

Cambridge Centre for Risk Studies
Advisory Board Meeting 13 January 2015

Research Showcase 2015

Centre for
Risk Studies

Research Showcase Agenda

09:00 Registration & Coffee

Session 1: Cambridge Risk Framework

09:30 **Welcome and Review of Research Activities in 2014** Prof Danny Ralph

09:50 **Developing Frameworks for Managing Cyber Catastrophe Risk** Éireann Leverett

10:10 **Cambridge Risk Framework - Developments and Objectives** Simon Ruffle

10:30 Coffee Break

Session 2: Catastronomics

11:00 **Understanding the Economic Consequences of Catastrophes** Dr Scott Kelly

11:20 **Macroeconomic Modelling** Jaclyn Zhiyi Yeo

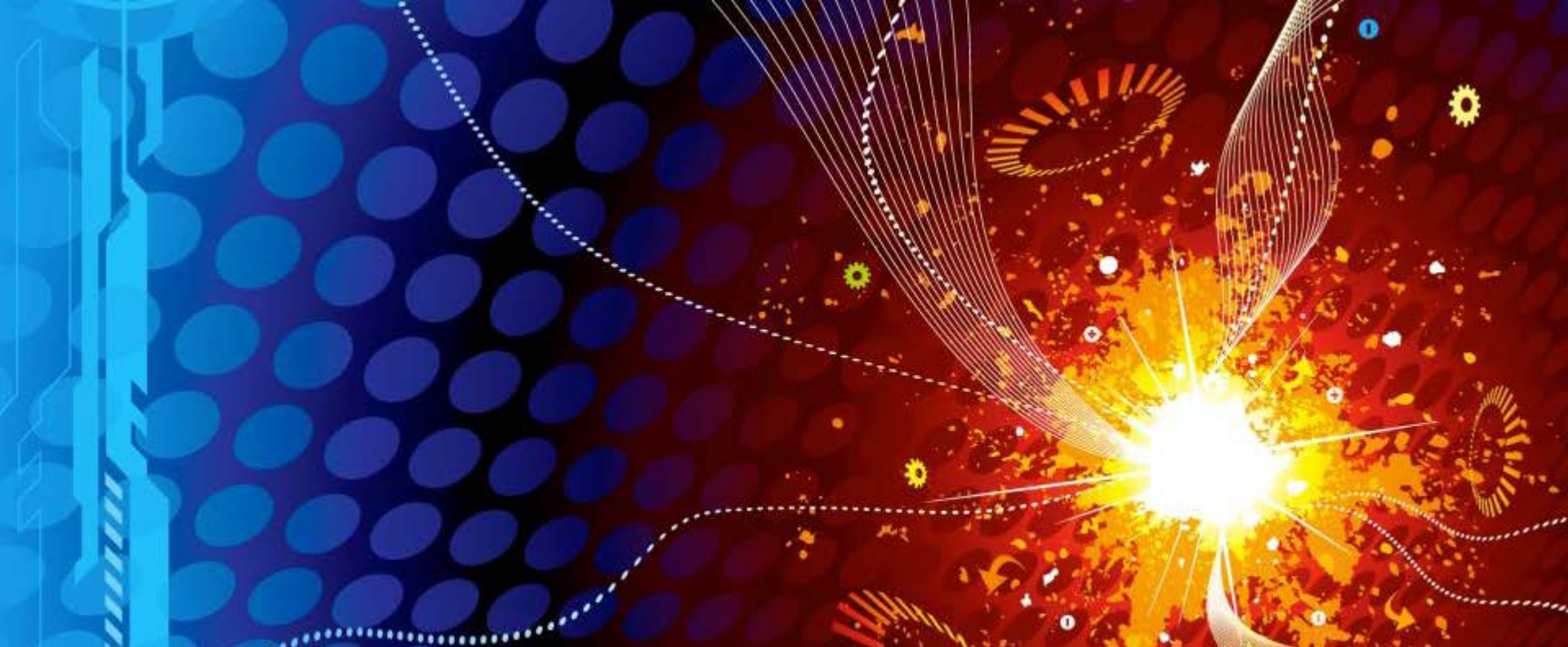
11:40 **Impact of Scenarios on Investment Portfolios** Jennifer Copic

