# 14

# Quantitative Man-Made Risks' Modelling

Gordon Woo

## 14.1 Man-Made Risks

The most accurate, reliable and reproducible quantitative predictions of the future are based on the laws of physics. System complexity and chaotic dynamics erode the accuracy of prediction. Nevertheless, all natural hazards are subject to the fundamental laws of physics, which constitute an objective scientific basis for natural catastrophe risk modelling, and hence the pricing of natural catastrophe bonds. Investors in flood risk can be assured that water will not run uphill; investors in weather risk know that offshore hurricane wind strength increases with sea surface temperature, and so on.

Natural catastrophe bonds constitute a very special asset class in that the default risk is tied to phenomena which are essentially outside human influence: human beings cannot induce tectonic earthquakes or cause hurricanes. As a consequence, natural catastrophe bonds are essentially uncorrelated with other financial assets: a stock market collapse does not affect the chance of an earthquake occurring in California. A freak exception to the immunity of natural catastrophe bonds against volatility in the financial markets arose following the sudden collapse of Lehman Brothers during the financial crash of 2007. This introduced an anomalous man-made component to the default risk of this asset class; bond principal is required to be held safe in riskless securities. This presumption turned out surprisingly to have exceptions.

G. Woo (✉)
Risk Management Solutions (RMS), London, UK

M. Pompella, N.A. Scordis (eds.), *The Palgrave Handbook of Unconventional Risk Transfer*, DOI 10.1007/978-3-319-59297-8_14

Economics has been called the dismal science, because economic forecasts are inherently ambiguous and lack the forecasting capability of the natural sciences. Precise mathematical predictions can be made under strict hypotheses such as assuming that markets are operated by rational human agents. However, the practical limitations of this assumption are commonplace, as witnessed by the rise of behavioural economics, and the growing impact of social psychology in economic decision-making.

Mortgage-backed securities were notoriously and disastrously mispriced in the years leading up to the great property crash of 2008; a financial disaster endogenously driven by market fear and greed. Exogenous hazards might also have caused these securities to fail. All property-related bonds include an implicit exposure to both terrorism and political risk. Mortgage-backed securities have always been at risk from a terrorist attack using a weapon of mass destruction. However, this risk was traditionally excluded as a factor in the rating of such securities; terrorism risk was deemed to be excessively ambiguous due to the vagaries of human behaviour.

Well into the post-crash recovery period, international property investment bonds were being offered in 2016 by a Singapore-based fund to retail investors paying as much as 10% per year over four years, with capital at risk. These bonds are asset-backed by tourist hotels and luxury apartments in different countries, but the value of the underlying property assets may decline for a variety of reasons. Occupancy of tourist hotels, for example, may fall off sharply if resorts are prone to terrorist attack. This has been the fate of tourist hotels in Tunisia and Turkey, and also France, where hotel occupancy rates were down by 8.5% after the 13 November 2015 Paris terrorist attacks. Furthermore, there may be overcapacity in the luxury apartment market and unfavourable changes in the local regulatory and fiscal regime concerning apartment developments. Sudden unexpected political changes can also affect property bonds. After the surprising UK Brexit vote in July 2016, the Singapore government warned of investment in UK property bonds.

Quantification of the risk of default of the above illustrative property bond is hard to estimate. Indeed, the issuer of such a bond typically makes no attempt to assess the risk. Legally, it is sufficient to warn potential investors that their capital is at risk. But just how much is at risk is generally unknown either to the issuer or the investor. The same applies for corporate bonds, which depend on the profitability of individual corporations. In the modern world, where destructive business change is more common than ever due to new technology, such as the advance of online commerce and robotics, the very existence and survival of a corporation may be questionable, let alone its profitability. As the unemployment in the rustbelt shows, long proven track record of corporate success is no guarantee of future survival.

ILS bonds are a special noteworthy asset class for bond investors because of the substantial effort made on behalf of the issuer to quantify the risk of default, whether caused by a natural or man-made peril. Extensive scrutiny of default risk analysis by intermediaries and rating agencies provides robust peer review. Epistemic uncertainty in the expected loss to ILS bonds is analysed and is factored into the pricing of such bonds. The spread of coupon to expected loss is typically higher for new types of ILS bonds, and those with a more complex structure. Innovation incurs a cost that issuers need to bear in mind in structuring a new ILS involving an exotic natural hazard, or a man-made hazard. However, as the market becomes more familiar with a hazard over time, the spread falls.

The coupon ultimately depends on ILS supply and demand. Aggressive lowering of a coupon may result in a cliff-edge drop in market enthusiasm for an issue. Investment grade bonds are especially attractive because of the larger community of investors licensed to buy such bonds. Rating agencies play an important role in stress-testing the risk analyses undertaken for ILS bonds.

All risks associated with natural hazards have a societal context. For example, coastal flood risk depends on the decisions made on strengthening sea defences. But the primary causes of geological, meteorological and hydrological hazards are external to human society. Progress in the scientific understanding of natural hazards, and engineering knowledge of building vulnerability, has facilitated their quantitative risk modelling.

There are other significant risks to society that have an origin internal to human society. These endogenous man-made risks include terrorism, cyber crime and other forms of political violence. Industrial and transport accidents should also be included.

The primary agents of man-made perils are human beings rather than the inanimate forces of Nature. Other hazards such as the spread of pandemic disease have an important human dimension, including a nexus with political conflict. The quantitative modelling of man-made risks is addressed in this chapter.

### 14.1.1 Principles of Terrorism Risk Modelling

Irrespective of the cause, where there are abundant data, especially Big Data, statistical methods of predictive analytics exist to model the associated risk. Thus, motor accidents are man-made (even for autonomously driven vehicles), and sufficient claims data exist to segment the motor risk by driver and vehicle, and model the risk in fine detail. However, where data are sparse, for both natural and man-made hazards, statistical methods lose power and predictability, even extreme-value methods based on extrapolating the tails of distributions.

All quantitative modelling of rare events should be based on principles. Event data are too sparse for statistical analysis to suffice alone. The principles should be rooted in empirical experience but transcend the finite boundaries of observation. Two universal characteristics of human behaviour that contribute significantly to the generation of man-made risks are malicious action and human error. Malevolence and benevolence are opposite sides of individual character. Here we are concerned with the negative aspects of human behaviour, leading to terrorism and political violence. The adversarial nature of terrorism and political violence is captured within the methodology of game theory, which addresses the strategic interactions between opposing groups. The behavioural aspects of these interactions are accounted for in behavioural game theory (Camerer 2003).

To accommodate the strategic aspects of terrorism, structured stochastic simulation methods are required. These can be based on the well-established methods and principles of theoretical physics, which represent the gold standard for accurate quantitative modelling. All natural hazards are a product of the Earth's environment, which is governed by the Laws of Physics. A core principle that explains the natural world is the principle of least action: *Nature acts always according to the simplest paths*. Discovered by the French savant, Pierre de Maupertuis in 1746, this universal optimality principle epitomizes the elegant simplicity of scientific theory, and the parsimony of the best mathematical modelling: the principle can be expressed in just a single succinct equation.

