveraging deterministic scenarios helps secure better-informed terrorism reinsurance strategies by aligning them more closely with realistic risk profiles.

Modelling capabilities need advancement, and to take advantage of future development, investment in data quality now will enable quicker adoption, resulting in more accurate loss estimates. Methods to assess new threats are also needed, fundamental methodology of the models has not changed drastically in recent years, and pressures from the market could promote future development to help pinpoint potential unexpected losses in a volatile, unpredictable WTPV space.

Lockton Re

Lockton Re, the global reinsurance business of Lockton Companies, helps businesses understand, mitigate, and capitalize on risk. With over 500 colleagues in 23 locations globally, the business is continuing to grow, pushing the reinsurance industry forward with smarter solutions that leverage new technologies—delivered by people empowered to do what's right for clients.

Lockton Re's reports, market commentary and insights focus on key topics, occurrences, or changes in the (re)insurance and broking market place that impact our clients and partners. In order to help guide relevance for the reader, we categorize this content into four areas—Exposures, Perils, Risk Transfer, and Placement.

Blackthorn

Blackthorn is a London-based advisory practice specialising in malicious risk, combining technical expertise in terrorism, political violence, civil unrest, and kidnap with strategic analysis of state and non-state threats.

We operate globally, supported by an extensive network and deep experience across diverse operating environments and industries, including critical infrastructure, extractives, construction, hospitality, and family offices. Our capability is further strengthened by specialist expertise in assessing and managing high-consequence risks associated with chemical, biological, radiological, nuclear, and explosive (CBRNE) materials.

With professional backgrounds spanning intelligence, law enforcement, the military, the United Nations, and civil defence, our team provides strategic resilience advisory, business continuity, security risk management, emergency preparedness, and crisis management services.

Authors and Contacts

Blackthorn.

LOCKTON REINSURANCE

AUTHORS

Niki Whitley
Director, Advisory
niki.whitley@blackthornrisk.com

Alex Theodosiou
Manager, Advisory
alex.theodosiou@blackthornrisk.com

AUTHOR

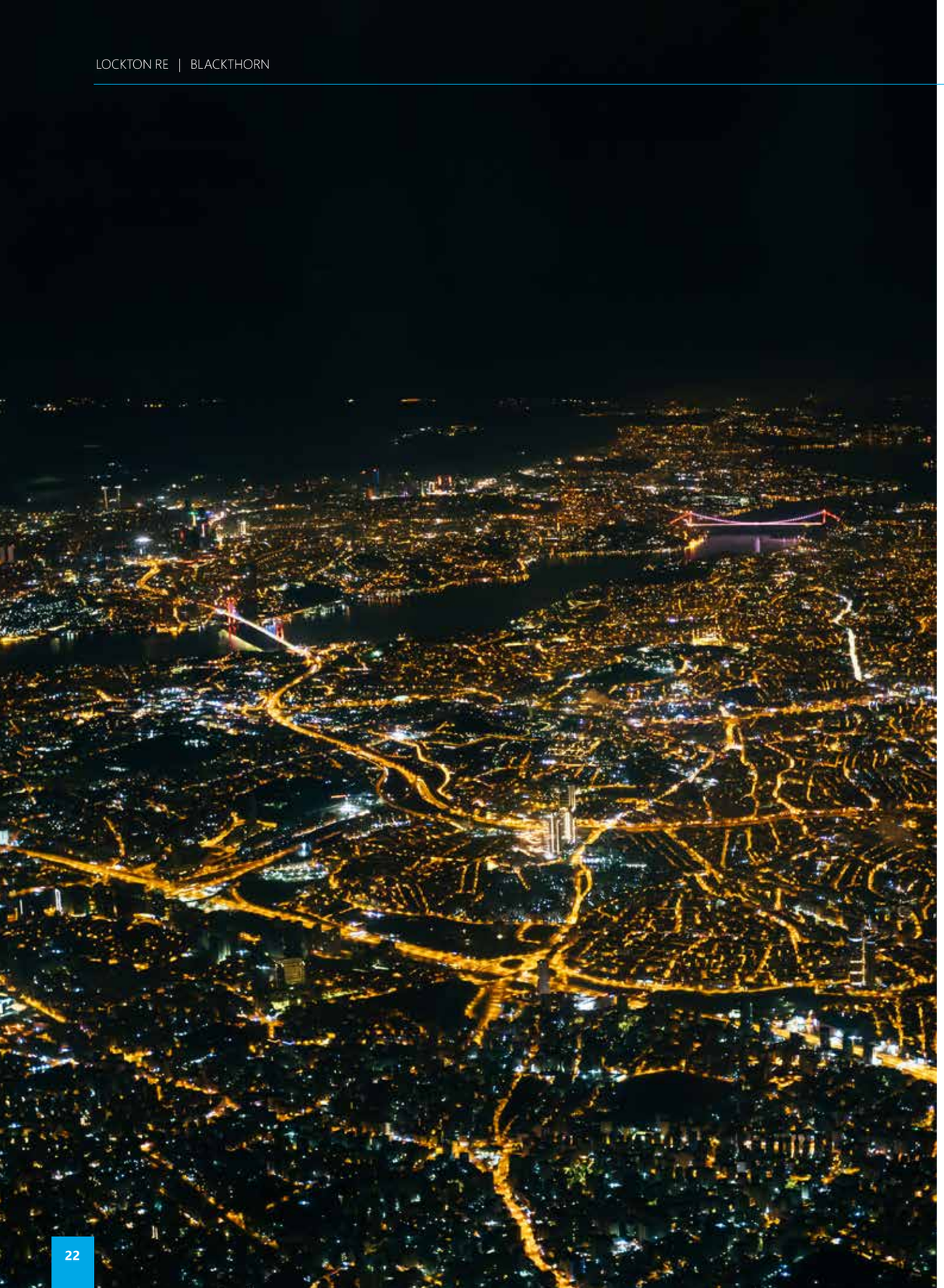
Paul Upton
Chairman Specialty
paul.upton@lockton.com

