Cambridge Centre for Risk Studies Working Paper Series

A Shock to the System – Research Programme of the Cambridge Centre for Risk Studies

Cambridge System Shock Risk Framework

A Taxonomy of Threats for Macro-Catastrophe Risk Management

Centre for Risk Studies

UNIVERSITY OF CAMBRIDGE
Judge Business School

Andrew Coburn, Daniel Ralph, Michelle Tuveson, Simon Ruffle, Gary Bowman

Working Paper 201307.20
Draft: July 2013
Availability for download at
www.risk.jbs.cam.ac.uk

Cambridge Centre for Risk Studies
University of Cambridge Judge Business School
Trumpington Street
Cambridge, CB2 1AG
United Kingdom
enquiries.risk@jbs.cam.ac.uk
www.risk.jbs.cam.ac.uk

Acknowledgement

This work was carried out with partial support from

NANYANG TECHNOLOGICAL UNIVERSITY
Institute of Catastrophe Risk Management

A Shock to the System – Research Programme of the Cambridge Centre for Risk Studies

Cambridge System Shock Risk Framework

A taxonomy of threats for macro-catastrophe risk management

Andrew Coburn[1]*, Gary Bowman[2], Simon Ruffle[3], Daniel Ralph[4], Michelle Tuveson[5],

20 July 2013

Abstract

This paper argues that there is a need for a systematic assessment of the taxonomy of macro-catastrophe threats that have the potential to cause damage and disruption to social and economic systems in the modern globalized world. It presents the threat taxonomy developed as part of the Cambridge Risk Framework and describes the methodology used, including a categorization based on causal similarity. The framework and the taxonomy are intended for use in a number of applications, including use in insurance accumulation management for complex threats that can impact multiple lines of business. The taxonomy provides a framework for populating with more detailed studies of each threat. A method of benchmarking and comparing between the threats is proposed, based on developing scenarios that illustrate the severity of event that might be expected with 1% annual probability of exceedance. The consequences of these scenarios can be assessed from their impact on specified categories of assets, liabilities and economic business sectors, and a standardized data structure for developing scenarios is outlined.

Keywords: risk management, disasters, catastrophe, taxonomy, threat, business management, scenarios, categorization

,

Author(s):

1. Director of External Advisory Board of the Centre for Risk Studies, University of Cambridge, and Senior Vice President, Risk Management Solutions Inc.
2. Research Associate, Centre for Risk Studies, University of Cambridge; Cambridge-Singapore Fellow; partial support from the Institute of Catastrophe Risk Management, Nanyang Technical University, Singapore, gratefully acknowledged
3. Director of Technology, Centre for Risk Studies, University of Cambridge
4. Professor of Operations Research, Judge Business School, and Academic Director of the Centre for Risk Studies, University of Cambridge
5. Executive Director of the Centre for Risk Studies, University of Cambridge

* Correspondence to: Andrew Coburn, University of Cambridge Judge Business School – Centre for Risk Studies, Trumpington Street, Cambridge, UK, CB2 1AG. Email address: andrew.coburn@jbs.cam.ac.uk

Working Paper 201307.20 www.risk.jbs.cam.ac.uk

1 Context and Objectives

1.1 Catastrophes and Society

The modern world is vulnerable to the disruption of the social and economic systems that serve it. Periodically events occur that disrupt our daily lives and force changes to the ways we do business, disrupt the trading patterns of commerce, interrupt economic productivity, and devalue financial instruments and assets. Extreme events are described as social and economic catastrophes. Where they cause severe impacts to more than one continent, they can be termed 'global shocks' or 'macro-catastrophes'. There are many potential causes of macro-catastrophe, ranging from epidemics, to financial credit availability, localized destruction of means of production, and geo-political disruption to trading systems. Managing the risks of disruption from macro-catastrophes is a major concern of government national security, international businesses, financial services and insurers, and investment managers across the world.

1.2 Catastrophe risk management in the insurance industry

The management of risk from natural catastrophes (hurricanes, wind storms, earthquakes, floods and others) is now a mature science. Natural catastrophe risk models have been available since the early 1990s. Companies and individuals owning property that is at risk from natural catastrophes in many parts of the world can buy insurance to transfer their risk, and the insurers and reinsurers can profitably offer this coverage, knowing from their catastrophe models how to safely diversify this risk and avoid incurring ruinous losses.

However, there are many other types of extreme events beyond natural catastrophes that pose a risk of loss to global companies. These are less well understood and the science around them may not be as well advanced. Some types of threats may not have been experienced in recent history and may be largely unappreciated. Recent years however have seen a series of occurrences of events that have been highly disruptive to global businesses, ranging from volcanic ash clouds, to disease outbreaks, to social unrest, cyber-attacks, and a wide range of other geopolitical, technological, financial, and environmental events that have impacted global trade and commerce. As each new type of event occurs, society reacts retrospectively to recognize the threat and put new safety measures into place, and companies often instigate new risk management techniques specifically for the threat that has just 'emerged'. And yet few of these disruptive events are unprecedented. It is common for risk management discourse to be around 'emerging risks' or unforeseen perils, 'Black Swans' or other surprises. Many companies have instituted 'emerging risk' monitoring systems, committees, or other processes.

It could be argued that instead of new threats becoming more common, globalization of our economy is the real driver of this emergence of frequent disruptive events: businesses that only a decade or so ago were serving regional markets and familiar with the variables of one localized part of the world are now serving global markets, carrying out business activities in hundreds of cities worldwide, and reliant on travel and communications infrastructure to interlink all their business activity into a global system. These interlinkages of the global business system are vulnerable in a very different way to the physical infrastructure of regional businesses of past generations. The world is a volatile place, and extremes of weather, geophysical processes, political and social patterns occur periodically in many locations – possibly no more frequently that they have done before. Now however, the global corporations notice these extreme events in an entirely new way, as they impact some part of the linkage structure of their global business.

Global businesses are looking for ways to manage the balance sheet risk of these disruptive events, and to be better prepared for future new or 'emerging risks'. Many of these macro-catastrophe risks are systemic in nature – i.e. they have the ability to impact not just a single company but many companies, including the main business counterparts of the business and possibly many parts of the economic system at the same time.

The systemic nature of these macro threats makes them more complex for insurance companies to cover. Traditionally insurance companies manage their risk across many different lines of business, such as property, casualty, marine, aerospace, energy, life, health, trade credit etc. These are compartmentalized and managed under the assumption that they are broadly independent. Some macro-catastrophes are capable of causing systemic losses across multiple lines of insurance business, and potentially even simultaneously causing a financial markets crisis, in which the insurer suffers losses in their investment portfolio at the same time as experiencing high claims levels.

Insurers and global corporations both have an interest in understanding the global risk landscape of macro-catastrophe threat. If these threats are better understood, they can be managed effectively by diversification and risk management. If they are insurable, then insurance companies could extend their utility to global corporations in offering coverages that provide protection to the corporate balance sheet, in ways that may not be possible today.

1.3 Emerging Risk Terminology

There is a lot of different terminology currently being used to describe these various types of systemic and unexpected risks. In some cases the terms have subtle differences. Terminology in common use includes the following, with a suggested definition of this term and an example.

Emerging Risks

A cause of potential extreme loss that is becoming apparent or more significant than previously understood, either because the threat itself is growing, or because society is increasing its vulnerability to that cause of loss.

e.g. cyber catastrophe risk, climate change, laboratory-originated pandemics

Correlated Risks / Cascading Risks / Consequential Risks

One type of peril triggers an event of another type, to cause a much more extreme event.

e.g. a large earthquake causes a tsunami that triggers a nuclear meltdown

Clash Risks / Contingent Risks / Network Risks / Macro-Catastrophes

An event that causes losses across several lines of insurance business or that causes loss in unexpected locations or across multiple geographical markets because of the interconnectivity of business connections to the region affected.

e.g. Thailand floods causing contingent BI losses to US business supply chains

Systemic Risks / Financial Contagion / Exogenous and Endogenous Risks

Economically-impactful threats that ripple through business and financial systems. The term 'systemic risk' is commonly used in financial risk management to mean events and practices capable of causing consequential effects throughout the financial system, so tends to have a specific meaning in financial regulatory practices.

e.g. Housing price bubble

'Black Swans'[1] / 'Known Unknown'[2] Risks

---

1 Taleb (2010) *The Black Swan: The Impact of the Highly Improbable.*

2 Term popularized in a press statement by Donald Rumsfeld, United States Secretary of Defense, February 2002, addressing the absence of evidence linking the government of Iraq with the supply of weapons of mass destruction to terrorist groups.