Session 3: FinCat

12:00 **Contagion Modelling of Financial Crises** Dr Olaf Bochmann

12:20 **Financial Catastrophe Risk Research** Dr Andrew Coburn

13:00 Lunch (Common Room)



Centre for Risk Studies Research Showcase 13 January 2015
Session 1: Cambridge Risk Framework

Review of Research Activities in 2014

Centre for
Risk Studies



Professor Danny Ralph

Academic Director
Centre for Risk Studies

Overview of research

- Outputs of Cambridge Risk Framework
- Catastronomics as a subject illustrated by Cambridge Risk Atlas
- Financial Catastrophe research on endogenous shocks
- Cyber Catastrophe include SITEs and Digital Exploration Tool
- Dissemination

Philosophy of Cambridge Risk Framework

Cambridge Risk Framework aims to provide

■ Universality of risks

- “All threats” represented by Taxonomy of Threats

■ Frequency of risks



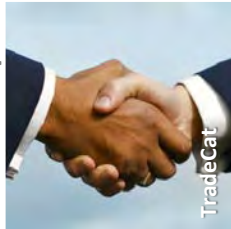



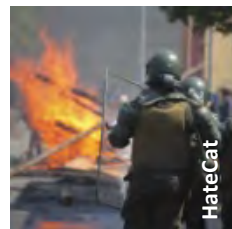


































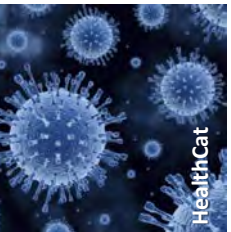

















- “Likelihood” represented by 1-in-100 year events

■ Severity of risks under various metrics

- Direct impacts
 - Human cost
 - Damage bill for industrial capacity & infrastructure
 - Underwriting exposure
- **Systemic** impacts
 - GDP@Risk: global economic loss cumulated over 5 years
 - Financial markets
 - Critical Infrastructure

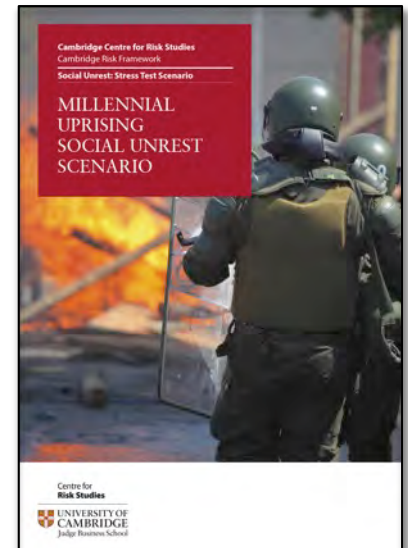
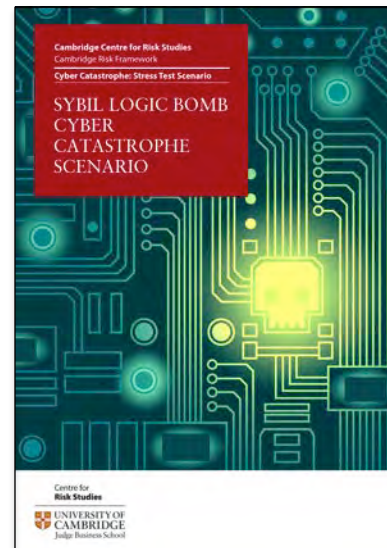
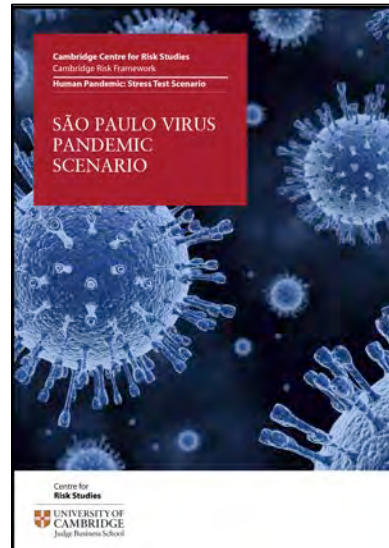
Comparability of Threats

