Proceedings of 'Think Outside the Risk', Aon Benfield Hazards Conference, Gold Coast, Australia, 22-24 September 2013

EVOLVING RISK FRAMEWORKS: MODELLING RESILIENT BUSINESS SYSTEMS AS INTERCONNECTED NETWORKS

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

ABSTRACT

Research currently being undertaken at the Centre for Risk Studies, University of Cambridge, is based on the fact that the globalization of international business over the past 30 years means that catastrophes anywhere in the world are now capable of disrupting the processes and travel networks that underpin commercial activity. Catastrophes no longer impact a single geographical region, but disrupt international supply chains, business travel schedules, and market demand patterns. Assessing the exposure of a modern global business to international catastrophe risk requires understanding the interconnectedness of the activities and dependencies within their business system. We need to understand an international business as a complex system and assess its potential for disruption, feedback mechanisms, and catastrophic collapse, from the wide variety of potential threats to it. The Cambridge Risk Framework provides a platform for mapping a business system as an interconnected network, and simulating the flows and agents that it comprises, and testing the impacts of events on the network performance.

The framework includes a macro-threat taxonomy of all the potential large scale causes of socio-economic disruption, drawn from an extensive review of historical catalogues and potential future hazards. Threats ranging from economic (financial and trade disputes), geo-political events, natural and environmental catastrophes, through to humanitarian and health crises are categorized. From this threat typology, stress test scenarios are developed to evaluate the impact of different types of events on the business system. Multiple stress tests help assess the resilience of the business system to all types of interruptions, and enable senior managers to evaluate the costs and benefits of potential risk management strategies.

A case study based on an international consumer electronics supply chain is used to illustrate the application of the framework, applying a scenario stress test to investigate the resilience of the supply chain, and to evaluate alternative mitigation strategies. Suggestions are also given on how to use this approach to overcome some of the limitations of business interruption insurance and its extensions.

INTRODUCTION

The main purpose of this paper is to introduce the Cambridge Risk Framework and to illustrate its application to the analysis of the resilience of business systems, in particular through an international supply chain risk case study. There are limitations in the basic Business Interruption insurance product, and its extensions (such as Contingent Business Interruption and Non-damage Business Interruption), in covering supply chain risk and this paper proposes that using an approach such as the Cambridge Risk Framework should enable insurers to address some of these limitations.

The Cambridge Risk Framework derives from the intersection and combination of research into the areas of catastrophe modelling and extreme risk analytics with that of complex systems and network failures. The objective underlying the Cambridge System Shock research project is to advance the development, codification and application of scientific knowledge into how socio-economic systems can be made more resilient to the threats of catastrophic failures. One of the many potential applications of this framework is to provide a platform for systematically evaluating the potential socio-economic disruptions from a range of catastrophes to any global network of business activity.

This paper argues that many of the major threats to societal and business systems are not well understood, and hence the risks not often covered by insurance or the subject of well-developed models. If these threats could be better understood, then the resilience of society and business can be improved. The paper then outlines the Cambridge Risk Framework of Macro-Threats, how the

taxonomy has been derived and structured, and how it provides calibrated scenarios for stress test analysis. As an exemplar of a business system, the paper considers international supply chain risks, their nature, growth and network characteristics. Then, an example of the application of the Cambridge Risk Framework is presented, where a stress test scenario generated from the Macro-Threat taxonomy is used to analyze the resilience of a particular international supply chain network. Finally the paper suggests ways in which the Cambridge Risk Framework and its applications can be further developed.

CATASTROPHES: SOCIETY AND BUSINESS

Society and catastrophes

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. Extreme events may be 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'[1]. There are many potential causes of macro-catastrophes, 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, and financial services and re/insurance companies across the world. Therefore there is a need for a systematic taxonomy and assessment of these macro-catastrophe threats to support their efficacious risk management.

Managing business catastrophic risks

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. Individuals and companies 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 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 in a global system. These inter-linkages 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, global

[1] A formal definition of a macro-catastrophe threat is proposed in Coburn et al (2013).

corporations notice these extreme events in an entirely new way, as they impact some part of the linkage structure of their global operations.

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 commercial counterparties 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, aviation, transport, 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[2], 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.

Re/insurers and international corporations both have an interest in understanding the global risk landscape of macro-catastrophe threats. 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 international corporations in offering coverages that provide protection to the corporate balance sheet, in ways that may not be possible today.

THE CAMBRIDGE RISK FRAMEWORK[3]

The main components of the Cambridge Risk Framework are shown in Figure 1.
This paper is principally concerned with introducing some components of the Cambridge Threat Observatory (primarily the Taxonomy of Macro-Threats), and presenting a Resilient International Supply Chain case study from the Network Manager.

THREAT OBSERVATORY: TAXONOMY OF MACRO-THREATS[4]

A taxonomy of threats

A systematic evaluation of threats that could cause future macro-catastrophes would be useful for various aspects of risk management. An objective of the research programme of the Centre for Risk Studies at the University of Cambridge is to develop a systematic and evidence-based approach to threat assessment and risk management for macro-catastrophes, to improve the resilience of societal and business systems. 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.

The typology of threats is proposed as a framework, intended to be used to structure and collate information about the state of knowledge of each threat. It is designed 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.