A strategic surprise from extremely unlikely events outside the realm of regular expectations, and only able to be predicted in retrospect. The emphasis of this meaning is on the unknowability of the type of event, and our inability to anticipate its occurrence due to our own preconditioning.
e.g. Collapse of the Soviet Union

'Dragon King'[3] events
An event of a class of threat that occurs with a greater magnitude than was expected, a 'meaningful outlier'.
e.g. 9/11 attack as a far larger terrorist attack than had been previously experienced

Unmodelled risks / Unmodellable risks / 'Pear-Shaped Phenomena'[4]
Insurance industry terms for risks that are less well understood than traditional perils, but that can cause insured loss, or represent insurance opportunities that are underexploited. These are low-probability, high-consequence events that have not been commonly quantified, that represent challenges in conventional modelling terms, and are sufficiently below the insurance radar that many in the industry may not have considered them. They are risks that are recognized to be foreseeable and amenable to risk analysis and could be future priorities for parties that carry, price, and transfer risk.
e.g. Volcanic ashcloud fissure eruptions (Laki 1783); meteorite airbusts (Tunguska Siberia 1908).

1.4 A Taxonomy of Threats

A systematic evaluation of threats that could cause future macro-catastrophes would be useful for these various different aspects of risk management. The objective of the System Shock research programme of the Centre for Risk Studies at University of Cambridge is to develop a systematic and evidence-based approach to threat assessment and risk management for macro-catastrophes. This paper sets out the approach to categorizing the threat typology that is being used as a framework for collation of the state of knowledge about each threat type.

Each type of threat exhibits different mechanisms of disruption, exposes specific vulnerabilities and poses different challenges for improving resilience of systems in risk management. A taxonomy of different causal mechanisms is an important first step in categorizing threats.

1.4.1 State of knowledge about each threat

The typology of threats is proposed as a framework, intended to be used to collate information about the state of knowledge of each threat. It is intended to develop a standardized set of information, including a historical catalogue, case studies of past events, and a summary of the main literature on the topic. The state of knowledge is intended to include an assessment of the frequency and severity of occurrences of each threat. In many cases frequency and severity estimates will be highly uncertain, but it is intended to use broad categories of magnitude assignment and a first-order estimation of the likely return period of different magnitudes of events worldwide.

The framework is proposed as a way of identifying the total landscape of risk, and to benchmark the states of knowledge about each threat. It is clear that some threat types are much better understood than others. A standard framework will enable threats that are least understood, but thought to be capable of destructive events, to be prioritized for more detailed research. Where significant threats are identified, these can be investigated and the science developed into more detailed models if necessary. The framework will enable the development of catastrophe models in the new or emerging categories of threat as and when this becomes appropriate. Ultimately it may be possible to develop

---

[3] Sornette (2009) '*Dragon-Kings, Black Swans and the Prediction of Crises*'.
[4] Blong (2013) '*Pear-Shaped Phenomena: Low Probability, High Consequence Events*'.

stochastic models of many different categories of threats that will enable a holistic assessment of all major threats. This however will require significant resources and is beyond the scope of this round of research development. This research activity is to develop the framework that will define the major areas of threat. Population of the framework is likely to be incremental and prioritized by the importance of the threat and perhaps by the need for better understanding.

1.4.2 1% annual probability stress test scenarios

A relatively simple first-order assessment of the importance of a threat can be obtained by producing a scenario of a severe example of the threat, for users to assess how it would impact them.

Stress test scenarios are a commonly-used method of exploring the impact and risk management implications of improving resilience to different types of threat. When choosing useful scenarios for each of the different threats, it is important to ensure that they are comparable. In the framework we propose to produce scenarios that are benchmarked to the same likelihood of occurrence. To select the appropriate return period, we reviewed areas of interest by different stakeholders.

Different stakeholders clearly have interest in different return periods of risk. Corporations interested in managing operational risk are concerned about risks that are perceived to threaten business viability with return periods that range from decades to around a century[5]. Investment fund managers tend to focus in risks that manifest around the 95th percentile – i.e. a 1-in-20 year return period[6]. Insurance companies are concerned about events that threaten their ratings and financial health with return periods in the range of 50 to multiple hundreds of years, with companies purchasing reinsurance to cover losses that might occur with return periods such as 150 years, 250 years, or 450 years[7]. Solvency II regulations, due for implementation in Europe in 2015, require insurance companies to model their losses at the 99.5 percentile – i.e. the 200 year return period[8]. Large reinsurers are known to espouse risk management philosophies that ensure financial security at the 1-in-1000 year event.

For the risk framework we selected the 1% annual probability of exceedance – i.e. 100 year return period for a standard benchmark. We are also interested where possible, in defining the 0.1% (1,000 year return period) magnitude, but the development of scenarios for the 1,000 year events is of much lower priority. Our proposed standard stress test scenarios for each threat class developed for the risk framework will be standardized on the 1-in-100 year return period. In reality this is a highly approximate assessment of this order of magnitude, rather than any precise assessment. The intention is simply to ensure that scenarios of different threat types are not widely dissimilar in their likelihood.

For example a scenario of the worst infectious disease epidemic likely to be experienced with a 100 year return period (1% probability of exceedance per year) should be compared with the impact of a scenario of a trade embargo that is of a similar rarity, assessed as a 1-in-100 (1%) probability of occurring.

It is worth noting that the taxonomy of threats lists over 50 different types of macro-catastrophes. It should ultimately be possible to define a scenario to represent the 1% annual probability event for each of them. If they could be assumed to be independent, then a company could reasonably expect to have to manage one of these scenarios about once every two years. The collective probability of the

---

[5] Survey of Chief Risk Officers, perception of risk and threat probability levels of concern. Gary Bowman to provide reference.

[6] Value-at-Risk models and investment downgrade probabilities are commonly managed to the 95th percentile over an annual cycle. RiskMetrics (2010).

[7] Return periods of interest in insurance risk management, Lloyds (2005);

[8] Solvency II requires European insurers' internal models to provide solvency capital requirement calculations for the 99.5%ile (i.e. 200 year return period). CEIOPS (2010).

scenario suite may be an important factor in developing robust business systems to survive these frequent extreme shocks.

A suite of scenarios for standard return periods for each threat type is proposed.

1.5 Expecting the Unexpected

Common practice in risk management is to prepare for future crises by using illustrative scenarios. Scenarios tend to be used to develop 'resilience' in the systems being managed and so it is sometimes argued that the choice of scenarios is less critical than observing and addressing the failure modes that result. This point of view acknowledges that the failure modes addressed depend on the scenarios chosen but hopes that the main weaknesses of the systems under management will emerge from exploring a limited number of arbitrary or ad-hoc scenarios.

It is also usually acknowledged that scenarios cannot and will not accurately anticipate the next future crisis, so choosing scenarios is at best a token exercise. It is commonly claimed that future crises are unforeseeable, and that the world's complexity means that catastrophic failures and disruption arises from randomness with too many potential future permutations to consider. Some have even argued that any kind of expectation and preparedness for future crises is of minimal usefulness, highlighted in the theory of the 'Black Swan' – strategic surprise from extreme events outside the realm of regular expectations, and only able to be predicted in retrospect[9].

This has led to a degree of fatalism towards threat assessment. Because it is difficult to anticipate rare crises and because very low probability events require a thorough theoretical understanding in place of a statistical dataset of historical observations, the task of rigorous evaluation of potential future threats has appeared daunting. If future events will always be unprecedented and unexpected, then expending effort on evaluating potential threats in any detail would be pointless.

However this is not the case. There are a finite number of fundamental causes of macro-catastrophe. Nearly all macro-catastrophes are caused by a process that has occurred generically before, usually in a different form, or a different location, but it is rare for a catastrophe to be completely unprecedented. The 9/11 Al Qaeda attack is cited as a 'Black Swan' example, and clearly the scale and sophistication of that particular event, and the political and economic consequences, was unexpected by almost everyone. But terrorism and acts of political violence have been recorded for centuries. A taxonomy of threats might identify the fundamental cause – in this case terrorism – but may not be able to encompass the detailed manifestation or severity of all the potential events that can transpire from this cause. Nevertheless knowing that terrorism is a category of phenomena with potential for destructive acts is a better formulation of the risk landscape than one that ignores it.

There are very few incidences of some entirely new phenomenon. Macro-catastrophes reappear throughout history in various different manifestations, in different places, and with different characteristics, but from similar recurring underlying processes. The fact that they are 'unexpected' is more to do with human perception and short memories than to a unique new process occurring.

1.6 Updating Catastrophe Characteristics

The characteristics of any macro-catastrophe event when it occurs is always different, and unique to the location, circumstances that prevailed at that point, and the systems, technologies and assets that were affected during that period of history. The differences in characteristics from previous manifestations are the real attributes of surprise that turn them into global shocks.

---

[9] Taleb (2010).