George Wragg
Senior Cat modeller
george.wragg@lockton.com

CONTACTS

Isabella Gaster
Lockton Re Global Head of Marketing
+44 (0)7795 400981
isabella.gaster@lockton.com

Elizabeth Miller Kroh
Lockton Re Head of Marketing, North America
+1 (445) 248 2228
elizabeth.kroh@lockton.com



Footnotes

[1] States that seek to fundamentally alter the prevailing international order.

[2] Additive manufacturing ('3D-printing') is a dual-use technology that enables rapid prototyping and customisation while allowing weapons or components to be produced outside regulated supply chains. While predominantly utilised to fabricate firearms, it is also increasingly being used to customise UAVs, a development that could enable more sophisticated, high-profile drone attacks with greater loss potential.

[3] For terrorist purposes, this might include automated attack planning (including facilitating the design of biological or chemical weapons), enhanced hostile reconnaissance and the generation and dissemination of propaganda or misinformation (potentially amplifying wider civil unrest).

[4] A strategy that blends conventional military force with nonmilitary tactics such as cyberattacks, disinformation, economic pressure and proxy forces to weaken an opponent while avoiding open war.

[5] Activity that captures state-linked hostility conducted below the threshold of open state-on-state conflict (including using non-state proxies), intended to coerce, disrupt or erode a government's operational capacity.

[6] A measure of explosive power based on an equivalence to the net explosive quantity of TNT high explosive.

[7] The largest swarm of drones acting in unison to date included 10,197 devices for a light show in the Chinese city of Shenzhen in 2024, demonstrating that the technology for massed, coordinated drone activity now exists.

www.blackthorn.com

Blackthorn.

1-3 Leadenhall Market, London EC3V 1LR

Blackthorn, Blackthorn Risk, Blackthorn Advisory, and Blackthorn Insurance Brokers are trading names of CHC Insurance Services Limited which is a company authorised and regulated by the Financial Conduct Authority under firm reference number 995548 to carry on insurance distribution activities. CHC Insurance Services Limited is registered in England and Wales under company number 10942687. Not all activities are related to Lloyd's.

Blackthorn specifically disclaims any express or implied warranty, including but not limited to implied warranties of satisfactory quality or fitness for a particular purpose, with regard to the content of this publication. Blackthorn shall not be liable for any loss or damage (whether direct, indirect, special, incidental, consequential or otherwise) arising from or related to any use of the contents of this publication.