---

2 The World Trade Centre (WTC) 9/11 event gave rise to major losses in over twenty different classes of insurance – not just tens of billions of dollars of property damage and business interruption losses, but WTC was the world's first workers compensation and life insurance 'catastrophes' (with thousands of people injured or killed as a result of the one event), and the world's largest insured art loss (with many expensive works of art destroyed in the collapsed office blocks).

3 For further details see the Cambridge Risk Framework website http://CambridgeRiskFramework.com

4 This section is based on Coburn et al (2013).

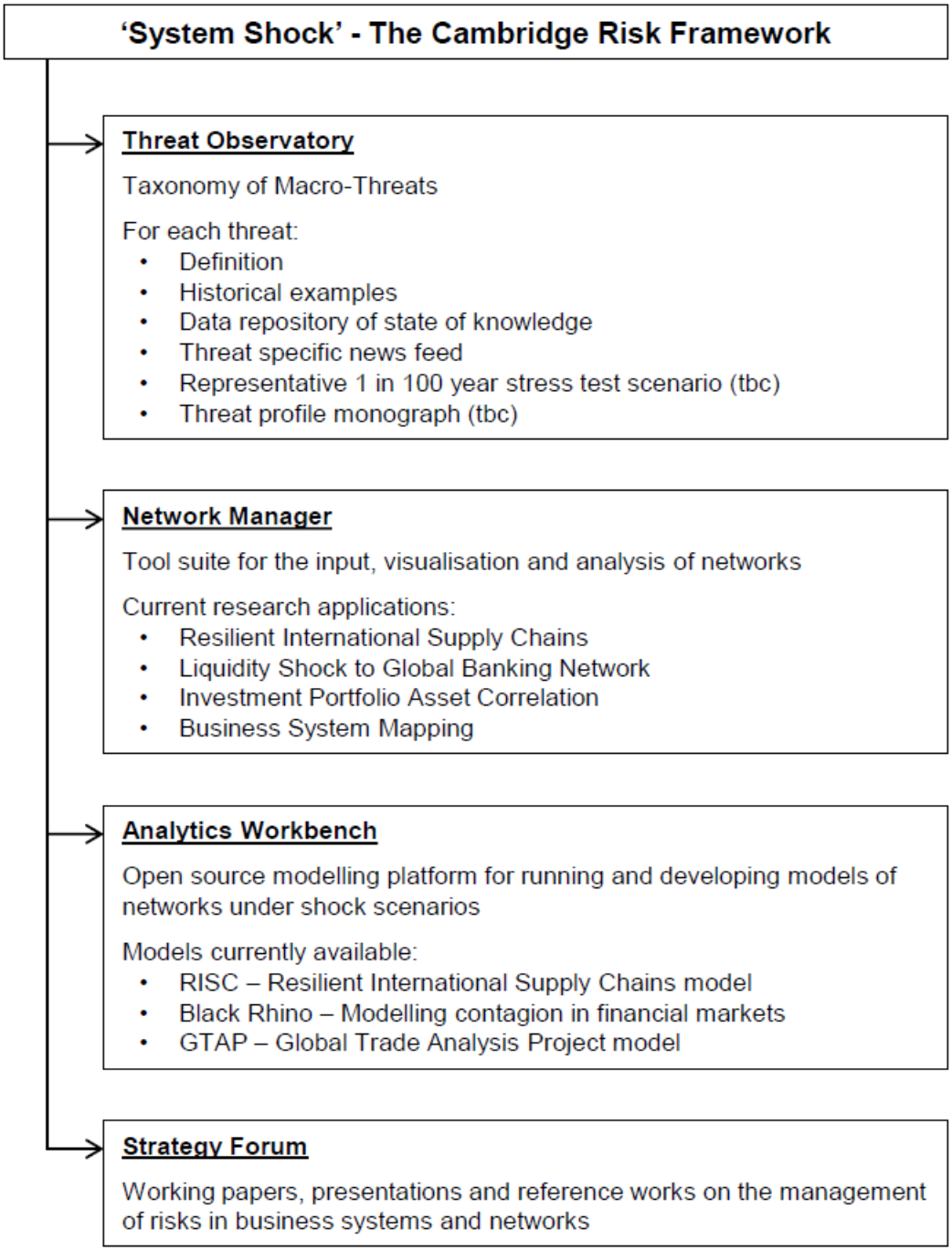


Figure 1: The Cambridge Risk Framework research platform.

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 standardised framework enables 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 of the new or emerging categories of threat as and when this becomes appropriate. Ultimately it may be possible to develop 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 the initial phases of research development. The current research activity is to develop the

framework to define the major areas of threat. Population of the framework is intended to be incremental and prioritized by the importance of the threat and by the need for better understanding.

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 scenarios are being developed that are benchmarked to the same likelihood of occurrence. To select the appropriate return period, areas of interest by different stakeholders have been reviewed.

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 on 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]. Proposed Solvency II regulations, due for implementation in Europe in 2015 or thereafter, 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 the 1% annual probability of exceedance – i.e. 100 year return period - has been selected 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) could 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 (see Appendix 1) 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 scenario suite may be an important factor in developing robust business systems to survive these extreme but frequent shocks.

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

5 From a survey of Chief Risk Officers, on perception of risk and threat probability levels of concern..
6 Value-at-Risk models and investment downgrade probabilities are commonly managed to the 95th percentile over an annual cycle.
7 Return periods of interest in insurance risk management.
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). https://eiopa.europa.eu/fileadmin/tx_dam/files/publications/submissionstotheec/CEIOPS-Calibration-paper-Solvency-II.pdf

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 events beyond the experience of the manager and therefore unable to be anticipated[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-catastrophes. 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, were 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.