A few decades after this discovery, a French translation was made of a masterwork of military strategy: *The Art of War*. Written about 2500 years ago by Sun Tzu (McNeilly 2001), this essential strategic handbook for generals and statesmen embodies key principles that can guide the quantitative modelling of man-made risks. Indeed, many of the principles can be expressed in mathematical form.

A counterpart of the principle of least action in Nature is that attackers in human conflict follow the path of least resistance. Thus, Sun Tzu notes: *Now an army may be likened to water, for just as water avoids heights and hastens to the lowlands, so an army avoids strength and strikes weakness*. For attacks by terrorists, cyber hackers or warring states, quantitative risk modelling is unified by the principles of adversarial conflict, such as those laid out by Sun Tzu.

The well-defined principles underlying quantitative terrorism risk modelling minimize the need to resort to expert judgement (Woo 2011, 2015). Within the bounds defined by the Western counter-terrorism environment, terrorists maximize their operational utility by abiding by the classic principles of terrorist modus operandi: substituting hardened targets; following the path of least resistance in weapon selection; and leveraging their scarce resources to achieve the greatest impact. The metric for impact includes not just loss inflicted but also the media attention gained. An insightful ISIS slogan is that media is half Jihad. Media coverage is essential for terrorist recruitment and funding, as well as for propaganda. This is so important that in 2002, Osama bin Laden wrote that the media war may reach 90% of the preparation for battles (Awan 2016).

## 14.1.2 Target Substitution

*Following the path of least resistance* is a principle that governs terrorist behaviour and explains much of terrorist modus operandi, including targeting. A key characteristic of terrorist targeting is target substitution. Given two targets of similar terrorist attractiveness or utility, the target with inferior security is likely to be attacked. This applies on all spatial scales, from country to city to district, street and individual level. Apart from being a logical consequence of learning from the master strategist Sun Tzu, there are numerous examples to cite as evidence. Here is an example of individual target substitution.

The assassination of Theo van Gogh on the streets of Amsterdam on 2 November 2004 is a clear illustrative terrorist paradigm. As a film director, he had made a film about a Muslim apostate, Ayaan Hirsi Ali, who was under police protection. Theo van Gogh disdained any such protection and was stabbed to death when cycling in Amsterdam by a Moroccan-Dutch Jihadi, Mohammed Bouyeri. Impaled in van Gogh's chest was a knife, attached to which was a message: "There shall be no mercy for the unjust, only the sword raised at them". This was addressed not to him, but to the apostate. This is how we know this was target substitution.

A corollary of target substitution is that, unlike with natural hazards, the likelihood of any target being attacked cannot be assigned independently of other potential targets. This is the law of the jungle: in a herd of gazelles, the chance that any one will fall as prey to a lion depends on the number of vulnerable gazelles. In earthquake engineering, the strengthening of a building does not affect the likelihood of it experiencing strong ground shaking. But increasing the security around a building does reduce the likelihood of it being subject to a terrorist attack.

### 14.1.3 Terrorist Weaponry

Another aspect of modus operandi in which terrorists follow the path of least resistance is in their choice of weaponry. Given two weapons of similar effectiveness and reliability, the weapon that is easiest and least expensive in resources to procure is likely to be used. Off-the-shelf military weapons are therefore popular: AK-47s, mortars, surface-to-air missiles and so on. Improvised explosive devices are a mainstay of the terrorist arsenal, as are vehicle bombs, referred to as the terrorists' air force because of their damage capability.

The pragmatic opportunist terrorist approach to choice of weapon was expressed by the radical imam, Abu Hamza, in his injunction: "You can't do it by nuclear weapon, you do it by the kitchen knife, no other solution. You cannot do it by chemical weapons, you have to do it by mice poison". It is extremely difficult for terrorists to procure weapons of mass destruction. Technically, they are complex to manufacture in a reliable and secure way, and buying them on the black market runs the risk of all illicit markets: the problem of lemons. The quality of merchandise is highly uncertain and unreliable, and cannot be gauged by the seller's reputation. There are no guarantees of operability. Furthermore, the black market is flooded with offers from secret agents of the world's intelligence services.

Apart from being laden with explosives, vehicles can be used directly and opportunistically as weapons by being driven into groups of pedestrians. Chemical energy is substituted by kinetic energy. This type of attack has been used in Jerusalem as a protest against Palestinian occupation. An especially large attack of this kind occurred on 14 July 2016, when a Tunisian, Mohammed Bouhlel, drove a 19-ton refrigerated truck into Bastille Day crowds along the Promenade des Anglais in Nice. Eighty-six people were killed and more than 300 injured. Another Tunisian, 24 year-old Anis Amri, killed 12 people and injured 48 others when he rammed a 40-ton truck into a Christmas market in Berlin on 19 December 2016.

### 14.1.4 Severity of Weapon Attack Modes

A major concern of terrorism risk assessment is the severity of attack using a specific weapon mode. Insurance accumulation risk in an urban area may be gauged from a loss analysis using a five-ton bomb scenario. But how likely is such a weapon mode? Attack severity is constrained by the logistical burden of acquiring the skilled personnel, material, testing facilities and financial resources required for a weapon attack mode: the bigger and more ambitious the weapon, the greater is the logistical burden. Most importantly in a hostile counter-terrorism environment, attack severity is limited by the persistent and pervasive threat of arrest and plot disruption. Once a weapon of a particular size has been developed, an expedient terrorist choice would be to deploy it without delay. Alternatively, a riskier decision may be made to continue to develop a larger more potent weapon, which would pose a greater logistical challenge and would require extra material and financial resources, more time and more operatives. Accordingly, for the operatives involved, it would carry an increasingly higher likelihood of arrest.

Consider the principal attack modes which scale upwards in respect of potential weapon size. These are vehicle bombs, and CBRN weapons. Suppose that the weapon sizes are labelled as small, medium, large and very large. For vehicle bombs, these would be 0.5, 1, 2 and 5 ton. In an oppressive counter-terrorism environment, it is hard and perhaps foolhardy for a terrorist organization to skip weapon sizes because the extra development and testing time for a new superior weapon would present an excessive risk of interdiction or malfunction. Lack of adequate time in weapon development and testing is a major source of human error in terrorist operations.

To illustrate the principle of progressive weapon enhancement during a prolonged terrorist campaign, waged under sustained Western alliance counter-terrorism pressure, the best example is the decades-long IRA terrorist campaign in the UK. According to Stella Rimington, director-general of MI5, 80% of IRA plots were interdicted.