2011-12 Cambridge Taxonomy of Threats

Financial Shock	 FinCat	 Asset Bubble	Trade Dispute	 TradeCat	 Labour Dispute	Geopolitical Conflict	 WarCat	 Conventional War	Political Violence	 HateCat	 Terrorism	
	 Market Crash	 Sovereign Default		 Cartel Pressure	 Nationalization		 External Force	 Civil War		 Organized Crime	 Assassination	 Social Unrest
	 Bank Run			 Tariff War			 Nuclear War					
Natural Catastrophe	 NatCat	 Earthquake	Climatic Catastrophe	 WeatherCat	 Drought	Environmental Catastrophe	 EcoCat	 Sea Level Rise	Technological Catastrophe	 TechCat	 Nuclear Melttdown	
	 Volcanic Eruption	 Flood		 Tornado & Hail	 Electric Storm		 Wildfire	 Pollution Event		 Cyber Catastrophe	 Technological Accident	 Industrial Accident
	 Tsunami			 Heatwave			 Atmospheric System Change			 Infrastructure Failure		
Disease Outbreak	 HealthCat	 Human Epidemic	Humanitarian Crisis	 AidCat	 Famine	Externality	 SpaceCat	 Meteorite	Other	 NextCat		
	 Waterborne Epidemic	 Zoonosis		 Child Poverty	 Welfare System Failure		 Space Threat	 Ozone Layer Collapse		 Satellite System Failure		
	 Plant Epidemic			 Refugee Crisis								

Progress in 2014 building on 2013

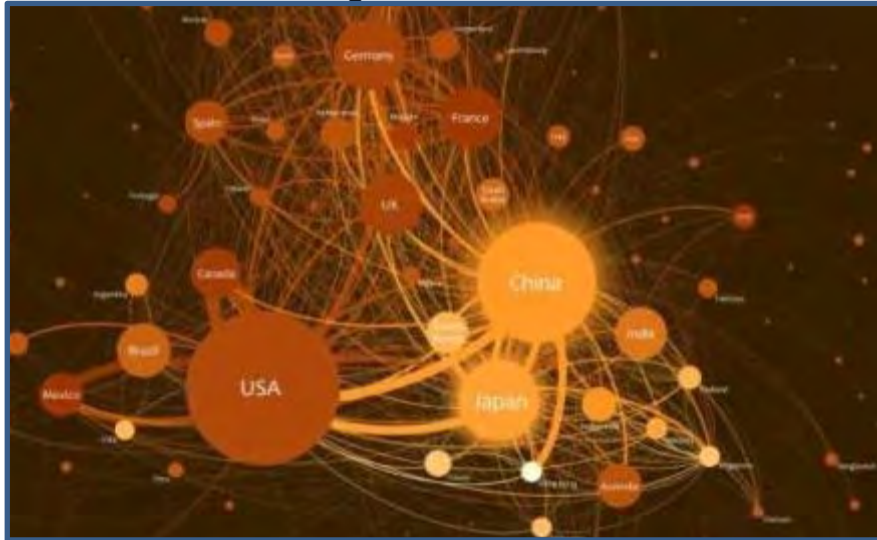
- Cambridge Risk Framework and 2013 Stress Tests
 - Geopolitical Conflict, Pandemic, Cyber Catastrophe, Social Unrest
 - Introduced global Macroeconomics & Financial market impact
- Whitepapers completed in 2014



- ‘GDP@Risk’ 2014 innovation
 - One measure economic damage across widely different shocks
 - Allows consistent Calibration and Comparison of unrelated shocks