Updating catastrophe characteristics

The characteristics of any macro-catastrophe event when it occurs is always different, and unique to the location, the 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.

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 and catalogue the fundamental causes of future catastrophes. What cannot be easily predicted is the specific characteristics of how the next future catastrophe of any type will play out. It is possible to illustrate

[9] Taleb N N, The Black Swan, 2007, Allen Lane, Penguin Books.

possible ways that a catastrophe of a given type and 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.

A new generation of catastrophe risk modelling

Probabilistic catastrophe models are routinely used by re/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 also 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).

However the current generation of catastrophe models remains focused on a specific geographical market and mainly focuses 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 macro-economy 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.

Definition of a macro-catastrophe threat

A ‘threat’ is defined as a potential cause of a socio-economic catastrophe that would imperil 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.

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 Cambridge Risk Framework research 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 (GDP).

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.

Methodology and data sources

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]. As the chronological catalogues were reviewed year by year, disruptive events fitting the criteria were identified and attributed to a cause using a long list of 'loose labels', which were then reclassified into a more refined grouping of threat categories.

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

---

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

Finally, 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 – so-called '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.

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 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 paper, and is available interactively online at the Cambridge Risk Framework website[24]. For taxonomy to be tractable and have a manageable number of categories, but also of sufficient granularity to be applied in more detail when appropriate, it should be hierarchical and capable of subdivision to increasingly

[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

[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

fine levels of resolution. Twelve primary categories of macro-catastrophe threats have been identified, 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 'Organized 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.

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. The section on correlation and causation, below, considers 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.

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 are 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.

Correlation and causation

The worst catastrophes are often 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 2. 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.

Applications of the taxonomy of macro-catastrophe threats

The objective of the Cambridge Risk Framework research project is to apply one or more stress test scenarios, drawn from the Threat Taxonomy, to a societal or business system, and model the impact. By investigating different risk mitigation strategies, the more efficient ways of improving the resilience of the system can then be evaluated. By way of illustration, this rest of this paper considers an international supply chain as an example of a business system, and describes the methodology of investigating its resilience to a 1 in 100 stress test scenario from the Threat Observatory using a model from the Network Manager.

EVALUATING THE RESILIENCE OF AN INTERNATIONAL SUPPLY CHAIN

Growth of supply chain risks[25]

Most large manufacturing companies depend on other companies to supply them with goods and services – many companies depend on hundreds of suppliers for thousands of components. These suppliers in turn often have many sub-suppliers, and so on. Supply chains are becoming increasingly more extended, more complex and more global. The disruption to the supply of a key service or component, however small in terms of size or value, can have severe financial and/or reputational repercussions up and down the supply chain. An Oracle survey of large organizations in the EMEA region found that 63% of businesses had reported that they had seen disruption to their value chain beyond their control – such as economic disruption (24%), adverse weather (19%), and bankruptcy of suppliers (16%) – and that it took an average of 63 days to get back to normal operations[26].

[25] This sub-section is based on Punter (2013).
[26] Two thirds of businesses hit by value chain disruption, SupplyChainStandard.com, 16 April 2013.

				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**													

Figure 2: The Correlation and Causation Dependencies of Threat Categories.

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 reasons for the growing significance of supply chain disruption include:

- **Changing business models (especially outsourcing)**. The trend in the 20th century was for manufacturing companies to become 'vertically integrated', i.e. to own and operate many of the stages of production that led up to the final manufacture and assembly of their products. For instance Ford Motor Company had its own electricity plant, iron ore processing facility, glassworks, docks, railway lines in Michigan and owned rubber plantations and forests overseas. However over recent decades the trend has been for manufacturing companies to move to a more 'horizontally integrated' mode of operation, i.e. leveraging their specialist expertise and/or scale in one or more particular stages of the production process and subcontracting or outsourcing the other stages to other specialized companies. This increases economy of operation, but also dependence on other, non-owned, companies.

  Many companies nowadays are less often manufacturers in the old sense of the word, but more assemblers. One prime example of this changing business model is Boeing. In the 1950s, 98% of the early 707 aircraft was built inside the US. For the recently launched 787 Dreamliner aircraft, Boeing is itself only responsible for about 10% by value (the tail fin and final assembly), with the rest of the manufacturing being outsourced (e.g. the wings are built in Japan, parts of the fuselage in Italy and Japan, landing gear in France, engines in England). Boeing now refers to itself as a 'systems integrator' rather than a manufacturer.

- **Offshoring and globalization**. Combined with outsourcing has been the globalization of business, with many of the outsourced operations also being offshored, primarily to access lower property and labour costs – often to countries in the Far East. However this increases the risks in the supply chain, including natural perils (such as recent earthquakes, tsunamis and floods in that region), political and economic risks (such as political or labour unrest, expropriation, intellectual property theft, foreign currency volatility), and transport risks.

- **Competition and cost pressures (or 'lean sourcing')**. Procurement functions usually focus on cost and quality, not risk, and may operate in a separate 'silo' to the risk management function. For instance, buying components from single suppliers to gain volume discounts, may lower cost but will increase vulnerability to suppliers' problems.

- **Production methods (or 'lean manufacturing')**. Modern manufacturing mantra, including just-in-time (JIT) delivery of components, or even zero inventory, regards any expenditure of resources for any goal other than the direct creation of value for the end customer to be wasteful and thus a target for elimination.