On 20 March 1972, a 100-lb gelignite car bomb exploded in Belfast. In the same year, the first IRA Ammonium Nitrate-Fuel Oil (ANFO) car bomb was developed. On 17 April 1979, a 1000-lb bomb was detonated in County Armagh, Ulster; the largest IRA vehicle bomb up to that time. On 17 January 1992, a van bomb of size up to 1500 lb was detonated in County Tyrone. On 10 April 1992 at the London Baltic Exchange and on 24 April 1993 in the Bishopsgate area of London, one-ton vehicle bombs were detonated. On 12 July 1994, police found a two-ton bomb hidden inside a lorry arriving at the English port of Heysham on a ferry from Warrenpoint, Northern Ireland. On 15 June 1996, widespread damage was caused in the Manchester city centre by a 3000-lb IRA bomb; the largest successful terrorist bomb deployed in UK.

As was the IRA custom, a bomb warning was given prior to the detonation of the Manchester bomb. The area was evacuated, and there were no fatalities, although there were several hundred injuries and massive property damage. Given that their attacks were not aimed at mass killings of civilians, which would have alienated their Catholic support base in Ireland, IRA attacks were deliberately planned to cause maximal damage and economic loss.

By contrast, Jihadis have absolutely no qualms about mass murder, indeed they have an explicit intent to kill civilians. This is self-justified as retribution for many thousands of Muslim deaths inflicted by the Crusader West. The time path of the Jihadi terrorist campaign against the Crusaders is multi-generational and lacks the urgent electoral cycle time scale of Western democracies. Accordingly, weapon development can take place patiently over decades.

Such has been the counter-terrorism pressure that there has yet to be a successful Jihadi car bomb attack against the Western alliance in the 15 years since 9/11. Before any massive Jihadi bomb of two tons or more is detonated in a major Western city, terrorism ILS investors may well have some preparatory warning by way of the prior occurrence of a lesser size vehicle bomb plot, possibly as part of a multiple target bombing attack. The above IRA bomb development sequence supports this supposition.

The same development time principle applies to Chemical-Biological-Radiological-Nuclear (CBRN) attacks, which remain an aspiration of Jihadis, but not yet a practical reality. Before any massive CBRN attack, some precursory lesser attack may provide an early warning indicator of increasing terrorist capability and progression on the demanding technical learning curve. As the anthrax letter scare in Autumn 2001 demonstrated, even a small quantity of anthrax can cause mass terror. If a terrorist cell has accumulated even a modest quantity of a highly toxic substance, there would be very strong counter-terrorism pressure to deploy it rather than to delay an attack by months to acquire much more. The law of diminishing returns would apply to the prospective terrorist gain. Operational research methods can quantify the balance between the risk of arrest and the reward of a more potent weapon. Since 9/11, denial of safe terrorist havens for laboratory R&D has meant that not even a minor Jihadi CBRN attack has been witnessed, and there is scant evidence of experimentation and preparation of toxic material. In Syria, chlorine bombs have been deployed, but these lack the lethal potency of nerve agents.

### 14.1.5 Frequency of Terrorist Attacks

Amongst the foremost concerns widely expressed about terrorism risk assessment is over the estimation of the annual frequency of the class of macro-terror attacks, defined as those which cause significant economic loss in excess of $1 billion, numerous casualties in excess of 50 fatalities, or harm to iconic national targets. This frequency is tightly constrained by counter-terrorism action, specifically mass electronic surveillance.

Spectacular macro-terror attacks require diligent planning, reconnaissance and attack preparation, and a number of trained operatives; the more ambitious and extensive a terrorist plot is, the more operatives are needed. No person lives in complete isolation. Every human being has his or her own social network, and terrorists need emotional, religious and operational support and encouragement from theirs. Social networks are amenable to a substantial degree of analytical characterization, providing a sufficient window on terrorist cell contacts for most plots to be interdicted. The various links between members of a social network provide key insight into the involvement of an individual in a terrorist plot. The singular achievement of the Western security services in interdicting the vast majority of significant plots since 9/11 is evidence of their command of terrorist communications networks, in particular monitoring electronic meta-data on who is contacting whom.

For terrorism frequency analysis in the Western alliance, the basic metric is not the number of successful macro-terror attacks, of which there are very few, but the number of plots, of which there are far more. Terrorist social network analysis by RMS has shown that the likelihood of a plot being interdicted through counter-terrorism surveillance increases progressively with the number of operatives as indicated in Table 14.1.

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 scarce terrorist resources. Discouragement of Jihadi plots 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.

As indicated above, for lone-wolf plots, the chances of plot interdiction through the methodical process of contact chaining are only about a quarter. The tragically common US occurrence of lone-wolf shooters suggests that the interdiction rate could not be maintained at a higher level than this without a great deal of luck. Less methodically, more interdictions may occur through lucky tip-offs or random searches, or through the deliberate entrapment of

**Table 14.1** The likelihood of a terrorist plot being interdicted

| 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 |

terrorists. The latter has been a popular if controversial FBI tactic; civil libertarians may question whether sting operations would ultimately lead to real attacks without external assistance. A conservative and robust approach to frequency modelling involves simulating plot sequences with interdiction rates based on counter-terrorism surveillance leading to courtroom terrorism convictions, but without any additional supplement to the interdiction rates to account for lucky or contrived interdictions.

The Five Eyes Alliance is the foremost international intelligence gathering collective. It comprises the five English-speaking countries: UK, USA, Canada, Australia and New Zealand. Recognizing the tight surveillance in the Five Eyes Alliance, terrorism insurance in these countries is effectively insurance against the failure of counter-terrorism. No terrorism insurance loss can occur without a gross breach of security and intelligence failure, which are the responsibility of the state. It is salutary for insurers to reflect that the prime impact from a terrorist attack is not the insurance loss, but the casualties, economic damage, national and international political repercussions, and of course public fear and apprehension. Such are the serious societal consequences that as the principal stakeholders in security, Western governments have been committed to spending heavily on counter-terrorism, even during times of economic austerity.

Terrorism is a man-made rather than natural hazard. This is generally perceived to be a negative and destabilizing characteristic for insurance purposes. However, because terrorist plots are conceived by human beings, they can be (and usually are) thwarted in a way that hurricanes and other hazards of Nature cannot. In 2004, when four hurricanes struck Florida, Governor Jeb Bush was powerless to stop their repeated landfall in his state. Unlike hurricane risk, terrorism is a control process: as and when the threat is raised, the counter-terrorism response is also raised. Also, as and when terrorist attacks do occur, the forces of counter-terrorism react promptly to suppress the likelihood of further attacks. This response has happened after each of the notable successful attacks against the Western alliance since 9/11.