LOCKTON REINSURANCE

www.locktonre.com

261 Fifth Avenue, New York • NY 10016

The St. Botolph Building, 138 Houndsditch • London EC3A 7AG

Lockton Re is a trading name and logo of various Lockton reinsurance broking entities and divisions globally and any services provided to clients by Lockton Re may be through one or more of Lockton's regulated businesses.

Our regulated entities are: Lockton Re, LLC in the USA, Lockton Re, LLC, 261 Fifth Avenue, 10th Floor, New York, NY 10016, in California, Lockton Re Intermediary Insurance Services, LLC (License number 0G76373); Lockton Re LLP in the UK Registered in England & Wales at The St. Botolph Building, 138 Houndsditch, London, EC3A 7AG. Company number OC428915 and authorized and regulated by the Financial Conduct Authority with FRN 921278; Lockton Re (Bermuda) Limited in Bermuda (Registration number 56292) Seon Place, 141 Front Street, Hamilton HM19, Bermuda; Lockton Re (Germany) GmbH, Ludwigpalais, Ludwigstraße 8, 80539, Munich, registered with the Commercial Register of the Munich Local Court under HRB 275178, authorized as an insurance broker pursuant to Section 34d para. 1 GewO and regulated by the Chamber of Commerce (IHK), Munich and Upper Bavaria with Company Registration Number: D-I5DQ-33IIL-38; and Lockton Re is a trading name of Lockton (MENA) Limited. Lockton (MENA) Limited is registered in the Dubai International Financial Centre (DIFC), GD 6, DIFC PO Box 506794 Dubai, UAE commercial license number 0970, and is regulated by the DFSA, the independent financial services regulator for the DIFC; Lockton Re LAC Series of Lockton Specialties, LLC, (Latin America & Caribbean) registered under license number 8331631 in the Missouri Department of Commerce and Insurance and under license number W697048 in the Florida Department of Financial Services, with its business address at 1221 Brickell Avenue, Suite 1500, Miami, FL 33131, USA; Lockton Re Brasil Corretora de Resseguros Ltda., (Brazil) registered under permit number 7,610 at SUSEP - Superintendência de Seguros Privados, with its business address at Avenida das Nações Unidas, 14171, cj. 1401, São Paulo, SP, Brazil; Lockton Chile Corredores de Reaseguros SPA., (Chile) registered under license number C-282 at CMF - Comisión para el Mercado Financiero, with its business address at 90 Orinoco, office 2001-A, Las Condes, Santiago, RM, Chile; Lockton México Intermediario de Reaseguro, S.A. de C.V., (Mexico) authorized by Comisión Nacional de Seguros y Fianzas, with its business address at Av. Santa Fe 481, Piso 20, Colonia Cruz Manca, Cuajimalpa. C.P. 05349, Mexico; Lockton Corredores de Reaseguros Ltda., (Colombia) registered under Resolution number 1801 at Superintendencia Financiera de Colombia, with its business address at Carrera 11 No 86 - 60, Bogotá D.C., Cundinamarca, Colombia.

Lockton Re provides this publication for general informational purposes only. This publication and any recommendations, analysis, or advice provided by Lockton Re are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. It is intended only to highlight general issues that may be of interest in relation to the subject matter and does not necessarily deal with every important topic nor cover every aspect of the topics with which it deals. The information and opinions contained in this publication may change without notice at any time. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Lockton Re shall have no obligation to update this publication and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as reinsurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your applicable professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the information contained herein could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. This publication is not an offer to sell, or a solicitation of any offer to buy any financial instrument or reinsurance product. If you intend to take any action or make any decision on the basis of the content of this publication, you should seek specific professional advice and verify its content.

Lockton Re specifically disclaims any express or implied warranty, including but not limited to implied warranties of satisfactory quality or fitness for a particular purpose, with regard to the content of this publication. Lockton Re shall not be liable for any loss or damage (whether direct, indirect, special, incidental, consequential or otherwise) arising from or related to any use of the contents of this publication.

#0875_10.25