- **Geographic clustering / local specialization**. There are efficiencies for companies in the same or similar industries to locate in the same geographic area. This clustering gives rise to production synergies – such as leveraging sub-suppliers, joint development of manufacturing and labour expertise, and reduces transport costs – but increases interdependence risk and common exposure to threats. This was illustrated in the Thai Chao Phraya floods of July 2011, when nearly one-third of the world's hard disk drive manufacturing capacity was lost[27].

- **Size and complexity, criticality and vulnerability**. For many companies supply chains have become large and complex – Boeing's commercial arm handles more than 750 million aircraft parts a year, from 1,200 companies operating 5,400 factories – and critical – one survey suggested that 60% to 70% of the cost structure of many companies is embedded in their supply chain[28].

- **Modern communications**. The growth of the internet and social media has increased the pressures on supply chains. Any news or rumours of potential shortages can spread quickly leading to panic buying, exacerbating any real or perceived product shortages; similarly any allegations of product deficiencies or poor labour conditions or other unethical behavior by any suppliers can quickly disrupt distribution and sales of products.

[27] For more details of this event see the Thai Chao Phraya floods, July 2011 case study in Punter (2013), pp. 27-30.
[28] From Stone R E, Dittman J P and Mentzer, J T, 2010, The New Supply Chain Agenda: the five steps that drive real value, Harvard Business Press, page 7.

The main impacts of any supply chain disruption affecting the quantity and/or quality of goods and/or services available are one or more of the following:

- Increase in costs
- Loss or deferral of sales
- Loss of market share
- Fines or other actions by regulators
- Damage to brands and company reputation

Supply chain insurance – limitations

Insurance can play a role in financing supply chain risk. A review of the supply chain insurance market published by Airmic[29] reported that many Airmic members considered the coverage available to be insufficient and too costly, and the collection of the required underwriting information overly onerous. On balance, existing contingent business interruption insurance coverages were viewed to have weaknesses, particularly in light of recent events.

A survey of European risk managers by FERMA (*Federation of European Risk Management Associations*) on supply chain risks[30] reported that only 14% of respondees felt that existing coverage and capacity was adequate, and just half said they insured against contingent or non-damage business interruption. Also 46% said that coverage and capacity were not sufficient, 28% found conditions too restrictive and 26% stated that the cost was too high.

The definition and scope of relevant insurance coverages, as outlined in the Airmic review, are broadly:

- **Business Interruption (BI)** insurance covers economic losses and increased cost of operation resulting from physical damage to the insured's business operations caused by a specified peril at the insured's own premises.
- **Contingent Business Interruption (CBI)** insurance covers economic losses and increased cost of operations as a result of physical damage caused by a specified peril to property at the premises of a (often named) supplier, customer or other business partner. Similar coverage may be provided under a Physical Damage/BI policy with a customer and/or supplier extension.
- **Supply Chain (SC)** insurance covers economic losses and increased cost of operations caused by any specified event or circumstance that results in disruption to the normal business operations of the insured. Such a policy does not usually cover 'all risks', but may exclude such perils as war, terrorism, nuclear, regional pandemic**,** and quality related issues (including product recall).

Some of the problems with these coverages were demonstrated in recent events such as the Japanese earthquake/tsunami and Thailand floods of 2011, both of which impacted manufacturing regions; these issues include:

- CBI is generally limited to physical damage to or at a supplier's or customer's premises[31]. Much of disruption to Japanese manufacturers following the earthquake in 2011 was from the rolling power blackouts and from evacuations due to the Fukushima nuclear disaster (ordered by the Japanese Government[32]), and that is not a covered peril under CBI[33]. Similarly, most

[29] Airmic review of the supply chain insurance market, Airmic Technical, December 2012, www.airmic.com/sites/default/files/Supply%20Chain%20insurance_1.pdf
[30] Risk managers and underwriters set to clash on supply chain risk, Jon Guy, reinsurance, January 2012, page 10.
[31] One-year anniversary of Japan earthquake and tsunami is a reminder that businesses need better risk management and supply chain coverage, Insurance Information Institute, 8 March 2012.
[32] Quake creates claims concerns, Judy Greenwald, Business Insurance, 28 March 2011.

of the losses resulting from the Eyjafjallajökull volcanic ash cloud in April 2010 were not covered, because it did not cause physical damage[34].

- Where CBI cover was in place, it was usually inadequate compared to the losses suffered[35] – with low sub-limits or total limits of insurance coverage, which were quickly exhausted by direct property damages[36].

- A large proportion of disruptions originate below the first-tier supplier, so that companies need to ensure any CBI insurance covers multi-tier, rather than just first-tier or named suppliers[37]. However the perils covered and limits available on second-tier suppliers and beyond may be very restricted, if available at all[38] – particularly where they are not named.

- SC (and to a large degree CBI) insurance policies have to be individually developed for each policyholder. Collection of the required underwriting data is a huge challenge and with manuscript policies, exclusions and sub-limits vary, and premiums are not insignificant.

- Adjusting BI, CBI or SC insurance losses is very problematic – there are many contingencies and 'what-ifs', with potentially various intertwining factors involved, including in the example of the Japanese 2011 event, the earthquake, tsunami, fires, power outages, infrastructure and nuclear damage[39]. Further issues that may arise, for example, include: Were sales lost, or just deferred? How much extra expense is justified or necessary? How to assess and allocate losses between named and unspecified perils, and/or between named and unnamed suppliers? How to allocate sub-limits on policies between specified perils (e.g. between earthquake and flood)?