When Michael Chertoff was appointed Secretary of Homeland Security in February 2005, President Bush instructed him not to let 9/11 happen again. He did not. Following this instruction, Secretary Chertoff kept a clean terrorism sheet for his entire four-year term of office—but Hurricane Katrina struck catastrophically in August 2005. Al Qaeda commented with *schadenfreude* that the hurricane had joined the Jihad. After the failed Christmas Day 2009 airline bombing by Umar Abdulmutallab and the failed Times Square bombing by Faisal Shahzad on 1 May 2010, the Director of National Intelligence, Dennis Blair, lost the full and complete confidence of President Obama and was compelled to resign.

### 14.1.6 Dependence on Human Behaviour

One of the main concerns about terrorism risk modelling is that it is perceived to be too dependent on human behaviour. Nobody can read the mind of a terrorist, so how can the risk of a terrorist action be estimated? There would indeed be a strong dependence on human behaviour if terrorists were allowed to attack at will. In many countries of the world, where the law enforcement and security services are ineffective or corrupt, terrorists are allowed to attack at will, and terrorism risk is then very dependent on human behaviour. In Pakistan for example, where the ISI intelligence service openly supports the Taliban because of unresolved Indian border disputes, terrorists may attack at a time and tempo of their own choosing. In Pakistan, terrorism risk is governed by Taliban behaviour.

By contrast, in the countries of the Five Eyes alliance, terrorism is controlled through a broad range of tough counter-terrorism actions, including massive and indiscriminate electronic surveillance, and terrorists cannot attack at will. Indeed, in a parliamentary Inquiry after the Edward Snowden surveillance revelations, Andrew Parker, the director-general of MI5, insisted that such surveillance was essential if terrorists were not to be able to attack at will. Terrorist behaviour is tightly governed by controls placed on what terrorists can do without being arrested. In particular, the trend towards smaller lone-wolf plots is a causal reflection of the practical difficulty in organizing larger plots without counter-terrorism disruption. On assuming the leadership of Al Qaeda after the death of Osama bin Laden, Ayman al Zawahiri recommended the strategy of lone-wolf plots. He had learned a basic lesson of conspiracy, which dates back to Imperial Rome: when others are listening, conspiracies should be kept small. Back in 2006, he had boasted of an Al Qaeda plot bigger than 9/11. This was the ambitious liquid explosives plot aimed at bringing down seven transatlantic passenger jets from UK to USA and Canada. This large complex plot was interdicted, and the terrorists convicted and jailed.

Another concern widely expressed about terrorism risk assessment is over the lack of access to classified information. Clearly, real-time classified information is needed to stop the next terrorist plot. But it is not the task of a terrorism risk analyst to forecast the next terrorist attack, just as it is not the task of a hurricane risk analyst to forecast the next hurricane, nor the obligation of a seismic hazard analyst to forecast the next earthquake, even if this were possible.

Regarding the terrorist threat, there is a need for information on past terrorist plots. In the Western democracies, such information is publicly available (with some time delay) from documentation on courtroom convictions: any genuine plot will lead ultimately to terrorist conviction. Nobody acquitted in court should be designated as a terrorist. As corroboration, the compendium of plots against the West by Mitch Silber (2012), director of intelligence analysis at NYPD, does not include any plots outside the public domain.

Besides classified information on the terrorist threat, there is also classified information on counter-terrorism activities. Some information of this kind has been privately accessed by RMS since 9/11 through convening annual closed intelligence and terrorism meetings alternately in London and Washington DC. Other important sensitive information has been publicly disclosed in large volumes by the NSA whistleblower Edward Snowden in June 2013 (Harding 2014). This unauthorized disclosure confirms that the principal agent for counter-terrorism control is massive electronic surveillance and acquisition of communications meta-data, involving multiple contact chaining of terrorist suspects. The details of this surveillance were hitherto classified, but nonetheless have been deliberately leaked into the public domain.

## 14.2 Terrorism Risk Bonds

The ILS market for terrorism risk has been very limited. Crucial to the development of this market is the balance of market supply and demand for terrorism coverage. In the aftermath of 9/11, insurers were paranoid about exposure to a catastrophe risk that had not been adequately appreciated nor priced—a classic Black Swan. Inevitably, the price of terrorism risk coverage was high. But even then, the number of insurers offering coverage was strictly limited. Many insurers refused to cover terrorism risk and excluded this risk from their policies.

Progressively over time since 9/11, the understanding of terrorism risk has improved, and the actual insurance loss experience has been small. This has largely been a consequence of effective counter-terrorism action within the Western alliance. Such plots that have been successful have been comparatively small. The great majority of terrorist plots have been interdicted; others have failed for technical reasons attributable often to human error.

As a result, the price of terrorism cover has fallen quite considerably. Contrary to what might be anticipated of a commercial market, the number of insurers prepared to offer coverage has increased substantially, despite a fall in premiums. The development of terrorism insurance markets has been broadly supported by government backstops. In UK, France, Spain, Germany and Australia, the respective organizations are Pool Re, Gareat, Consorcio, Extremus and the Australian Pool Reinsurance Corporation.

The US Terrorism Risk Insurance Act (TRIA) of 2003, and its legislative successors in 2005, 2007 and 2015, have provided a government backstop for US terrorism insurers. At each renewal of TRIA, arguments have been put forward by free market proponents that diminished coverage of TRIA might encourage the development of the US terrorism ILS market. This remains to be seen. If a terrorism act is certified, insurers are eligible for payments under the Program. These depend on multiple factors, including the Program Trigger, individual insurer deductibles, the Federal share of compensation, and the Program Cap. The Program Trigger is the amount of aggregate industry insured losses that must be exceeded before any Federal payments are made. The Program Trigger was $120 million in calendar year 2016; increasing by $20 million per year thereafter until $200 million in 2020. If aggregate industry insured losses exceed the Program Trigger, an insurer must pay its individual insurer deductible—that is an amount of losses that equal 20% of its direct earned premium in TRIP-eligible lines for the prior calendar year—before becoming eligible for Federal payments. The Federal share in calendar year 2016 was set at 84% of insured losses in excess of a particular insurer's deductible, with the insurer remaining responsible for a continuing co-participation share of 16%. The Federal share was set to decrease by one percentage point a year through 2020, at which time the Federal share would be 80%, and the insurers co-participation share 20%.

For large insurers, the individual insurer deductible may be sufficiently sizeable for the Federal cover to be relevant only for the very largest terrorist attacks. But for such extreme events, the Federal cover is very helpful. In the absence of such Federal cover, the prospect of alternative risk transfer to the capital markets would become closer.

On 12 January 2015, the Terrorism Risk Insurance Program Reauthorization Act of 2015 was signed into law by President Obama. In the drafting of the 2015 reauthorization bill, consideration was given by the House Financial Services Committee to various alternative wordings that would have reduced the coverage given by the US government backstop. One such alternative would have focused US government involvement in the terrorism insurance market on covering terrorism losses from attacks using weapons of mass destruction.