Translating the mechanism of cause into the likely outcomes that would result today is an exercise of scientific study, imaginative analysis, and methodical modelling. An infectious disease outbreak today will travel faster through our dense urban populations and be spread more rapidly through international travel, but be more mitigated by modern medical treatments than a similar disease a century ago, but the underlying viral evolution that has produced new pandemics at intervals throughout history is an underlying causal mechanism that will give rise to more events in the future.

Today's technologies, global interconnected economies, and sophisticated financial systems have more complexity than in previous eras. Regulatory frameworks, information flows, and education levels of individual actors may mean that events can play out in very different ways than they have in the past. However the phenomena that cause the downturns, the crashes, and economic catastrophes are driven by similar causes that have recurred through history: human nature, disputes, asset value bubbles, destruction of economic value, collective distrust, and other economic fundamentals.

The proposed Cambridge threat taxonomy framework is intended to capture the fundamental causes of future catastrophes. What cannot be easily predicted is the specificity of how the next future catastrophe of this type will play out. It is possible to illustrate possible ways that a catastrophe of that type and that severity could play out, and possibly even describe the range of variables that could influence the event. The Cambridge framework is intended to result in illustrative scenarios of a standardized level of likelihood for each threat type, but not exhaustive enumeration of all possible manifestations of catastrophes that could result.

1.7 A New Generation of Catastrophe Risk Modelling

More formal processes could potentially be used to explore the entire range of catastrophe outcomes, and might be considered in future refinements. Techniques for this have for example been developed for use in probabilistic catastrophe modeling, a well-established branch of stochastic mathematical modeling used in the insurance industry and elsewhere. In these, a particular type of catastrophe, for example hurricane catastrophe risk in southeastern United States, is explored through stochastic simulation of all major variables that influence the landfall location, central pressure, radius of the storm and other characteristics of destructiveness of this particular type of natural catastrophe. These provide a good understanding of the 'landscape of risk' – risk relativities, concentrations, elements most at risk, and overall metrics of loss likelihood – that feed into risk management decisions. Probabilistic catastrophe models are routinely used by insurance companies for risk management of property and casualty insurance portfolios for a range of natural catastrophe perils, such as hurricanes, earthquakes, coastal and riverine flooding, windstorms, tornado and hail, tsunami, volcanoes, wildfire and others. Models have been developed for terrorism and industrial accidents. In life and health insurance, probabilistic models have been developed for pandemic excess mortality risk and longevity risk (the risk of a population greatly exceeding the life expectancy assumed in pension liability reserving).

The current generation of catastrophe models are focused on a specific geographical market and mainly focus on direct losses that might be inflicted on exposures in that region. There is a growing realization that extreme events can cause indirect losses and consequential impacts on business systems and even insured exposures far beyond the geographical areas affected by the event. Events that can cause disruption to business operations, supply chains, trading links, communications and executive travel, creditors and commercial counterparts, markets served, and the macroeconomic environment are becoming of increasing concern for global businesses. New generations of catastrophe models are being developed to assess risks to global business networks, and to estimate how effects might propagate through the macroeconomy and even influence the financial markets and investment portfolios. A holistic description of the full range of potential threats is essential for this new generation of models.

2 Definition of a Macro-Catastrophe Threat

A 'threat' is defined as a potential cause of a socio-economic catastrophe that would threaten human and financial capital, damage assets, and disrupt the systems that support our society, with an ability to impact on an international or global scale.

2.1 Criteria for inclusion

Threshold criteria are used to qualify a threat type. Criteria are intended to eliminate smaller types of threat that might cause localized severe impacts but not register on a global scale. The thresholds are proposed to help prioritize the focus and resources of the System Shock project.

The criteria are that an event of this type has occurred in the past 1,000 years, or could occur somewhere in the world with an annual likelihood of greater than 1-in-1,000 (0.1%), with impacts in a single year above at least one of the following minimum thresholds:

Human Injury:	Kill more than 1,000 people or injure or make seriously ill more than 5,000 people
Disruption:	For a major region or nation, or for a particular international business sector, it would cause normal life patterns and commercial productivity to be substantially interrupted for more than one week.
Cost:	Physical destruction of property and infrastructure costing $10 billion to replace, or similar level of loss of value of assets
Economic impact:	At least one country loses at least 1% of Gross Domestic Production

There are many different dimensions of ways that catastrophes impact our society. Different threats cause impacts that are more severe in some dimensions than others. Some threats like Disease Outbreak cause more human deaths and injury than other impact types, with disruptions and costs arising from the human impact. Other threats, like Cyber Catastrophes, may cause no human injury but have a significant impact in disrupting business activities and causing high levels of cost.

The different dimensions of impact are not equivalent, and no attempt is made within the framework to draw equivalences between them. The impact of each threat type and the scenarios that are developed from it are considered independently. The thresholds for inclusion are simple indicators of events that might be considered significant, in one way or another. Events that achieve none of these thresholds are not included in the taxonomy.

3 Methodology and Data Sources

3.1 Chronological histories

The taxonomy of threats has chiefly been developed through an extensive historical review. The first iteration of the project (threat taxonomy version 1.0) reviewed events of the 21st, 20th and second half of 19th century – a review period of around 160 years. The second iteration (to produce the current threat taxonomy version 2.0) extended this review back as far as 1000 AD.

The research employed factual chronological catalogues of events of historical political and social significance, documented by year[10].

[10] Source catalogues reviewed included History Mole (http://www.historymole.com); History Orb (http://www.historyorb.com); Timelines of early modern history such as

As the chronological catalogues were reviewed year by year, disruptive events fitting the criteria were identified and attributed to a cause using a loose labelling. A long-list of categories were initially identified using loose labelling, which were then reclassified into a more refined grouping of threat categories. Events were not always easily identifiable as threats that fitted the threshold definition criteria. The economic criteria were difficult to establish for any early history events but in these cases an inclusive approach was taken and if the event appeared significantly disruptive it was included.

3.2 Disaster catalogues

In addition to chronological histories, catalogues of past disruptive events, disasters, and catastrophes were reviewed. There are a number of different types of catalogues available such as

- The Centre for Research on the Epidemiology of Disasters (CRED)[11];
- Thematic briefs and the event catalogue of the United Nations Office for Disaster Risk Reduction[12] and the United Nations Development Programme Disaster Risk Reduction[13]; which also produces guidelines for establishing disaster loss databases[14].
- World Bank Global Facility for Disaster Reduction and Recovery[15].
- Catalogues of catastrophic events, focused on, but not exclusively documenting those that cause loss to the insurance and reinsurance industry maintained by major reinsurers such as Swiss Re[16] and Munich Re[17].
- Organizations such as the UN's Humanitarian Early Warning Service[18] monitor and publish ongoing crises and early warning indicators worldwide, and maintain a database of past events.
- Global Risk Information Platform maintains a meta-catalogue of disaster databases[19].
- In addition there are several organizations that develop communities of risk management professionals who publish case studies, hold conferences on disaster mitigation and recovery, and act as information repositories. Organizations such as the Global Risk Forum at Davos[20]

(https://en.wikipedia.org/wiki/Timeline_of_early_modern_history) and Middle Ages (https://en.wikipedia.org/wiki/Timeline_of_the_Middle_Ages)

11 The catalogue maintained by the Centre for Research on the Epidemiology of Disasters (CRED) has a special focus on public health and epidemiology. http://www.cred.be/

12 United Nations Office for Disaster Risk Reduction http://www.unisdr.org/

13 The Disaster Risk Reduction unit of the United Nations Development Programme (UNDP) publishes project briefs and coordinates disaster catalogues by region and institution. http://www.undp.org/content/undp/en/home/ourwork/crisispreventionandrecovery/focus_areas/climate_disaster_risk_reduction_and_recovery/

14 UNDP, 2009, *Guidelines and Lessons for Establishing and Institutionalizing Disaster Loss Databases*; http://www.undp.org/content/dam/undp/library/crisis%20prevention/disaster/asia_pacific/updated%20Guidelines%20and%20Lessons%20for%20Estabilishing%20and%20Institutionalizing%20Disaster%20Loss%20Databases.pdf

15 World Bank Global Facility for Disaster Reduction and Recovery maintains a knowledge center of resources on past projects and studies of the effects of disasters on economic growth. https://www.gfdrr.org/KnowledgeCenter

16 Swiss Re maintains *Sigma* a quarterly report on the insurance industry, including cataloguing important loss events, and maintains an annual report of natural and man-made disasters. http://www.swissre.com/sigma/

17 Munich Re maintains *Topics* newsletter reporting significant disasters worldwide, and publishes important retrospectives and analysis, such as Natural Hazards database and world map. https://www.munichre.com/touch/portal/en/service/login.aspx?ReturnUrl=%2ftouch%2fpublications%2fen%2flist%2fdefault.aspx%3fcategory%3d17&cookiequery=firstcall

18 UN's Humanitarian Early Warning Service http://www.hewsweb.org/hp/

19 A meta-catalogue of disaster databases is maintained by the Global Risk Information Platform (http://www.gripweb.org)

20 Global Risk Forum at Davos http://www.grforum.org/

organize the Global Platform for Disaster Risk Reduction and the International Disaster and Risk Conference.