- Insurance companies are concerned that if they write too much CBI and/or SC insurance then it would be very difficult to control accumulation and aggregation of exposures.

Insurance products generally focus on the transfer of risk associated with tangible and measurable assets, not on intangible and/or immeasurable assets such as risk to reputation, nor on other impacts such loss of market share and reduction in share price – all of which can be impacted by a supply chain disruption.

Finally, insurance cover (however extensive) for any risk (supply chain or other) mainly treats 'symptoms' (not causes) – it does not prevent losses. Effective supply chain risk management should also include prevention and mitigation measures – to enhance the resilience of the supply chain.

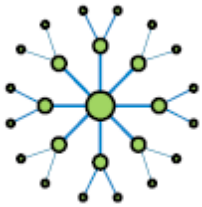
Network topology and vulnerability[40]

Supply chains are networks of business processes, linked by transportation stages, information flows, financial transactions, and personal interactions. Supply chains can in fact be viewed as 'systems of systems' – they overlay and leverage the company's manufacturing and distribution system with that of its suppliers' systems and various transport infrastructures (e.g. air, road, rail and sea routes) and business communication and other infrastructures (e.g. telephone, Internet, utilities). Characterizing the topology of these networks can identify key features, such as inter-connections and dependencies, and stress analysis of the topology can provide insight into their vulnerabilities, such as choke-points and concentration risk[41].

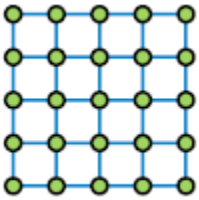
---

33 Supply risks take priority, Rodd Zolkos, businessinsurance.com, 27 November 2011.
34 Supply chain disruptions not covered, Judy Greenwald, Business Insurance, 12 March 2012, page 4.
35 Risk managers must get a grip on supply chain exposures, Tony Dowding, Commercial Risk Europe Special Conference Report, Airmic, 12-13 June 2012.
36 Insuring ever-evolving commercial risks, Swiss Re, sigma No. 5/2012, page 25.
37 One-year anniversary of Japan earthquake and tsunami is a reminder that businesses need better risk management and supply chain coverage, Insurance Information Institute, 8 March 2012.
38 Skittish insurers scrutinize CBI coverage requests but market still open, Michael Voelker, Property Casualty 360 – National Underwriter, 8 March 2013.
39 Quake creates claims concerns, Judy Greenwald, Business Insurance, 28 March 2011.
40 This and following sub-sections are based on Ralph et al (2012).
41 For more details on the use and analysis of Networks in Economics see Goyal S, Connections, 2007, Princeton.

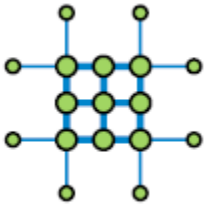
The topology of a network provides an indication of its vulnerability. Some basic network topologies are:



High-order star
e.g. air travel networks.
The whole network is vulnerable to failure at the "hub" node at the centre of the star.



Low-order "scale free" network
e.g. the Internet.
There is considerable redundancy in the network with many alternative paths from any one point to another. Therefore there is low vulnerability to any individual node failure.



Core periphery network
e.g. the global banking network.
The core central component network of key nodes displays good redundancy, giving low vulnerability to individual failures in the core, but widespread failure in the core will bring down the whole network.

Networks on networks

Any significant business system is a network built on many other networks, and will inherit the vulnerabilities of these underlying networks. When analyzing such a business system network, it can be thought of as three levels, starting with the simplest and working up in complexity:

- **Substrate or infrastructure networks**, which provide basic needs such as utilities (water and waste, and power - electricity, oil, gas), telecommunications (wire and wireless) and physical infrastructure such as transport nodes (airports, railway terminals, ports) and specialist buildings. They are characterized by high capital cost and inflexibility. Utilities tend to have a core periphery topology and medium redundancy; telecommunications of most types are scale free with high redundancy.

- **Primary networks**, such as roads and railway lines, are the key systems of a modern economy. They have a high capital cost but have some flexibility. Air transport has a high-order star topology and low redundancy; cargo shipping has a medium-order star topology and medium redundancy.

- **At-risk networks**, are the networks that businesses are faced with managing, and are composed of a wide variety of substrate and primary networks. Risk assessment of a given supply chain involves understanding the vulnerabilities of the substrate and primary networks that it relies on.

Case study: consumer electronics supply chain[42]

The production of consumer electronic goods requires the sourcing of raw materials from all around the world, but some of which are found in only a few locations, and then the manufacturing of components and final assembly. The high capital cost of high technology manufacturing plants (for example, a semiconductor fabrication plant can cost over $1 billion to build, with values as high as $3 billion to $4 billion not being uncommon) and low transport costs tend to favour clustering of the manufacturing and assembly processes, using specialized but low cost labour (most often located in Far East countries). This production element of the supply chain produces overall a high-order star topology for this industry, with intrinsic vulnerabilities to localized disruptions, as was illustrated in the Thai floods of 2011[43]. Overall the complete supply chain at-risk for a consumer electronics company also includes the primary networks of air transport, cargo shipping, communications and many other networks to get from raw material extraction to distribution of final product.