The future terrorism ILS market is heavily dependent on the political motivation in Washington DC to reduce government involvement in the private insurance market. With the White House and Congress all in Republican hands following the 2016 elections, some ILS developments may be anticipated as the third extension of the original 2002 Terrorism Risk Insurance Act (TRIA) sunsets at the end of 2020, coinciding with the end of the first term of the Trump Presidency.

### 14.2.1 Golden Goal Finance Ltd.

The only previous standalone ILS was Golden Goal Finance Ltd., issued by FIFA in 2003 in respect of the cancellation of the 2006 World Cup in Germany. The context to this issuance is noteworthy. After the Al Qaeda terrorist attack on 11 September 2001, the event cancellation insurance for the 2002 FIFA World Cup in Korea/Japan was itself cancelled. Warren Buffet stepped into this sudden protection gap as the insurer of last resort. Although there were terrorist threats to the 2002 FIFA World Cup, the tournament was held without terrorist disruption. Once the tournament had ended, FIFA set about obtaining coverage for the 2006 World Cup in Germany. The prevailing price for terrorism coverage was high in 2002, and offers of terrorism insurance turned out to be expensive. Less costly was the issuance of an event cancellation bond.

There has been a misapprehension that the German government had the authority to cancel the 2006 World Cup in Germany. This would have made this a political risk, rather than terrorism bond. This is not the case. It was FIFA's tournament, and it was FIFA's decision as to whether the tournament was cancelled or not. The German government's major role was in providing military-level security, including flying AWACS aircraft to provide early warning of any aviation threat.

Sold largely to European banks less than two years after 9/11, this $260 million bond issuance was a notable counter-example to the prevailing belief that terrorism risk was not securitizable. A key aspect of this transaction was its careful structuring that earned it an A3 rating from Moody's. Without this investment grade rating, the bond coupon would have been unfavourable relative to the price of insurance, and the bond would not have been issued.

Crucial to the bond rating was an innovative terrorism risk analysis which developed an elaborate event-tree of pathways to tournament disruption. This took account of the tight German military security protecting the event; the security-dependence of terrorist target preferences; and the history of terrorist plots against major sporting events, which included an Algerian terrorist plot against the 1998 World Cup in France.

The principles of terrorism risk modelling outlined above were invoked for the Golden Goal Finance Ltd. Risk analysis. In particular, the principle of terrorist target substitution was used in an original way. The likelihood of any one target being attacked cannot be assigned without consideration of all the others that might be substituted. By enumerating other targets, this likelihood becomes bounded.

The risk analysis for Golden Goal Finance Ltd. also allowed for the possibility of the tournament being replayed in 2007 in the event of any terrorist incident in 2006, and the redundancy in available German football stadiums which contributed to the tournament resilience against disruption from any external hazard. No plausible terrorist strike could have prevented tournament football being played to completion, even if several stadiums were out of action. Furthermore, even if 2006 were a dreadful year for terrorism in Germany, there was the possibility of replaying the tournament the following year—the next major international tournament was the European Nations Cup in 2008. Recognition that cancellation was a double-event contingency was a crucial element of the terrorism risk analysis.

Ever since 9/11, there has been an insurance market sentiment that the assessment of terrorism risk is far more uncertain and volatile than natural hazards, that the risk is too ambiguous, and hence would be difficult to securitize. But this sentiment ought to change with the understanding gained of the counter-terrorism security constraints which have suppressed terrorism losses across the Western alliance since 9/11, despite political turmoil in the Middle East. The benign terrorism insurance loss experience in the period since 9/11 should encourage terrorism ILS investment. During this period, there have been numerous terrorist plots against the Western alliance, but only a handful of successful attacks. Furthermore, for each of the few major successful attacks (Madrid 2004, London 2005, Boston 2013, Paris 2015, Nice 2016), one or more of the terrorists were previously known to the security services, and might have been tracked, and eventually arrested.

### 14.2.2 Future Terrorism Catastrophe Bonds

In his TRIA testimony to congress in November 2013, John Seo of Fermat Capital publicly expressed a vision for a substantial growth in the terrorism ILS market. His vision may well be shared by other ILS fund managers, who may be overweight on US hurricane risk, especially Florida risk, and seek further diversification. Hurricane Matthew in October 2016 would have reinforced the need and encouraged the quest for diversification. At one stage, as it moved past the Caribbean, Hurricane Matthew threatened to be "The Big One". It might have made landfall near Palm Beach in Florida as a category 4 storm, and caused a major loss to ILS portfolios.

Excess mortality bonds provide a valued source of ILS diversification, and these bonds are much in demand by ILS funds. Already, holders of excess mortality bonds are exposed to some terrorism risk (including CBRN), so this asset class is not new. Seo (2013) argues for the bundling of coverage with risks that are better understood, and/or the exclusion of risks that are less well understood.

The most obvious property insurance bundling would be the inclusion of some conventional terrorism risk (non-CBRN) within a natural hazard bond. As with natural hazard ILS, there is scope for enterprise in the design of terrorism triggers so that they meet the coverage needs of the issuers as well as the investment return requirements of ILS fund managers. This search for a mutually agreeable trigger may lead to a focus on a variety of domains of terrorism risk.

The existence of government backstops for terrorism losses limits the need and hence opportunity for risk transfer to the capital markets. Otherwise one risk domain could correspond to a massive vehicle bomb of two tons or more in Manhattan, London, or other European financial hub city.

An international terrorism insurer may issue a multiple country bond involving a group of countries or individual cities. The trigger might be a major synchronous attack in one or a number of specific cities. The UK Prudential Regulatory Authority has requested property and casualty insurers to stress test their capital reserves against a synchronized terrorist attack with two ton bombs detonating in London and New York, and another in Paris, Frankfurt, Hong Kong, Singapore or Sydney. The accumulation risk management challenge posed by this extreme scenario could be addressed by considering alternative risk transfer to the capital markets. The risk associated with this particular scenario is very low because of the close counter-terrorism collaboration between intelligence services in USA, UK, France, Germany, Singapore and Australia.

CBRN risk is already included within excess mortality ILS. For property insurance, an environmental protection bond might be issued to help pay the huge clean-up costs following an attack causing widespread radiological or toxic pollution. The anthrax letters sent to US government offices soon after 9/11 incurred massive clean-up costs. Demolition of a senate building in Washington DC was not a viable political option, but for ordinary buildings, this may be considerably cheaper than the immense cost of thorough decontamination. As a consequence, widespread geographical dispersal of anthrax letters would have enormous costs.

There has yet to be any kind of CBRN attack against the Western alliance, although chlorine bombs have been deployed in Syria, sarin stocks have been held by the Syrian government, and radioactive material at the University in Mosul, Iraq, has been identified by ISIS as a potential source for a dirty bomb. A probabilistic risk analysis for a CBRN attack can be undertaken using event-tree logic of the type familiar from probabilistic safety assessment studies for nuclear installations. Inevitably, there is an inherent degree of parameter uncertainty in CBRN modelling. This would be reflected in the price for any ILS instrument.