3.3 Counter-factual evidence and scientific conjecture

In addition to identifying historical precedents of past events, the list was supplemented by a literature review of scientific argument for potential future catastrophes that may not have been manifested in the experience of the past millennium.

Some types of threats are counter-factual – i.e. they did not actually occur but potentially they could have done with minor changes in circumstance. These are 'near-miss' events. For example the worst historical example of a nuclear power plant meltdown, Chernobyl, USSR, 1986, released 10% of its inventory, approximately 5,200 petabecquerels. The Nuclear Regulatory Commission of United States anticipates scenarios for much more severe events than this, with up to 60% release of a nuclear power station's inventory[21]. Similarly there has never been an example of two nuclear-armed adversaries using nuclear weapons in conflict, but history relates that the 13-day Cuban Missile Crisis of 1962 brought such a scenario perilously close. The proposed taxonomy of threats includes extreme nuclear power plant meltdown as a threat type, and also includes nuclear war as a 'counter-factual' threat type.

Where scientists have postulated future catastrophes that have not been seen in the past millennium, we have incorporated these where there is a legitimate debate and a significant evidence base of science that is being advanced. In this taxonomy we are not assuming that these hypotheses are proven, or to be expected, but they are included on the basis that there is uncertainty around the possibility of its occurrence, and that a conservative approach is to include them as a potential threat, with high levels of uncertainty. Uncertainty classification of the taxonomy is important, and a scale to reflect these different types and degrees of uncertainty is being considered.

A key area of scientific hypothesis about macro-catastrophes relates to uncertainties about climate change, and the potential for reaching tipping points in which rapid change may occur in parts of our environment. Examples of these include the potential for sudden and rapid ice shelf collapse bringing about sea level rise (Environmental Catastrophe: 7.1 Sea Level Rise); The potential for rapid desalination to trigger permanent shifts in ocean currents (Environmental Catastrophe: 7.2 Ocean System Change); and similar sudden and permanent changes in the flow of the jet stream (Environmental Catastrophe: 7.3 Atmospheric System Change). Scientists proposing these hypotheses cite evidence that these changes have occurred before in geological timescales, but the probability of these changes being triggered in the next few decades is highly uncertain. The proposed framework includes these potential threats, but it is intended to study these hypotheses in more detail to qualify what the 99th percentile of uncertainty might suggest as a scenario, and whether this could pose a genuine concern.

3.4 Peer review process

The taxonomy of macro-threats version 1.0[22] was subjected to peer review from October 2011 through to March 2012. The taxonomy was presented on a website with the ability for posting comments. Email postings invited the broader community of researchers and practitioners that have a relationship with the Centre for Risk Studies (a list of around 350 contacts) to review and submit

---

21 NRC publishes a regulatory guide 1.195 (2003) for 'Design Basis Accident' scenario for 60% inventory loss. http://pbadupws.nrc.gov/docs/ML0314/ML031490640.pdf

22 An archive of the original Version 1.0 threat taxonomy is available on the Cambridge Risk Framework website. http://cambridgeriskframework.com/downloads

comments and feedback. The Annual Meeting of the Centre for Risk Studies in December 2011, attended by 110 participants, was also used to present version 1.0, with an open-forum discussion topic session. Individual interviews were also held with specialists with interests in developing the taxonomy. Around 50 individual suggestions and comments were logged from this process.

The feedback was incorporated into a redesign of the Threat Taxonomy to produce version 2.0. This included better definition of thresholds for inclusion and exclusion, a restructuring of a number of categories and types, and changes in nomenclature and iconography. Individual changes that were incorporated into version 2.0 are fully documented in the threat observatory of the research website[23].

The Taxonomy of Threat version 2.0 is included as Appendix 1 at the end of this document, and is available interactively online at the Cambridge Risk Framework website[24].

4 Categorization

For a threat classification system to be useful, it has to be tractable – a manageable number of categories and classes – and wide ranging to cover as many causes of threat as possible. This means that the taxonomy consists of limited numbers of classes of threat that are necessarily large and imprecise. The intent is to capture the broad types of threats: ones that might impact our systems in different ways to the others. Some threat types could be considered as belonging to more than one category, and our peer review processes identified differences in opinion about in which category they best belong, but we have made assignments that best align with the concept of causal similarity.

4.1 Hierarchical system

For a system to be tractable and have a manageable number of categories, but also of sufficient granularity to be applied in more detail when appropriate, any taxonomy should be hierarchical and capable of subdivision to increasingly fine levels of resolution. The Cambridge taxonomy is designed as hierarchical, with two levels of typology defined initially, but further subdivision into more types is expected as detailed studies are developed.

We have identified twelve primary categories of macro-catastrophe threats, each of which is subdivided into threat types, with between three and six types in each category.

Types can be further subdivided as appropriate. For example the category of 'Political Violence' has the five types 'Terrorism'; 'Separatism'; 'Civil Disorder'; 'Assassination', and 'Organised Crime'. 'Terrorism' as a type can be further subdivided into different types of terrorism for example by the ideological motivation, such as: 'Religious Militants'; 'Left-Wing Ideologues'; 'Right Wing Militias'; 'Eco-terrorism'; 'Regional Separatists' and others. Similarly most of the threat types identified in the taxonomy can be further subdivided into variant types.

This subdivision requires domain expertise of the threat type and so at this stage we have proposed that subdivision of threat types is an activity that would be carried out by Subject Matter Editors (SMEs) in each threat category as and when required.

23 Changes incorporated into Version 2.0 of the taxonomy are documented at: http://cambridgeriskframework.com/whatsnew

24 The Cambridge Risk Framework Threat Observatory uses the threat taxonomy as the hierarchy for an information repository, including filtered news sources, listings of information resources and recommended reading, and threat profile working papers where available. http://cambridgeriskframework.com/taxonomy

4.2 Grouping by cause

There are many different ways of categorizing threats – they could be divided by systems that they affect, or by their mechanisms of harm, or by their timescales of impact, or other characteristic. We have chosen to categorize by cause.

The twelve primary categories are considered as natural groupings of the *causes* of threats. We have used a concept of 'causal similarity' to group and structure the taxonomy. Where causes are very dissimilar, then we can broadly assume that they may be independent. The assumption of independence is a very useful one for statistical manipulation and combination of events. So as a first-order assumption, the primary taxonomy threat categories can be considered to arise from causes that are broadly independent. In the section on correlation and causation, below, we consider in more detail how an event of one category could be correlated with underlying factors that would in fact make both categories more likely, or where one category could trigger a follow-on catastrophe of another category, or exacerbate its coincidental effects. However, the general structure preserves the concept of first-order independence for the initial trigger event. The hierarchy is structured by 'causal similarity' – the higher up the hierarchy, the more dissimilar the underlying causes are.

5 Threat Categories

The primary categorization is intended to capture the main causal divides in the typology of macro-catastrophe threats. A number of the primary categories are man-made threats, dealing with the social, economic and financial system extremes. These are categorized by '**Financial Shocks'**, broadly the endogenous shocks in the financial system that arise when the financial system experiences failures of internal mechanisms, information asymmetry, or market inefficiency. These are significantly different in cause to the '**Trade Disputes'** that harm international commerce and damage national economic productivity. '**Geopolitical Conflict'** is a specific process of militarized disputes between nation states and factions within countries. We have differentiated this from '**Political Violence'** processes and causes, where grievances and ideological differences cause factions to promulgate dissent and to attempt to bring about political change through asymmetrical actions.

These broad categories of 'man-made' catastrophes are considered as separate from more natural phenomena, and within these we have differentiated broadly different mechanisms of cause. So for example, '**Disease Outbreaks'** are driven by mutation processes of micro-organism pathogens, which is broadly independent of other mechanisms of macro-catastrophe, such as 'Climatic Catastrophes'. '**Natural Catastrophes'** are driven by mechanisms of geological processes and very specific conditions of meteorological cyclogenesis, and is a category of perils specifically recognized and modeled by the insurance industry. '**Climatic Catastrophes'** are extreme variants of normal weather systems, and are recognized as different mechanisms of extremes from the meteorological drivers of wind storms and floods, although clearly these have similarities. '**Environmental Catastrophes'** are a third variant of extreme weather system in encapsulating the potential catastrophic manifestations of gradual climate change processes.