[42] A demonstration of the application of a System Shock scenario on an international supply chain described here is provided on the Network Manager http://cambridgeriskframework.com/page/22

[43] For further details see the Thai Chao Phraya floods, July 2011 case study in Punter (2013), pp. 27- 30.

The case study presented here considers the supply chain for a fictional consumer electronics producer, manufacturing and distributing a 4G tablet computer. Raw materials are sourced from all over the world (including South America, South Africa and Australia), components are manufactured in stages of increasing complexity at various locations, before final assembly in Shanghai, China – as shown in Figure 3 – and then the finished products are then distributed for sale to markets in North America, Europe, Southeast Asia and elsewhere – as shown in Figure 4.

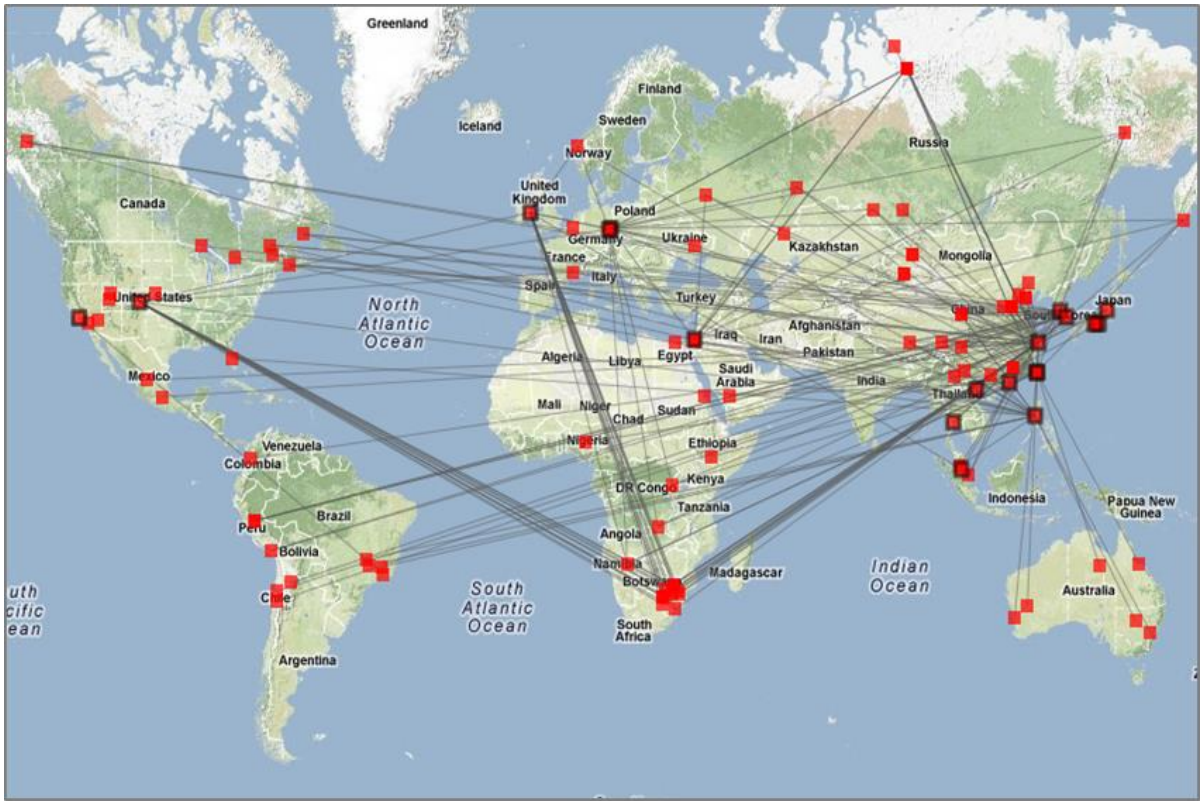


Figure 3: Geographical network of supply chain for production of a consumer electronic good.

Figure 4: Geographical network of supply chain for distribution of a consumer electronic good.

The production and distribution networks are then combined and transformed from the geographical representations in Figures 3 & 4 to a topological diagram of the network, as shown in Figure 5 – which depicts choke-points and dependencies and other characteristics of the graph.