2013-14 Network Models and Interconnected Risks

International Trading Networks



Travel Flows of People and Goods



Business Relationships between Companies



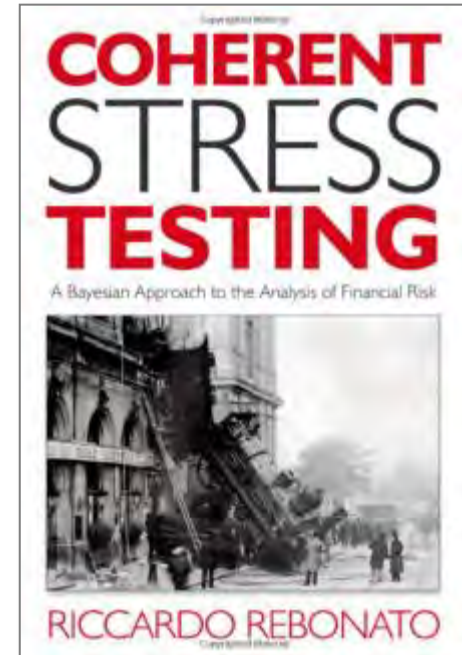
Communications and Social Media



Catastronomics

The Economics of Catastrophe

- Aim: systemise the modelling of economic impact of systemic threat scenarios
 - Philosophy of structural or coherent stress tests
- Use GDP@Risk to standardize impact across threats and units of analysis
- Proof of principle for cities as units of analysis
 - Cambridge Risk Atlas
 - World City Risk 2025