The category of '**Technological Catastrophe'** has some affinity with man-made catastrophes, and some peer review feedback suggested that this might be better aligned with causes that are malevolent, but the main emphasis proposed here is that although the mechanism of harm originated from manufactured items, the causes of major historical catastrophes have been predominantly accidents of one type or another. There are examples of malevolent attempts to cause technological catastrophes, such as attacks on nuclear power stations, but these would be a subtype of the threat and could be identified as such and incorporated in the threat assessments in that way. '**Humanitarian Crises'** are catastrophes that are triggered by changes in populations, such as through mass migrations, or demographic shifts, or depletion of natural resources. Again, although there are potential links with causes of other catastrophes, and clearly geopolitical conflicts and climatic, environmental, natural, and other catastrophes can trigger humanitarian crises, these crises can also occur independently and themselves be a cause of catastrophic impacts.

'**Externalities**' are threats that arise from causes outside the earth's atmosphere, from space objects or solar ionization processes, and these are clearly independent of other catastrophic triggers.

The '**Other**' category of macro-catastrophe threats is a recognition that although the categorization has been as exhaustive as possible, there remains the potential for new causes of disruption to become recognized.

6 Correlation and Causation

6.1 Multiple Compounded Shocks

Figure 1: The Correlation and Causation Dependencies of Threat Categories.

			Consequence											
			1	2	3	4	5	6	7	8	9	10	11	12
			Financial Shock	Trade Dispute	Geopolitical Conflict	Political Violence	Natural Catastrophe	Climatic Catastrophe	Environmental Catastrophe	Technological Catastrophe	Disease Outbreak	Humanitarian Crisis	Externality	Other
Primary Trigger	1	**Financial Shock**	4	3	2	2	1	1	1	1	1	2	1	1
	2	**Trade Dispute**	3	4	2	3	1	1	1	1	1	1	1	1
	3	**Geopolitical Conflict**	3	2	4	3	1	1	1	1	1	2	1	1
	4	**Political Violence**	2	2	3	4	0	0	0	3	3	2	1	1
	5	**Natural Catastrophe**	2	2	2	1	4	2	3	3	2	2	1	1
	6	**Climatic Catastrophe**	3	2	3	2	3	4	3	2	2	3	1	1
	7	**Environmental Catastrophe**	3	2	2	2	3	3	4	2	2	2	1	1
	8	**Technological Catastrophe**	2	2	2	2	2	2	0	4	1	1	1	1
	9	**Disease Outbreak**	3	2	1	1	1	1	1	2	4	2	1	1
	10	**Humanitarian Crisis**	2	2	3	3	1	1	1	1	2	4	1	1
	11	**Externality**	3	2	2	1	3	3	3	3	2	2	1	1
	12	**Other**												

The correlation categories are:

0	The two threat types are uncorrelated, and if they occurred coincidentally, their consequences would be broadly the same as if they occurred independently
1	No mechanism for this threat to directly cause an event of the second threat type, but the consequences of a coincidental second event shortly afterwards would be made significantly worse, for example because resources would be already committed and abilities to respond and contain would be weakened
2	There is some potential for an event to contribute to the causal mechanisms that would trigger the occurrence of an event of the second type
3	An event of this type potentially can directly trigger an event of the second type
4	An event of this type potentially can directly trigger another sub-category of threat within the same threat category

The worst catastrophes are combinations of events, where a primary catastrophe causes secondary effects by triggering another 'follow-on' catastrophe. The escalation of consequences can be worse than if they had happened separately. For example the Japan Tohoku catastrophe of March 2011 was a magnitude 9.0 earthquake that triggered a 20 metre tsunami, that caused an INES level 7 nuclear power plant industrial accident. The correlations and potential causal mechanisms for one type of catastrophe to trigger another is an important element of risk assessment.

The most surprising and unexpected catastrophes tend to fall into this category of multiple compounded shocks.

The potential for one class of threat to trigger or exacerbate the effects of another threat type is considered systematically in the matrix in Figure 1. A qualitative assessment is made for the potential for one event to trigger another, categorized by the degree of causation and exacerbation that would result. Not all combinations can be related back to identifiable historical precedents, but it is possible to conjecture potential mechanisms and plausible scenarios where one catastrophe can lead to another.

7 Precedents

There are a number of other frameworks and classification systems for considering macro-catastrophes. Each has merits and limitations.

7.1 WEF Global Risks Report

The World Economic Forum has been publishing a review of Global Risks[25] annually since 2005. Risks are structured into Economic, Environmental, Geopolitical, Societal, and Technological. It develops a listing of global risks in terms of impact, likelihood and interconnections, based on a survey of experts from industry, government and academia. The annual review makes this a useful guide to the changing perceptions and importance assigned to the risks identified. The framework is derived from expert opinion and is crowd-sourced from a broad range of analysts.

[25] The 2013 version of the WEF Global Risk Report is available http://reports.weforum.org/global-risks-2013/

7.2 OECD Global Future Shocks project

The OECD Global Future Shocks project[26] presents a framework for understanding systemic risks and profiles five leading threats: Pandemic; Critical Infrastructure Disruption from a cyber attack; Financial Crisis; Geomagnetic Storm; Social Unrest. It focuses on how the direct and secondary critical infrastructure disruptions can occur, and measures to prepare for these future shock scenarios. The working definition of future global shocks is: "a rapid onset event with severely disruptive consequences covering at least two continents."

7.3 UK Government National Risk Register

The UK Government Cabinet Office publishes a National Risk Register for Civil Emergencies[27]. This is a taxonomy of risks of civil emergencies in the UK or to UK interests. These are divided into malicious attacks and other risks, and considered on a matrix of likelihood vs impact scale. The highest priority risks are defined as Pandemic influenza; Coastal flooding; Catastrophic terrorist attacks; Volcanic eruptions abroad; Severe wildfires. This is the public version of a classified National Risk Assessment of over 100 different scenarios for civil authority preparedness.

7.4 Australian Government National Risk Assessment Framework

The National Risk Assessment Framework[28] was designed to improve risk management practices for the emergency management sector and to foster consistent base-line information on emergency risks. The natural hazards covered in the framework are bushfire, earthquake, flood, storm, tropical cyclone, storm surge, landslide, tsunami, tornado and meteorite strike.

8 Applications

A standardized definition of a taxonomy of macro-catastrophe threats has a number of different uses in areas of business risk. Macro-catastrophes impact individual companies, but more significantly they impact multiple companies at the same time, and produce systemic effects across the whole macro-economic environment, producing potential impacts on the financial system and investment assets. As such there are many stakeholders in ensuring that these macro-catastrophes are well understood and that their risks are managed. Each set of stakeholders is likely to use the taxonomy in different ways to assess and manage their risk.

The proposed taxonomy framework includes a standardized structure for defining threats and a standard data structure for defining a scenario for various risk stakeholders.

8.1 Insurance risk management

Insurance companies have the potential to be impacted by a macro-catastrophe in at least three important dimensions – underwriting, operational, and investment risk. The threat taxonomy provides a systematic framework for identifying which threats an insurer is best able to manage, for identifying the threats that insurers are less familiar with, and for monitoring emerging or changing risks that might pose a new threat to the insurer's balance sheet. Where categories of threats are

---

26 OECD Global Future Shocks report http://www.oecd.org/governance/48256382.pdf

27 UK National Risk Register of Civil Emergencies 2013 Edition https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/211867/2900895_NationalRiskRegister_acc.pdf

28 Australian Government, Geoscience Australia, National Risk Assessment Framework http://www.ga.gov.au/hazards/governance/policy/national-risk-assessment-framework.html

identified that an insurer has less familiarity with, the potential impact of these can be explored through illustrative scenarios for each threat, as described above (1.3.2).

Insurers also recognize the shifting demand of global corporations for protection against macro-catastrophic threats to their international businesses. Some emerging threats that are of concern to global businesses – such as cyber risk, business interruption from pandemics, or contingent business interruption from multi-cause perils - may be areas that insurers could offer new products and services around if the insurer can get comfortable with the understanding of the threat, identify the ‘fire-breaks’ and limits to loss, and develop sufficient underwriting expertise about the peril. Some threats identified in the taxonomy are no longer easily accommodated in traditional insurance products of peril-specified direct-loss coverages. Some threats cannot be easily managed in geographical accumulation zones. There may be potential for new classes of insurance business and new approaches to product designs that could arise from a framework approach to the global threat landscape and the risk posed to the interconnectivity and dependencies of modern business systems.

Insurers are familiar with stress test scenarios and they use a wide variety of hypothetical models of threat situations, ranging from estimates of probable maximum loss from ‘design events’, to realistic disaster scenarios, stochastic event sets of catastrophe models, and regulatory solvency capital tests.