### 14.2.3 Terrorism Parametric Trigger Bonds

Parametric trigger catastrophe bonds are popular with investors because of the concerns they have over either indemnity or modelled loss catastrophe bonds. With either of the latter type of bonds, uncertainty over the characterization of the portfolio at risk is a worry for investors For example, the portfolio might be adversely selected, and suffer anomalously high indemnity losses. In addition, a modelled loss may be particularly conservative, and so exaggerate losses. On the other hand, an issuer would have concerns with parametric triggers because of basis risk: a mismatch between a bond payout, if a trigger event occurs, and the higher actual loss incurred by the issuer.

With a terrorism trigger bond, there are a variety of possible triggers that might be adopted. The simplest trigger would be based on the specific attack weapons deployed, for example improvised explosive devices of various explosive sizes, and the towns and urban locations which were targeted. Other pieces of information might be introduced into the trigger definition so as to reduce the basis risk. These might include the terrorist organization responsible, the number of operatives, and so on. In the event of a possible trigger occurrence, there may be some ambiguity over determining the parameters selected to define a parametric trigger. To establish whether or not a defined trigger event has actually happened, an independent agency would have to be nominated to certify that an event was an act of terrorism, and that the attack details match those required to trigger the bond.

For geographical regions where terrorism is endemic at a high level, and attacks are commonplace, for example Pakistan, there are a number of global terrorism databases that provide a public information source for trigger frequency estimation. For other regions, for example countries of the Western alliance, where counter-terrorism forces are much more capable and trustworthy, structured terrorism modelling methods allowing for a high rate of attack interdiction are required for the quantification of trigger risk, which is likely to be low.

There are some interesting possible multi-year trigger structures, which would take account of the extra development time for large attack modes. Thus, a bond might trigger for the first significant attack, but thereafter would not trigger for larger subsequent events. For example, any vehicle bomb might provide an initial payout, but subsequent payouts would only be for events of the original triggering size or less. Alternatively, the risk transferred might just be for surprising large attack modes, and the bond would only trigger if there were no small or moderate events previously.

## 14.3 Pandemic Risk

Terrorism risk has been included in all excess mortality ILS transactions since Vita Capital in 2003, but it constitutes only a minor proportion of the mortality risk, which is dominated by pandemic influenza which has been called “Nature’s biological weapon”. More died in the 1918 pandemic than in the Great War.

Since the SARS outbreak in 2003, the mortality implications of a major infectious disease have been securitized in excess mortality bonds, primarily issued by life reinsurers. New influenza strains like bird flu H5N1 and swine flu H1N1 are the predominant threat source. But emerging diseases like coronaviruses (such as SARS) are also a concern. Animal reservoirs of viruses are a common source of threat in Asia and Africa. Countries with fragile veterinary surveillance systems are especially liable to be the source of an emerging disease.

The two key parameters that drive the risk for any specific threat are the lethality rate, and the reproductive ratio $R_0$, which is the average number of people infected by one person. The population spread of a pandemic is assessed using an epidemiological SIR model. The acronym SIR stands for Susceptible-Infected-Removed. As the pandemic spreads along the social networks of the infected, some of the susceptible population also become infected. The availability of an effective vaccine reduces the susceptible population. Those that are infected may either recover, possibly with the assistance of an anti-viral treatment, or else die. In either case, they are removed from the population susceptible to the disease.

A stochastic model for pandemic risk includes an ensemble of scenarios spanning the range of possible influenza viruses and emerging zoonotic diseases. The shift of a virus to being either more lethal or more contagious happens randomly, so is amenable to stochastic modelling. For evolutionary biology reasons, there is a negative correlation between the lethality of an infectious disease and its degree of contagion. It is not in the evolutionary interest of a highly contagious virus to kill too many of its hosts.

Excess mortality bond trigger definition is based on a mortality index, which is a function of mortality levels in a selected basket of countries, weighted in a country-specific manner according to age profile. Various tranches can be structured, with the uppermost tranches being exposed only to catastrophe pandemics. Some of these might be linked with political conflict. The pricing of the various tranches is based on the expected loss, as quantified by excess mortality risk modelling, multiplied by a spread factor to allow for uncertainty.

### 14.3.1 Linkage with Political Risk

Insurance linked securities may include an explicit as well as implicit exposure to political risk. For example, excess mortality bonds are exposed to the mortality rate in designated countries rising substantially above the current level. Pandemic disease is the primary risk, but significant excess mortality might also arise from terrorism, and from a deadly war.

Moderate epidemics arise from a modest genetic drift in a human virus. A more severe pandemic risk is associated with a genetic shift in a human virus, against which there is little population immunity. Although such a shift is in itself a hazard of Nature, pandemic risk has a major man-made component. Viruses spread from one infected individual to another through human social networks. As mentioned above, a key parameter governing the severity of a pandemic is the reproductive number, which is the average number of others infected by one person. This parameter has some dependence on political conflict risk, since the spread and control of a pandemic are affected by the prevalence of war. The ability to treat the sick, and to track contacts of the infected, is eroded by the outbreak of war. Mass movements of people during the course of war, through refugee displacement and troop mobilization and demobilization, can also have a major impact on the spread of a pandemic virus.

A benchmark for a pandemic of insurance catastrophe proportions is the 1918 pandemic, the worst in modern history. The high case fatality rate of 2.5% is much higher than for the other pandemics of the twentieth century in 1957 and 1968, which were of the order of 0.1%. Far more people died of the influenza pandemic than in the Great War itself. The two global disasters were causally connected. The influenza was spread through the demobilization process after the war ended. But the influenza took hold beforehand, having most likely been brought to the Western Front by a cohort of 100,000 Chinese labourers in the Chinese Labour Corps. They were despatched there by the Chinese government in the forlorn hope that by assisting the Allied war effort, China might be given back its northeastern port city of Tsingtao, a former German colony. This never happened, but the outcome was a great pandemic stemming from the mass transport of the Chinese Labour Corps from China by train across Canada and onto England and the Western Front. It turns out that most of the major pandemics in human history have been associated with unusual mass population movements.

Almost a century later, political conflict and mass refugee migration characterize our turbulent times. The nexus between political conflict and pandemic, which was so catastrophic in 1918, could be revisited in our own time. Counterfactually, had there been a civil war in Sierra Leone in 2014, as there was in the 1990s, the dispersion of war refugees would have made it very difficult to contain the spread of Ebola within West Africa in 2014. Had the highly lethal Middle East Respiratory Syndrome (MERS) become more contagious in 2015, the migration of more than a million refugees from the Middle East conflict zone would have brought pandemic disease to the heart of Europe. This might have been exacerbated by intentional spreading of MERS by supporters of ISIS, as is discussed below.