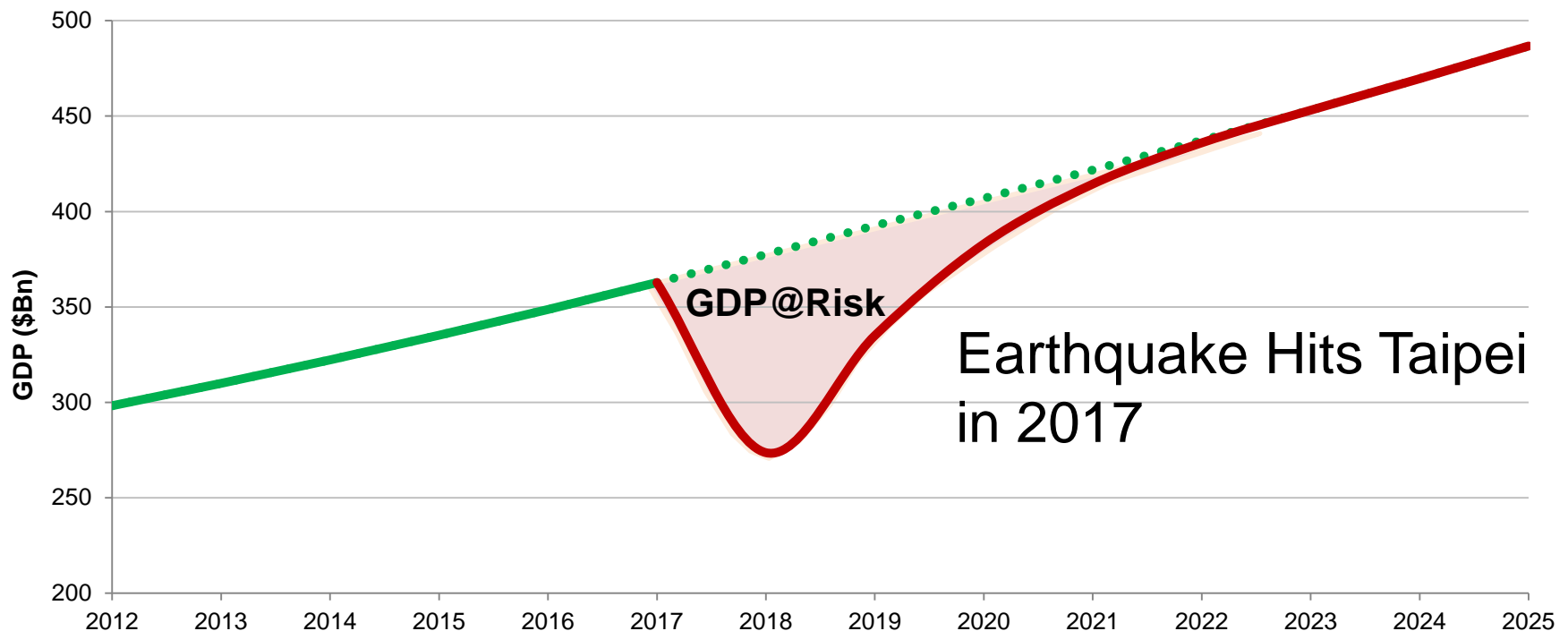


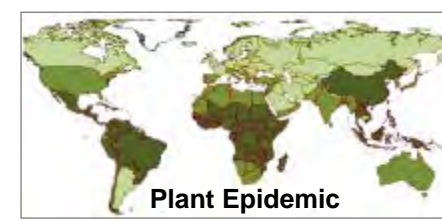
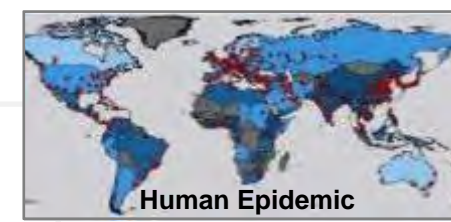
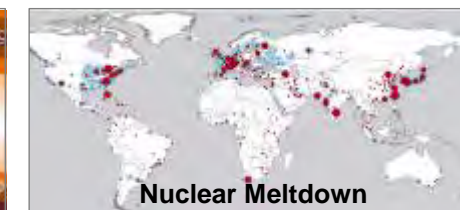
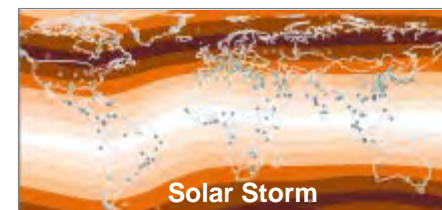
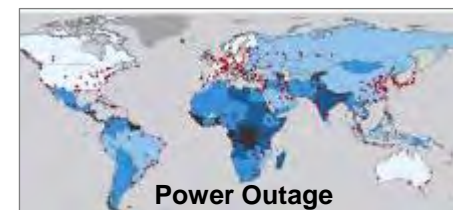
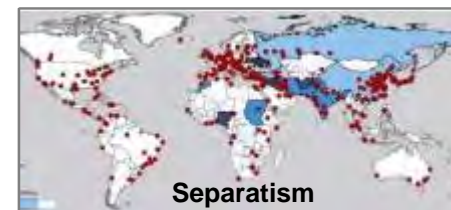
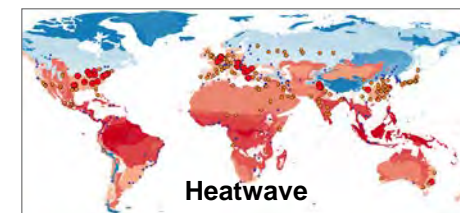