The scenarios being developed to populate the taxonomy of threats are being designed to help manage insurers’ risks in the following areas:

8.1.1 Underwriting risk

Firstly an insurer may experience underwriting loss – i.e. see a large number of claims be made on the insurance policies they write and in some of these macro-catastrophe events, there is the possibility that losses could occur across a large number of different lines of business in ways that might be unexpected. The scenarios are being developed so that the consequences of a threat can be assessed to each major line of insurance business. A standard data structure is proposed for a threat scenario that will capture a loss estimation across multiple lines of insurance business. Table 1 provides a listing of proposed categories of lines of insurance business to be included in the scenario impact assessment.

Table 1: Standard scenario impact assessment categories for lines of insurance business

Non-Life - P&C
- Property
- Casualty & Liability
- Contingent Business Interruption
- Specialty
- War & Political Risk
- Aerospace
- Aviation
- Agriculture
- Energy
- Marine & Specie

Life & Health
- Life
- Health
- Accident & Disability
- Annuity & Pensions

Financial
- Trade Credit
- Counterparty Risk
- Equity investments
- Bond investments
- Foreign Exchange investments

Applications of scenarios that are being developed include checking policy wordings, terms and conditions, and insurance product coverages, and estimation of the scale of potential losses.

8.1.2 Operational risk

Secondly the same event could impact the business operations of the insurance company itself, causing issues with operating processes, payment systems, welfare of staff, and potentially affecting business counterparts, suppliers and partners it deals with. Scenarios are intended to provide checklists or information to assist insurance companies how they would be impacted operationally by the events described in the scenarios. The structure for assessing the operational risk is to describe timelines and phases in the progress of the scenario that would have business operational implications and to develop estimates of impacts to the macroeconomic environment, for a standardized listing of economic sectors, as listed in Table 2.

Table 2: Standard scenario impact assessment categories for macroeconomic sectors.

11	Agriculture, Forestry, Fishing and Hunting
21	Mining, Quarrying, and Oil and Gas Extraction
22	Utilities
23	Construction
31	Manufacturing
42	Wholesale Trade
44	Retail Trade
48	Transportation and Warehousing
51	Information
52	Finance and Insurance
53	Real Estate and Rental and Leasing
54	Professional, Scientific, and Technical Services
55	Management of Companies and Enterprises
56	Administrative and Support and Waste Management and Remediation Services
61	Educational Services
62	Health Care and Social Assistance
71	Arts, Entertainment, and Recreation
72	Accommodation and Food Services
81	Other Services (except Public Administration)
92	Public Administration
00	General Population
ZZ	Defence

Coding uses standard categories from the Standard Industrial Classification (SIC)[29], or its equivalent in the UN Standard International Trade Classification (SITC)[30], or the equivalent in the North America Industry Classification System (NAICS)[31]. Coding translations can also be applied[32].

8.1.3 Investment risk

Thirdly the event could be so severe that it causes losses on financial markets and devalues the equities and bond assets in the insurer's investment portfolio. The scenario structure is intended to capture potential impacts from the portfolio on broad classes of investment assets, as listed in Table 3.

Table 3: Standard scenario impact assessment categories for investment portfolio assets

[29] Full coding structure for the Standard Industrial Classification (SIC), a UK standard, can be found at http://www.siccodesupport.co.uk/.

[30] Coding for Standard International Trade Classification (SITC), a UN international standard, is provided at http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=14;

[31] Coding for North America Industry Classification System (NAICS), a US standard, is provided at http://www.census.gov/eos/www/naics/;

[32] Ttranslations between SIC, SITS, NAICS and other codings can be obtained at http://dataweb.usitc.gov/classification_systems.asp.

Equities

- US Equities
- UK Equities
- EU Equities
- Japanese Equities
- Asia ex-Japan Equities
- US Small Cap Equities
- Emerging Markets Equities

Bonds

- US Government Bonds (ave 7 yr duration)
- UK Government Bonds (ave 7 yr duration)
- European Gov Bonds (ave 7 yr duration)
- Japan Gov Bonds (ave 7 yr duration)
- Corporate Bonds
- High Yield Bonds

Other Exchange Traded

- Property Index
- Private Equity
- Gold Commodities
- Other commodities
- Cash LIBOR 1 Month

For a specified stress test scenario in the framework, it is proposed that consequence analysis provides outputs to enable insurance companies to

a. estimate their underwriting losses across all of the relevant lines of business that might be impacted

b. evaluate how the scenario will cause operational impacts, and impair the macroeconomic environment

c. derive indicative estimates of how a scenario is likely to impact an investment portfolio.

The scenarios are designed to provide holistic business stress tests for internal risk management in insurance companies.

8.2 Business operational risk management

The taxonomy framework provides a checklist of threats that could cause disruption to international business operations. Many businesses today maintain an 'emerging risks' committee or monitoring process. The systematic framework provided by the taxonomy provides a structure to monitoring the emerging risks of interest. The structure is useful if the scenarios can be used to simulate threats and develop disaster preparedness measures and contingency plans for business operations. Adapting the scenarios to ensure that they are useful for preparedness planning is an objective of the research.

It would also be useful for businesses if the taxonomy framework provided indices of the current (and projected short term future trend) threat level for each and all of the threats, as early warning systems to assist with preparedness. The possibility of developing indices is currently being explored.

8.2.1 International Supply Chains

Global business systems are particularly encapsulated in international supply chains. The science of managing international business networks has rapidly evolved, transforming global supply chains into highly efficient backbones of modern business. But the drive for cost reduction has also reduced safety margins and increased the potential for systemic failures from extreme events. Current best-practice in supply chains recognizes how failures might occur, and develops efficient resiliency in operations and system design to optimize protection for the business. Supply chain interruption has become a major concern of global businesses, with disruptions causing serious impacts on a company's long run performance and equity risk. Top executives consider supply chain disruption to be one of the greatest areas of concern in running their business. Managers are increasingly refining their focus on efficiency to incorporate safety margins and incorporate measures to improve the resilience of supply chain operations – i.e. investing in just-enough safety margin to make a significant improvement on disruption, but not over-investing in wasteful measures. Analyzing and quantifying the value of resilience is an emerging area in the study of operations management.

Shock scenarios from the taxonomy framework have been used to test the resilience of international supply chains[33], and are a particular application of the Cambridge Risk Framework[34]. Research continues into modeling the impacts of scenarios in disrupting international supply chains, designing supply chains with 'efficient resiliency', and quantifying contingent business interruption resulting from macro-catastrophe events.

8.3 Government National Security

A systematic risk framework also enhances efforts by national governments to provide contingency planning for future threats to national security, for energy, food and natural resources security, and for civil defense resource allocation[35]. Prioritizing resources for civil emergences requires a systematic assessment of the frequency, severity and characteristics of the threats faced, along the lines of the structure proposed in the Cambridge Risk Framework. Scenarios developed in the framework would be useful if they can provide estimates of casualties, civil disturbance, damage to essential lifelines, transportation systems, utilities, and other inputs into the assessment and planning of the resources needed for public health, law and order, essential services, and humanitarian needs.

8.4 Financial Risk Management

The proposed taxonomy of threats is a rigorous catalogue of exogenous financial shocks, The framework also incorporates the purely endogenous shocks of the financial system itself: Threat category #1. Financial Shock is allocated to the endogenous types of financial threats, such as asset bubbles, bank runs, sovereign defaults etc.

Since the financial crisis of 2007-9, there has been considerable focus on understanding the mechanisms, causes, and propagation of financial crises in order to improve risk management for future crises. Few areas of economic and financial risk management have been untouched by changes that have been made in assessing asset and market risk, economic risk capital requirements, regulatory and supervisory changes, credit ratings, and acceptable levels of sovereign debt.

Much of the focus of economic and financial research that has underpinned these changes has been on credit withdrawal, liquidity evaporation, complexity economics, and the systemic risk to banking networks from asset bubbles, bank runs, market crashes and other macroeconomic phenomena. These are commonly referred to as *endogenous* shocks, where the financial system experiences failures of internal mechanisms, information asymmetry, or market inefficiency.

A comprehensive view of macroeconomic risk also incorporates *exogenous* shocks – major events from outside the financial system, typical unexplained by economics alone, that can destabilise the system or exacerbate a fragile economic environment. Historically, more financial crises appear to have been the result of endogenous processes than from pure exogenous shocks. The contribution of exogenous shocks appears minor but significant: a small number of crises have been directly triggered by geo-political events and other major crises may have been exacerbated by external events.

The threat taxonomy proposes a systematic structure for assessing all the likely causes of exogenous financial shocks to help investment risk managers estimate the statistical distributions of economic

33 A demonstration of the application of a System Shock scenario to an international supply chain is provided on the research platform: http://cambridgeriskframework.com/page/22

34 Ralph et al., (2012) 'Resilient International Supply Chains', Centre for Risk Studies, University of Cambridge.

35 An example is the UK Government National Risk Assessment, cited earlier in this paper.

risk. The scenarios being developed also explore the structural propagation of financial impacts from the macroeconomic loss to their influence on simplified investment portfolios, as outlined in Table 3. This helps financial risk managers consider portfolio optimization strategies that will mitigate the impacts of future exogenous shocks.