Any emerging infectious disease pandemic could spread in an unstable political region like a wildfire. Just as prevailing wind conditions are a key factor in modelling the spread of wildfire, so also population migration is an important factor in governing the spread of a pandemic. A key parameter in pandemic model is the reproductive ratio $R_0$, the average number of people infected by one person. A pandemic model should include scenarios with values of the reproductive ratio $R_0$ dynamically inflated by sustained mass migration, as characterizes zones of enduring conflict.

### 14.3.2 Bio-Terrorism

To compound the pervasive political conflict in the Middle East, there is the terrorism risk associated with the deliberate malicious spread of a pandemic in Western countries. The use of biological weapons by terrorists has a long history, and has an extensive literature. Ever since 9/11, the threat of Al Qaeda using biological weapons has been taken very seriously. Indeed, for counter-terrorism response, it has been the Pentagon that has funded research into the development of vaccines for plague and Ebola and other pathogens that might be weaponized by terrorists. Biological weapons are attractive to terrorists drawn to becoming bio-martyrs. The millenarian sect Aum Shinrikyo sent a medical team to the Congo in 1993 to investigate the prospects for weaponizing Ebola. This proved too difficult because Ebola was not highly contagious. Two years later, they launched a sarin gas attack on the Tokyo subway.

With the deployment of any terrorist weapon, the three factors that need to be taken into consideration to gauge the threat are (1) intent; (2) capability; and (3) opportunity. The intent by ISIS and other terrorist groups to use infectious disease as a biological disease is clear from their communications. Their capability to develop their own pathogens is minimal. However, if a lethal and transmissible infectious disease were to emerge, terrorist groups would have ample opportunity of spreading the disease at public gatherings, or on public transportation. Infectious disease propagates along social networks. Terrorists who spread disease maliciously become supernodes in these social networks. The epidemiological consequence of supernodes is to amplify the effective $R_0$ of the virus.

## 14.4 Political Conflict Triggers

Terrorism is one manifestation of political conflict. Terrorist campaigns constitute a form of asymmetric warfare, where the terrorist forces are far smaller than those of the nation states which they are attacking. Even with smaller forces, terrorism insurance is hardly viable if terrorists can attack at will, with little sanction from counter-terrorism forces. However, in those countries where this sanction is very disruptive, the possibility of interdicting most plots through surveillance means that terrorism insurance is quite widely available, where necessary with a government backstop.

Warfare is generally excluded as an insurable peril, although it is included in some policies. Opportunities for ILS triggered by political conflict may arise from considering how to mitigate consequential losses. When a natural or man-made disaster strikes, the consequent societal loss takes many forms. There is loss of life, physical and psychological harm; damage to infrastructure, homes, places of work and schools; loss of employment for adults; and lack of schooling for children. More generally, there may be damage to the economy as a whole, and to individual parts such as tourism, the service and manufacturing sectors, and so on.

Insurance products have been devised to cover the risk of most types of loss. One population group poorly served by insurance is that of children. The safety of children is of course paramount. However, the lack of schooling for survivors has not been given due attention, although this may blight the future lives of a cohort of children. Crucially, there is very high economic leverage in financing post-disaster children's education.

For countries, like those in the developed world, which have contingency funds for meeting the costs of occasional disasters, and which have the ability to raise funds through taxation or borrowing, insurance solutions are unnecessary. However, elsewhere, the significantly high benefit/cost ratio makes it worthwhile to seek insurance solutions for donations to improve education. Many developing countries in Africa, Asia and Latin America are exposed in their own way, and in varying degrees, to natural hazards and political conflict. For each country and major hazard to which it is exposed, the threshold severity level for causing substantial educational disruption can be identified. Beyond this level, a parametric trigger payout function might be defined which will depend on the amount and vintage of education funding at risk in the country concerned. This payout function would increase with the size of the hazard event above the specified threshold.

A risk analysis for an education bond would include a historical review of political conflict in the region where schooling is being protected. In addition, previous episodes of schooling disruption would be scrutinized and assessed for frequency and consequential educational loss. Trigger events relating to political conflict include ethnic, religious, colonial and separatist conflicts, civil wars, coups d'état, invasions and occupations. In contrast with natural hazard events, political conflict events may have a prolonged duration, and severely disrupt education for a very long time.

### 14.4.1 Political Conflict Risk Forecasting

In order to quantify the risk of the trigger events due to political conflict, a global model of political conflict needs to be developed. Global aggregation of past conflict data increases the database of extreme conflicts and facilitates international statistical frequency analysis. The model can then be regionalized by assigning conflict-propensity weights to individual countries, based on national conflict history and the current political threat landscape.

The risk assessment of political conflict is notoriously difficult because of the inherent uncertainty in the course of political events and in the course of a political conflict. The German general Helmuth von Moltke openly declared that "in war, everything is uncertain". Famously, he wrote that no plan of operation extends with certainty beyond the first encounter with the enemy's main strength. In contrast with the deterministic game of chess, the Prussian military invented board games with dice to introduce an aleatory element.

Inevitably, there is a degree of expert judgement in making any political risk forecast. There are superior methods for eliciting this expert judgement. Important lessons were learned following the intelligence debacle surrounding the 2003 Iraq War, where no evidence of weapons of mass destruction could be found, yet senior US intelligence officials remained adamant that Saddam Hussein definitely possessed such brutal weapons.

The massive intelligence failure associated with Iraq War led to a re-evaluation of intelligence assessment methods in Washington, and the establishment in 2006 of the Intelligence Advanced Research Projects Activity (IARPA). The scientific process of randomized control trials can discriminate those with particularly good judgement on political events. Superforecasters can be identified who have special skill in forecasting, as can be measured through a Brier score. It is not necessary to have years of intelligence experience to be good at forecasting political events. Indeed, many who do have such experience are rather indifferent or poor forecasters. Superforecasters have been identified as having some special traits. They are typically numerate, with a technical knowledge of Bayes theorem, even if they may not explicitly make their forecasts doing any actual Bayes theorem calculations. Rather, they edge towards the truth by implicitly following the Bayes principle of updating according to the weight of evidence using their own sense of intuition.

For any political conflict ILS, explicit use of Bayesian methods, including the construction of Bayesian Belief Networks (BBN), would optimize the forecasts made through progressive updating. Nevertheless, the pricing of political risk transfer ILS would be expected to incorporate a sizeable spread for the epistemic uncertainty in the underlying risk analysis.

## 14.5 Cyber Risk

ILS investors have expressed an interest in diversifying their portfolios away from natural hazards, especially hurricanes, and include some exposure to cyber risk. The insurance market for cyber risk is in a nascent development phase, with insurers wary of their potential cyber risk exposures across many lines of business, some poorly identified, and hesitant over estimates of probable maximum loss.