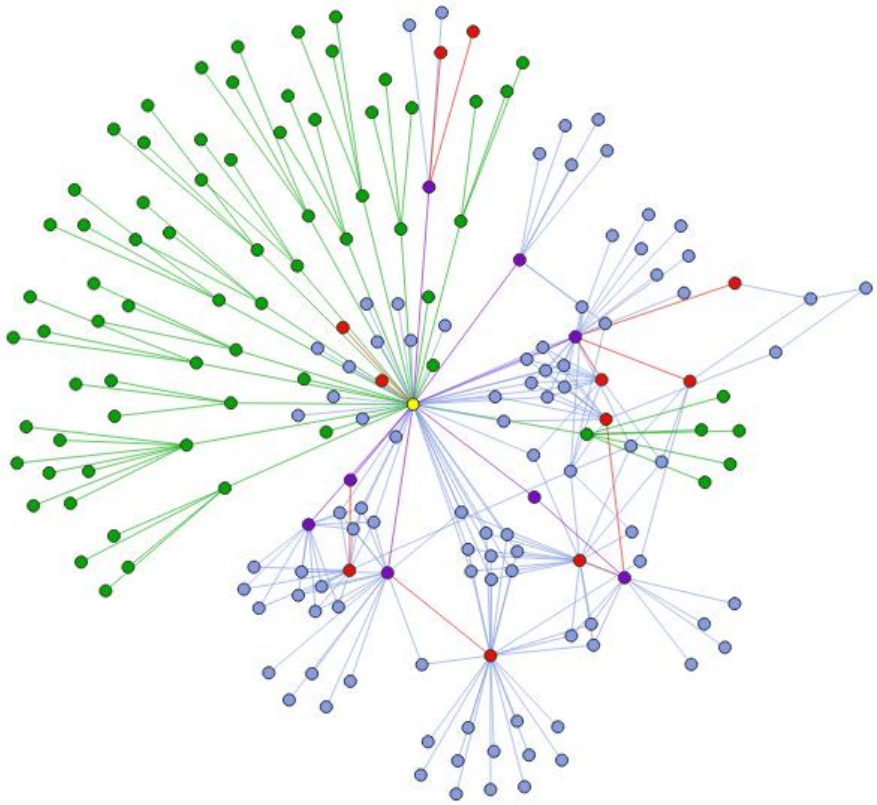


Figure 5: Topological representation of the supply chain network.

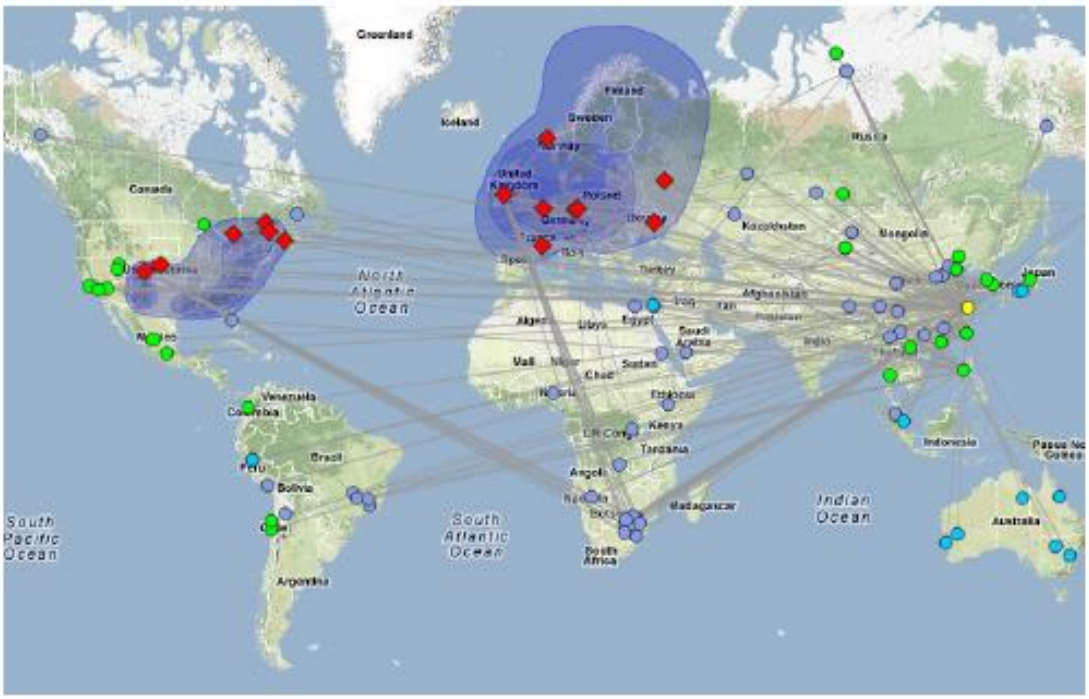


Figure 6: Impact of extreme winter weather scenario on consumer electronic good network.

The next step of the analysis is to apply a shock scenario from the Threat Observatory. The stress test applied here is a 1 in 100 years scenario of extreme winter weather across northern Europe and the US – under which freezing conditions, with heavy snow and ice, are experienced for over 6 weeks. The cold weather is so extreme that it reduces manufacturing productivity, stops transport and suppresses consumer demand. Analysis of the force-directed graph identifies the nodes of the network that lie within each intensity zone of the freeze event and assigns an intensity to each node. All of the nodes affected by the freeze event are highlighted in Figure 6 as a red diamond.

The model is then used to measure the disruption loss resulting from shocks to the system, as illustrated in Figure 7.

Figure 7: Illustrative impact disruption on original supply chain network.

Strategies to improve the resilience of the supply chain can then be introduced; these may include:

- Increased inventory safety margins – level of reserves of inventory maintained in different parts of the supply chain.
- Supplier diversification – maintaining more than one supplier for key parts of the process.
- Process diversification – removing choke-points in the supply chain by duplication of high level processes.
- Transport contingency – using alternative methods of shipping goods when routes are disrupted.

The network model is then re-run with the improvement strategies in place, and the 'revised' disruptive loss calculated, shown in yellow in Figure 8. The total disruptive loss is smaller and the recovery time shorter.

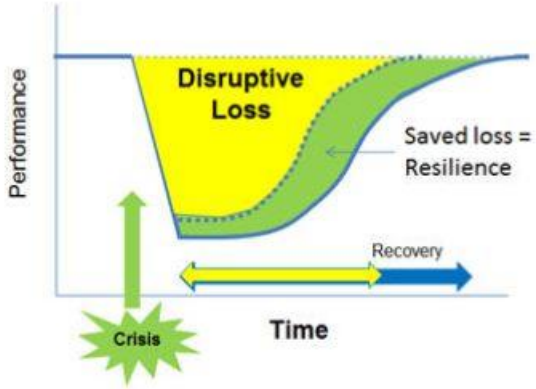


Figure 8: Illustrative impact of disruption on 'mitigated' supply chain network.