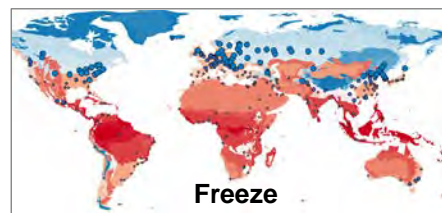
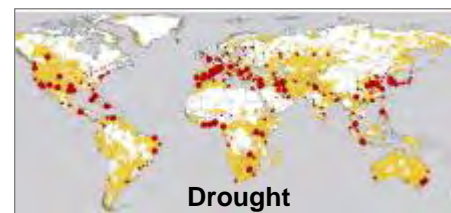
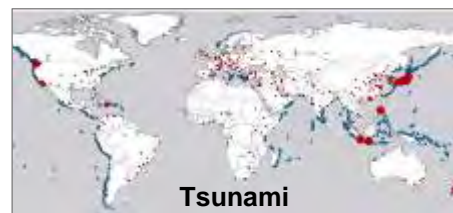
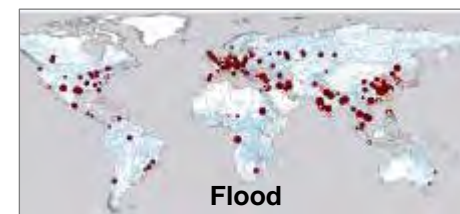
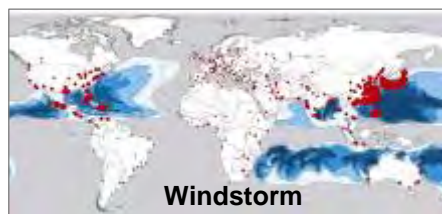
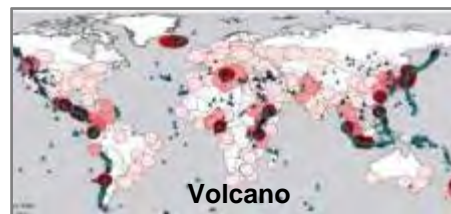
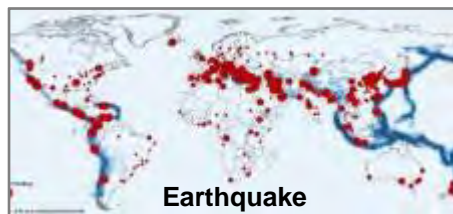
Catastrophonomics