9 Conclusions

A taxonomy of macro-catastrophe threats has been proposed to assess the risk of events that have the potential to cause damage and disruption to social and economic systems in the modern globalized world. To use this effectively in risk management, the threats identified in the taxonomy have to be translated into effective tools for managers to assess their exposure to them. We propose that the development of scenarios, linked with a review of the state-of-science about the threat, is a key part of achieving this. The development of scenarios for use in business risk management requires an agreed standardization of approach, methodology, and data architecture. This is the next stage of developing useful risk management tools that will improve society's ability to cope with the inevitable threats to our globalized business systems in the years ahead.

10 Acknowledgements

The research work on developing the Cambridge Risk Framework has been supported by a number of companies, primarily Deloitte, RMS, Catlin, HSBC, Lockheed Martin and Munich Re, academic partners including the Institute of Catastrophe Risk Management at Nanyang Technological University Singapore, and by many individuals and colleagues through their participation in workshops, interviews and the peer review process, but the Centre for Risk Studies would like to particularly acknowledge the contributions of Trevor Maynard, head of exposure management and reinsurance team at Lloyd's, and Dr. Dougal Goodman of the Foundation for Science & Technology.

11 References

UK Government, 2010, National Risk Register of Civil Emergencies 2010 edition, Cabinet Office. http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/media/348986/nationalriskregister-2010.pdf

OECD, 2011, Future Global Shocks: Improving Risk Governance; OECD Reviews of Risk Management Policies, OECD Publishing, ISBN: 9789264095205 ; http://www.oecdbookshop.org/

World Economic Forum, 2013, Risk Interconnection Map; http://www.weforum.org/documents/riskbrowser2010/risks/

Bracken, Paul; Bremmer, Ian; Gordon, David; 2008; Managing Strategic Surprise: Lessons from Risk Management and Risk Assessment, Cambridge University Press. ISBN:9780521709606

Blong, Russell, 2013, 'Pear-Shaped Phenomena: Low Probability, High Consequence Events', 13th Aon Benfield Hazards Conference, September 2013.

Taleb, Nassim Nicholas; 2010, The Black Swan: The Impact of the Highly Improbable, Allen Lane, ISBN: 978-1846145650.

Sornette, Didier, 2009, 'Dragon-Kings, Black Swans and the Prediction of Crises'; International Journal of Terraspace Science and Engineering. http://arxiv.org/ftp/arxiv/papers/0907/0907.4290.pdf

Ralph, D.; Bowman, G.; Coburn, A.; Ruffle, S., 2012, 'Resilient International Supply Chains', Centre for Risk Studies, University of Cambridge, Working Paper 201212.01 http://cambridgeriskframework.com/uploaded/documents/Resilient_International_Supply_Chains.pdf

UNDP, 2009, Guidelines and Lessons for Establishing and Institutionalizing Disaster Loss Databases; UNDP Regional Programme on Capacity Building for Sustainable Recovery and Risk Reduction.

http://www.undp.org/content/dam/undp/library/crisis%20prevention/disaster/asia_pacific/updated%20Guidelines%20and%20Lessons%20for%20Estabilishing%20and%20Institutionalizing%20Disaster%20Loss%20Databases.pdf

CEIOPS, 2010, 'Solvency II Calibration Paper', CEIOPS-SEC-40-10, Committee of European Insurance and Occupational Pensions Supervisors, 15 April 2010. https://eiopa.europa.eu/fileadmin/tx_dam/files/publications/submissionstotheec/CEIOPS-Calibration-paper-Solvency-II.pdf

Appendix 1: Taxonomy of Macro-Threats

	Category	ID	Title	Description	Historical Examples
1	**Financial Shock** **Events in the financial system causing short-run fluctuations and/or significant changes in long-run economic growth**	1.1	**Asset Bubble**	Pricing inflation and sudden collapse for a major sector or asset class	Sub-Prime Property bubble 2008; 'dot-com' bubble 1999; South Sea bubble 1720; Amsterdam Tulip bubble 1637
		1.2	**Financial Irregularity**	Corporate or accounting fraud; Rogue trading; Ponzi schemes; or other major irregularities	Worldcom 2002; Enron 2001; Jerome Kerviel (Societe Generale) 2008; Nick Leeson (Barings Bank) 1995; Bernard Madoff ($18 Bn ponzi scheme) 2009
		1.3	**Bank Run**	Bank failure; Credit default for major banks, banking system or market participant	Lehman Brothers 2008; Bear Sterns 2008; IndyMac 2008; Northern Rock 2007; U.S. Savings and Loan crisis 1980s/1990s
		1.4	**Sovereign Default**	Debt default, currency devaluation or government failure and/or change	Greek sovereign debt crisis 2010-; Argentina crisis 1999-2002; Russian crisis and LTCM 1998; Black Wednesday (UK withdrawal from ERM) 1992; Repudiation of Confederate debt (post US civil war) 1864
		1.5	**Market Crash**	Extreme correlated mass movement of share prices , possibly driven by information or perception about economic fundamentals	May Flash Crash 2010; Black Monday Stock Market crash 1987
2	**Trade Dispute** **Events causing widespread change or disruption to international trading conditions**	2.1	**Labour Dispute**	Strikes, mass refusal of employees to work, or picketing by aggrieved workforce to prevent commercial activity	International Labour Workers Union (ILWU) work-to rule slowdown 2002; UK Miners' strikes 1984-85; US West Coast waterfront strike 1934; UK General strike 1926; Dublin lock out 191
		2.2	**Trade Sanctions**	Country-to-country trade embargos denying entry or passage of commercial goods and services	Russia-Ukraine (Gazprom dispute disrupts gas supplies to Europe) 2009; US-EU ('Banana trade war') 1999; US-Cuba 1960
		2.3	**Tariff Wars**	Protectionism through the imposition of taxation of a particular set of goods or services	US tax on Chinese tyres 2009 (reciprocated by Chinese tax on US Chicken imports); US Steel tariff 2002 (withdrawn after EU threatens reciprocal tariff on Florida oranges and Michigan cars)
		2.4	**Nationalization**	Sovereign appropriation of foreign-owned assets in that country	Icelandic banks 2008; Venezuela (seizes operational control of Orinoco belt) 2007; Cuba (nationalises all foreign-owned companies) 1959; Egypt (nationalises Suez canal) 1956
		2.5	**Cartel Pressure**	Trading bloc of suppliers applies pricing or supply pressures	NAFTA Tortilla crisis 2007; Opec Oil Crisis 1973; DeBeers monopoly and Diamond syndicate 1889

3 Geopolitical Conflict **Military engagements and diplomatic crises between nations with global implications**	3.1	**Conventional War**	The engagement of two or more nations in military conflict, using conventional weapons to target military infrastructure and invade/defend sovereignty	Gulf War II Iraq 2003; Gulf War Kuwait & Iraq 1990-91; Falklands War 1982; World War II 1939-4
	3.2	**Asymmetric War**	Military action, insurgency and violent resistance carried out between combatants of significantly different power, resources, and interests	Iraqi insurgency resistance to the occupation of US forces from 2003; Afghanistan insurgency resistance to occupation forces of US and allies from 2001; Colombian guerrilla war 1963+
	3.3	**Nuclear War**	Military Conflict pursued using nuclear weapons	Bombing of Hiroshima and Nagasaki in Japan 1945; Near-misses include Cuban missile crisis 1962
	3.4	**Civil War**	Internal conflict within a country, including wars of succession and coups d'etat	Libya civil war 2011 (coup 1969); Sri Lankan civil war 1983-2009; Darfur, Sudan 2009; Rwanda 1990-93; Bosnia 1992-95; Russian coup 1993; American Civil War 1861-65
	3.5	**External Force**	Blockades, No-Fly zones, missile attack or other military action by external forces to prevent national authorities pursuing internal policies deemed harmful or repugnant	Libya (No Fly Zone) 2011; Israeli sea and land blockade of the Gaza Strip, since 2000; Iraq (NFZ) 1991-2003; Bosnia and Herzegovina (NFZ) 1993–95; Egyptian blockade of Straits of Tiran to Israel-bound ships (1956-57)
4 Political Violence **Acts or threats of violence by individuals or groups for political ends**	4.1	**Terrorism**	Politically-motivated single or coordinated attack(s) to inflict societal and/or economic fear and disruption	2001 World Trade Center Attack by Al Qaeda; Sarin gas attack on Tokyo Subway by Aum Shinrikyo; London July bombings 2005; Mumbai shooting massacre 2008; Beirut US barracks bombing 1983
	4.2	**Separatism**	Sustained campaign of violence for regional independence	Sri Lanka, Tamil Tigers 1983-2009; Russia-Chechnya 1990-2009
	4.3	**Civil Disorder**	Riots and civil disobedience, through to uprisings and revolutions	Arab Spring 2011; France banlieues riots 2005; Palestinian Intifada 2000-; Fall of Berlin Wall 1989
	4.4	**Assassination**	Assassination of a major political leader	Benazir Bhutto 2007; Yitzhak Rabin 1995; Anwar Sadat 1981; Attempt on Ronald Reagan 1981; John F. Kennedy 1963; Czar Nicolas II 1918; Franz Ferdinand 1914
	4.5	**Organized Crime**	Crime waves, Campaigns of criminal extortion, piracy, or mass illegal activities that debilitates commercial activity	Somalia Piracy in Horn of Africa 2005-2010; Mexican Drug War 2006; Piracy Malacca Straits 2004; First Mafia war, Italy, 1962