'Resilience' is measured as the reduction in disruption loss due to the improvement strategies. The aim is to achieve 'efficient resiliency' where the investment in improvement strategy is outweighed by the benefits of reduced disruption loss.

CONCLUSIONS

As international business systems increasingly span an uncertain and catastrophe-prone world, corporate managers have to manage more complex risk. There is a recognized appetite for corporate risk managers to obtain protection, but the ability of insurers to offer appropriate products is limited by the constraints of insurers needing to understand the risk properly, to assess exposure aggregation, and to quantify the risk with some level of confidence.

This paper shows that to understand the risk properly it is necessary to use a risk framework that combines threat assessment with network behavior analytics. The ability to model a business system, such as an international supply chain, under various stress scenarios greatly enhances the relative evaluation of alternative risk management or mitigation strategies to improve its resilience.

The objective of the research being pursued at the University of Cambridge Centre for Risk Studies is intended to facilitate the development of a family of new business interruption insurance coverages – by providing assistance to re/insurers in aspects such as pricing, peril specification, and accumulation monitoring.

This is an ambitious research agenda, and is at an early stage, although the initial proof-of-concept has been established, and various simple examples have been developed. The current research agenda includes the following objectives:

- Develop the modelling of supply chains to provide a more accurate representation of business processes, flows of goods, time and delivery constraints and other aspects.

- Improve the understanding of emerging risks and extend the modeling of scenarios that will cause systemic disruption across multiple locations and interactions of the economic and social business environment that supply chains operate within. The current research programme of the Cambridge Risk Centre is developing a number of additional scenarios to use as systemic shock tests for supply chains and international business systems including:
    - A geopolitical conflict in Southeast Asia that disrupts shipping routes, air travel, and international trade
    - An infectious disease pandemic that infects a large proportion of the workforce and causes difficulties in staffing and order completion
    - A cyber catastrophe of a large scale attack on the communications and data storage required for modern business operation
    - Civil unrest scenarios of widespread protest movements, general strikes, and riots that cause disruption of productivity across many parts of the world

- Profile the different types of international supply chains, by industrial sector, global market, and patterns of service provision, understand the data required to describe a supply chain and assess its risk, and find ways of simplifying the task of profiling a typical supply chain, and make it easier for underwriters to classify, parameterize and model supply chain risk.

The Cambridge Risk Framework is proposed as an approach for organizing information to assess the complex risk of network disruption from catastrophe shocks. It is currently being tested on case studies and real-world datasets of supply chain risks.

Collaborative work with business organizations, relevant governmental departments and others is welcomed and will enable specific network characteristics to be analyzed. A collective approach is needed to fully understand the risk for international supply chains and to create a more resilient world for the socio-economic systems they underpin.

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.

REFERENCES

Coburn A, Ralph D, Tuveson M, Ruffle S and Bowman G, 2013, A Taxonomy of Threats for Macro-Catastrophe Risk Management, Centre for Risk Studies, Judge Business School, University of Cambridge, Working Paper 201307.20, http://www.systemshock.org.uk/uploaded/documents/Cambridge_Risk_Framework_Taxonomy_DRAFT_20_July_2013.pdf

Punter A, 2013, Supply Chain Failures: a study of the nature, causes and complexity of supply chain disruptions, Airmic Technical, www.airmic.com/sites/default/files/supply_chain_failures_2013_FINAL_web.pdf

Ralph D, Bowman G, Coburn A and Ruffle S, 2012, Resilient International Supply Chains, Centre for Risk Studies, Judge Business School, University of Cambridge, Working Paper 201212.01, http://www.systemshock.org.uk/uploaded/documents/Resilient_International_Supply_Chains.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 lockout 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	**Nationalisation**	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'état	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 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 destabilised 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**				

Source: Coburn et al (2013).

APPENDIX 2: Risk frameworks and classification systems

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

World Economic Forum (WEF) Global Risks Report
The World Economic Forum has been publishing a review of Global Risks[44] 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.

OECD Global Future Shocks project
The OECD Global Future Shocks project[45] presents a framework for understanding systemic risks and profiles five leading threats: Pandemic; Critical Infrastructure Disruption from a cyber-attack; Financial Crisis; Geomagnetic Storm; and 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."

Individual governments also produce frameworks for national risks, for example:

UK Government National Risk Register
The UK Government Cabinet Office publishes a National Risk Register for Civil Emergencies[46]. This is 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 versus impact scale. The highest priority risks are defined as Pandemic influenza; Coastal flooding; Catastrophic terrorist attacks; Volcanic eruptions abroad; and Severe wildfires. This is the public version of a classified National Risk Assessment of over 100 different scenarios for civil authority preparedness.

Australian Government National Risk Assessment Framework – Geoscience Australia
The National Risk Assessment Framework[47] 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.

Source: Coburn et al (2013) plus author.

[44] The 2013 version of the WEF Global Risk Report is available http://reports.weforum.org/global-risks-2013/
[45] OECD Global Future Shocks report http://www.oecd.org/governance/48256382.pdf
[46] 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
[47] Australian Government, Geoscience Australia, National Risk Assessment Framework webpage http://www.ga.gov.au/hazards/governance/policy/national-risk-assessment-framework.html