Cambridge Risk Atlas

■ Model GDP@Risk for world's top 300 cities

- Top 300 cities account for over half of global GDP
- 23 threats: Wind Storm, Solar Storm, War, Financial Crisis...
- Data compilation on cities, threat maps, and historical precedents for 23 different threats.

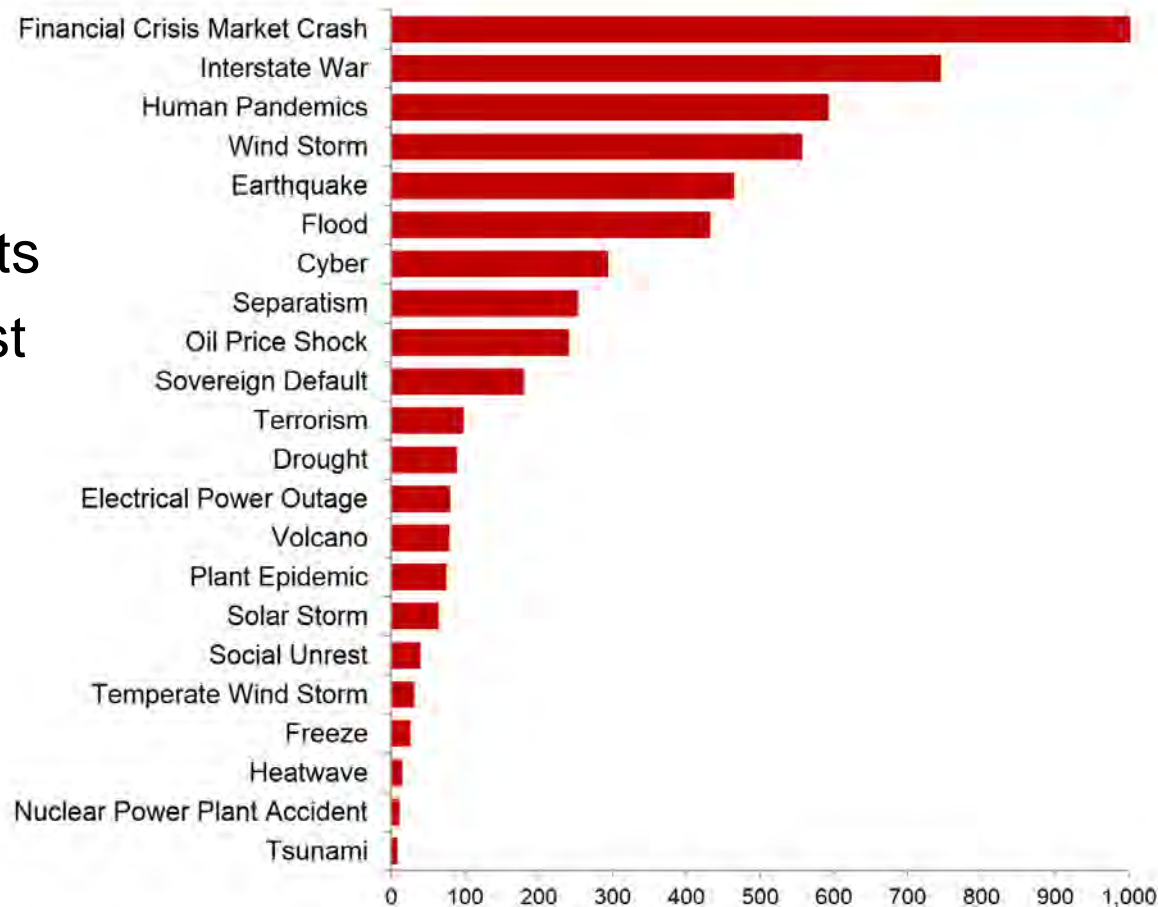




Catastronomics

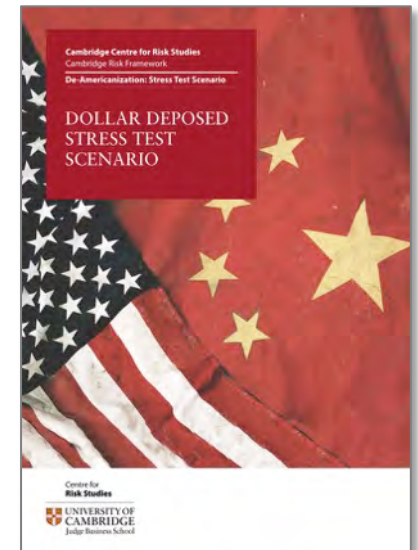
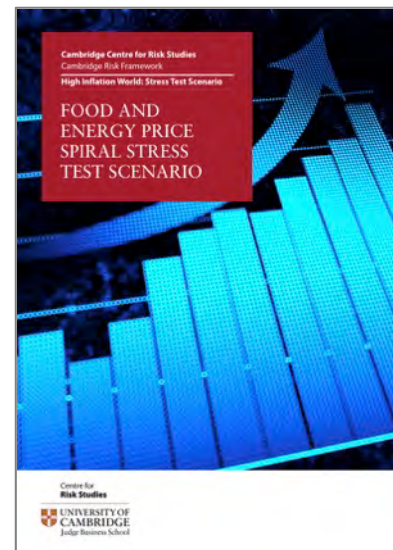
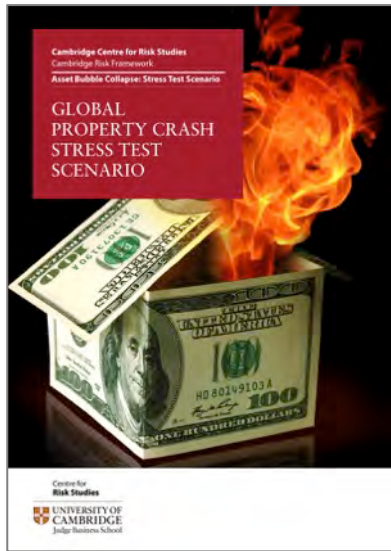
Cambridge Risk Atlas

- GDP@Risk for each city
- 1st holistic estimate of total catastrophe cost of all major taxonomy threats
- \$5 Tn of World's GDP lost to catastrophes per decade
 - 1.5% of world GDP pa
- Major advance in catastrophe studies
- Platform for 2015 research



Financial Catastrophe Endogenous Shocks

- Scenario analysis methodology developed for ‘exogenous’ shocks – external events – in 2013
- In 2014 began study of ‘endogenous’ shocks
 - Internal failures in the financial system
- Financial Catastrophe stress test scenarios