5	**Natural Catastrophe** **Naturally occurring phenomena causing widespread damage and disruption**	5.1	**Earthquake**	Seismic fault rupture causes high levels of damage to infrastructure of a major populated area	Tohoku, Japan 2011; Kobe, Japan 1995; Northridge, California 1994; Great Kanto earthquake, Japan 1923; San Francisco 1906; Northridge, California, 1994
		5.2	**Windstorm**	Hurricane/typhoon/cyclone wind system makes landfall onto a major populated area; European-type windstorm system, large scale, fast-moving, gale force wind speeds	Hurricane Katrina, USA, 2005; Hurricane Andrew, USA, 1992; European Windstorm Lothar 1999; Typhoon Mireille, Japan, 1991
		5.3	**Tsunami**	Coastal impact of a tidal wave, caused by offshore earthquake, marine landslide, or meteorite in the sea,	Boxing Day Tsunami 2004; Japan Tohoku tsunami 2011
		5.4	**Flood**	River Flood from high rainfall/sudden water release across one or more river systems; Coastal Flood from sea surge caused by low pressure weather systems, exceptional tides and extreme winds	River: Queensland Australia 2011; Coastal: East Coast UK 1953
		5.5	**Volcanic Eruption**	Ash, pyroclastic hot gasses, lava, and lahar-triggered mudflows cause localized destruction and regional disruption	Ash eruption of Eyjafjallajökull, Iceland 2010; Pinatubo eruption, Philippines, 1990
6	**Climatic Catastrophe** **Climatic anomalies or extremes causing severe and unusual weather conditions**	6.1	**Drought**	Extended period of below-average precipitation	Horn of Africa 2011; Texas, US 2011; Australia 1994; Europe 1976; Sahel, Africa 1960s-; China 1941; US 'Dust Bowl' 1931-38
		6.2	**Freeze Event**	Extended period of below-average temperatures	UK 2010; Moscow; Russia 2010; North American Ice Ice Storm 1998; Idaho Ice Storm 1961
		6.3	**Heatwave**	Extended period of above-average temperatures	US 2011; Russia 2010; France 2003; Chicago 1995; US 1980
7	**Environmental Catastrophe** **Crises leading to significant and widespread change to environmental or ecological equilibriums**	7.1	**Sea Level Rise**	Thermal expansion of the oceans or sudden ice shield melt changes coastline geography	Interglacial sea level rises in previous epochs
		7.2	**Ocean System Change**	Sudden switch in the circulatory systems of the ocean, such as the Gulf Stream, caused by salination or thermal changes, causes regional climatic change	Broecker' event 9,000 BC
		7.3	**Atmospheric System Change**	Rapid or sustained periods of change in patterns of meteorological circulation, such as jet stream, causes regional climatic change	Dansgaard-Oeschger' events 11,500 years ago
		7.4	**Pollution Event**	Spillage or major release of toxic chemicals into land or sea systems that causes environmental destruction	BP Oil Spill Deepwater Horizon 2010; Niger Delta Oil Spill 1998; Exxon Valdez oil spill 1989; Japan Mercury Pollution of Minamata Bay 1956
		7.5	**Wildfire**	Uncontrolled inferno, enhanced by natural landscape and environmental factors	New South Wales, Australia (Bush Fires) 2003; Oakland, California (Fires) 1991; Indonesia (Forest Fire) 1982; Wisconsin (Great Peshtigo Wild Fire) 1871;

8 Technological Catastrophe **Accidental or deliberate industrial events affecting local and global stakeholders**	8.1	**Nuclear Meltdown**	Major core meltdown of a nuclear power station, causing radioactive fallout over a large area of population and economic and agricultural productivity	Fukushima Daiichi, Japan 2011; Chernobyl 1986; Three Mile Island 1979; Windscale, UK 1957
	8.2	**Industrial Accident**	Fire, explosion or release of toxic chemicals from an industrial complex, storage facility or during transportation	Toulouse France Explosion 2001; Bhopal India
	8.3	**Infrastructure Failure**	Blackouts in the electricity supply network and other systems failures due to accidents and technical breakdowns	Great New York Blackout of 2003; Enron California brown-outs 2000
	8.4	**Technological Accident**	New technological advance proves to have unexpected societal effects and causes disruption or harm to human populations	Bisphenol A (BPA) ban from use in baby bottle manufacturing 2010; DDT 1940-72; Thalidomide 1957-61
	8.5	**Cyber-Catastrophe**	Computer networks, communications and information technology systems destabilized by computer virus, hacking, denial of service attacks or other cyber-security issues	Unlimited Operation' $45m cash stolen in 12 hours 2012-2013; 'Comment Crew' / 'APT1' espionage attacks 2006-2013; 'Stuxnet' attack on Iran Natanz nuclear facility 2010; 'Conficker' Worm 2007; 'MyDoom/Novarg' worm 2004; 'SQL Slammer' 2003; 'I Love You' Virus 2000
9 Disease Outbreak **Disease outbreaks affecting humans, animals and/or plants**	9.1	**Human Epidemic**	Influenza pandemics, emerging infectious diseases and re-emergent disease epidemics that cause death and illness in human populations	1918 Influenza Pandemic; 2009 Swine Flu Pandemic; HIV/AIDS 1982+; SARS 2002
	9.2	**Animal Epidemic**	Diseases in animals that cripple agricultural production of meat and poultry or destroy wildlife	Mad Cow Disease (BSE) Epidemic, UK 1987; Foot & Mouth cattle epidemic, Korea, 1997; Swine Fever, Netherlands 1997; Avian Influenza 2004;
	9.3	**Plant Epidemic**	Diseases in plants that impact food production in many agricultural areas or cause destruction of the ecological environment.	Sudden death syndrome (SDS) in soybeans US Corn Belt 2010; Dutch Elm Disease, Europe 1967; Wheat Stem Rust Outbreak, US 1962; Wheat Stem Rust Outbreak, West Africa 1999

10 Humanitarian Crisis **Impact of conditions on mass populations of people**	10	**Famine**	A large population suffers failure of their food supply, food distribution, or agricultural production system	Ethiopia Famine 1998-2000; North Korean Famine 1996; Bangladesh Famine 1974; Biafra Famine 1967-70; Great Chinese Famine of 1959-1961; Dutch famine 1944; Soviet Famine 1932-3;
	10	**Water Supply Failure**	A large population suffers failure of their water supply due to water resource conflicts, river diversion, aquifer depletion, or other cause	Horn of Africa drought 2011; Cochamba Water Wars, Bolivia, 2000; Klang Valley water crisis 1998; Sahel drought 1970s; Battle of Beersheba over water resources for Palestine 1917
	10	**Refugee Crisis**	Mass population movements cause instability and collapse of social infrastructure in the areas newly populated and depopulated	Exodus from Zimbabwe 2009; US Mass Migration to the industrial north 1930-; India-Pakistan partition 1947; Economic migration of Latin Americans to North America
	10	**Welfare System Failure**	Collapse of pension schemes, health programs and social security systems leading to deprivation and hardship for dependents. Breakdowns triggered by underfunding, and imbalances e.g. ageing populations	Post-Soviet ‘shock therapy’ dismantling of welfare system in Russia 1992; Municipal Pension Defaults, US cities, 2010; New Jersey Pension Fund insolvency, 2009; Ireland state pension credit downgrade, 2008
11 Externality **Threats originating from outside the earth's atmosphere including astronomical objects and space weather**	11	**Meteorite**	Ground impact of meteors that cause localized destruction, and dust clouds capable of causing periods of ash winter	Tunguska meteorite explosion, Russia 1908; Chicxulub Crater, Yucatan, Cretaceous–Tertiary extinction event
	11	**Solar Storm**	Solar flare activity that can impact satellites, communication technology, power distribution systems and other infrastructure	Carrington Event geomagnetic storm of 1859;
12 Other **Other threats**				