The insurance market is forecast to grow strongly in the decades ahead as online communication and business expands globally, and the issuance of cyber ILS is likely to follow this market trend, plugging notable gaps in market coverage. A prerequisite for market development is progress in cyber risk modelling. The modelling of extreme cyber risk is challenged by the comparatively short time period of data gathering. In its contemporary form, cyber risk is a twenty-first century phenomenon. Although cyber attacks are persistent and pose a continuous threat, estimation of an attack loss that might occur with a small annual probability of less than 1% clearly requires quantitative analysis beyond mere statistical extrapolation of limited past experience.

In order to address the challenge of modelling extreme cyber risk, it is instructive to explore how extreme cyber losses might arise. First, it is salutary to observe that there is a very large loss uncertainty associated with any attack scenario. There is a large human factor component both in the way in which a hacker drives forward an attack, and the way in which a defender counters it. Human error and misjudgement blight both the attack and defence. Furthermore, the availability of additional exploit tools can improve the prospects for navigating further within a target system, and remaining undetected.

So the loss impact on a single cyber target can vary substantially. Furthermore, the scaling potential of cyber attacks means that tens, hundreds, or many thousands of targets might ultimately be impacted. However, for persistent threats, there is a practical finite logistical time limit for a stealthy threat to remain unknown, especially in an increasingly sophisticated security environment for intrusion detection. This limits the scaling of cyber attack footprints to expand too far. Contingent on any cyber attack being launched, the loss outcome is thus highly variable. For any computer system attacked, the loss could vary enormously according to the number and type of zero day exploits used. The number of systems infected has the potential for scaling by orders of magnitude, according to the number of vulnerable systems.

An extreme cyber loss thus can readily arise from a common type of attack mode, but with a highly uncommon loss impact consequence. Expressing this insight in mathematical terms, denote the set of notable cyber attack scenarios as $\{S_j : j = 1, 2 \ldots n\}$. The annual frequency of the $j$th scenario is written as $f(S_j)$. Then the annual frequency of loss $L$ exceeding a very high threshold $X$ is written as the following summation over scenarios:

$$Freq(L > X) = \sum_j f\left(S_j\right) \times \Pr\left(L > X | S_j\right)$$

This summation receives significant contributions from the tails of the conditional loss distributions for events that may have occurred already in the twenty-first century. One such event is the Conficker Worm which was unleashed in November 2009, and infected millions of computers worldwide, and might have heralded the first digital world war (Bowden 2011). A basic practical probabilistic cyber risk model can be constructed from a rather compact number of scenarios, each of which is characterized by a broad conditional loss distribution.

### 14.5.1 Modes of Cyber Attack

A cyber attack is a crime, just as a terrorist attack is, but it need not have a political motive. Whereas a physical terrorist attack must involve one or more operatives in the country targeted, a cyber attack can be launched from well beyond the jurisdiction of the country attacked. Extradition treaties allow hackers to stand trial abroad, such as has forced UK hackers to submit to US justice for cyber crimes against US targets. However, many cyber attacks against Western countries are launched from Russia, China, Pakistan and so on, where there is very little prospect of bringing the cyber criminals to justice, and no sanction against their activities in their own countries. Indeed, foreign hacking may be encouraged, supported and sponsored at a state level.

Cyber risk modelling begins with the partition of cyber crimes according to motivation. Apart from the obvious financial motive, there are attacks by hacktivists espousing some political or social cause; there are acts of cyber espionage to steal confidential information; and acts of cyber warfare in preparation for a kinetic war. Cyberspace is acknowledged as the fifth dimension of warfare along with land, sea, air and space.

Financially motivated cyber attacks form the largest cyber event class. These can be modelled based on the economics of cyber criminal activity. Just as regular criminals can buy firearms and need not have the capability and labour to make such weapons on their own, so cyber criminals can buy exploit kits made by others, rather than endeavour to create their own hacking tools. There is a thriving market in the sale of exploit kits, made often by cyber criminal gangs based in Russia and the Ukraine. There is also an active market in the buying and selling of zero day exploits. Governments are active participants in this market, keen to maintain arsenals of effective cyber weapons in anticipation of a future cyber war. Governments hold the most powerful arsenals of cyber weapons, in readiness for war. The possibility of a security breach of a cyber arsenal is not hypothetical; it was demonstrated in 2016, when some National Security Agency weapons were picked up by a hacking team called Shadowbrokers. This demonstrates the catastrophe risk potential of cyber risk.

## References

Awan, A.N. 2016. The Impact of Evolving Jihadist Narratives on Radicalization in the West. In *Jihadism Transformed*, ed. S. Staffell and A.N. Awan. London: Hurst & Co.

Bowden, M. 2011. *The Worm*. New York: Atlantic Monthly Press.

Camerer, C. 2003. *Behavioral Game Theory*. Princeton, NJ: Princeton University Press.

Harding, L. 2014. *The Snowden Files*. London: Guardian Books.

McNeilly, M. 2001. *Sun Tzu and the Art of Modern Warfare*. Oxford: Oxford University Press.

Seo J. 2013. The Future of Terrorism Insurance: Fostering Private Market Innovation to Limit Taxpayer Exposure. In *Testimony to the Subcommittee on Housing and Insurance*. Washington, DC: US House of Representatives.

Silber, M. 2012. *The Al Qaeda Factor*. Philadelphia: University of Pennsylvania Press.

Woo, G. 2011. *Calculating Catastrophe*. London: Imperial College Press.

———. 2015. Understanding the Principles of Terrorism Risk Modelling from Charlie Hebdo Attack in Paris. *Defence Against Terrorism Review* 7 (1): 33–46. Ankara, Turkey.

**Gordon Woo** is a catastrophist, specializing in mathematical aspects of catastrophe risk modelling. He has extensive experience as a risk consultant for petrochemical, nuclear and airline industries. Since 9/11, he has focused on developing a quantitative framework for modelling terrorism risk, and is the chief architect of the RMS terrorism risk model. His work on terrorism has been publicized widely, and he is a regular lecturer at the NATO Centre of Excellence for the Defence against Terrorism, Ankara, Turkey. He has served as a terrorism expert panelist for both the US Department of Homeland Security and the UK Cabinet Office. *Newsweek* magazine has described him as one of the world's leading catastrophists. He undertook the terrorism risk analysis for FIFA's 2006 World Cup event cancellation bond: Golden Goal Finance Ltd. In 2004, for his work on terrorism risk, he was named by Treasury & Risk magazine as one of the 100 most influential people in finance. He is the author of the books, "The Mathematics of Natural Catastrophes" and "Calculating Catastrophe", both published by Imperial College Press, London. The latter has been translated into Italian as "Scienza e Coscienza delle Catastrofi", published by Doppiavoce. A top mathematics graduate of Cambridge University, with a postgraduate diploma in computer science, he completed his PhD at MIT as a Kennedy Scholar, and was a member of the Harvard Society of Fellows. He is a visiting professor at the University College London, and an adjunct professor at the Nanyang Technological University, Singapore.