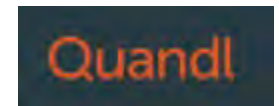


Financial Catastrophe

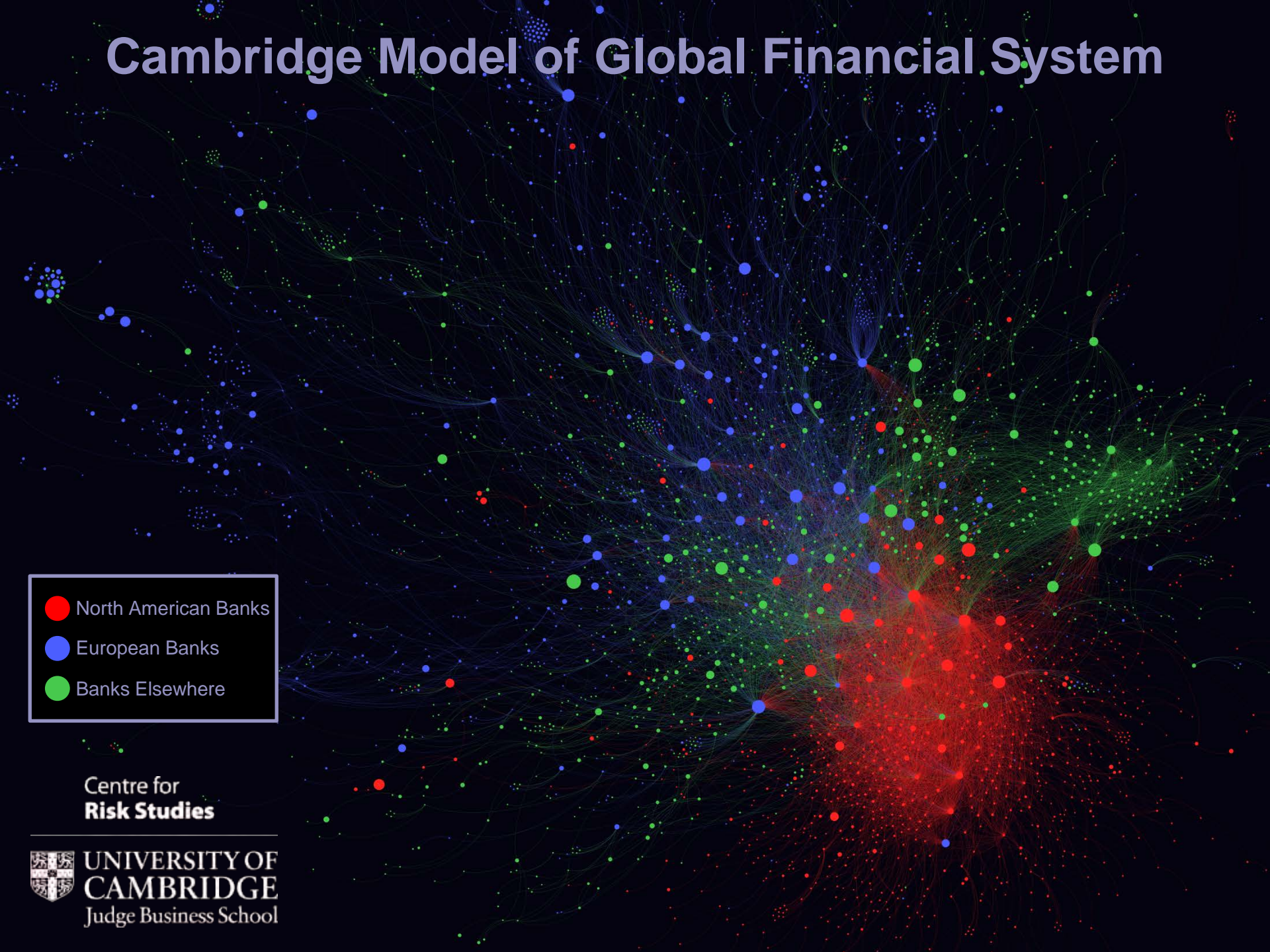
Developing a Model of Global Financial System

Data Sources include:

- Integrating multiple sources of data on banks, lending patterns, cross-holdings, and assets
- Network model of global financial system
 - One system \Rightarrow cover all jurisdictions and markets
 - Currently 18,000 banks
 - Balance sheet model of individual banks
- Three contagion mechanisms implemented
 - Counterparty failure (interbank lending network)
 - Devaluation of equity investments (cross-holding network)
 - Devaluation of commonly-held assets
- Future potential to link model to corporate enterprises



Cambridge Model of Global Financial System

- 
- North American Banks
 - European Banks
 - Banks Elsewhere

Centre for
Risk Studies



UNIVERSITY OF
CAMBRIDGE
Judge Business School

Financial Catastrophe

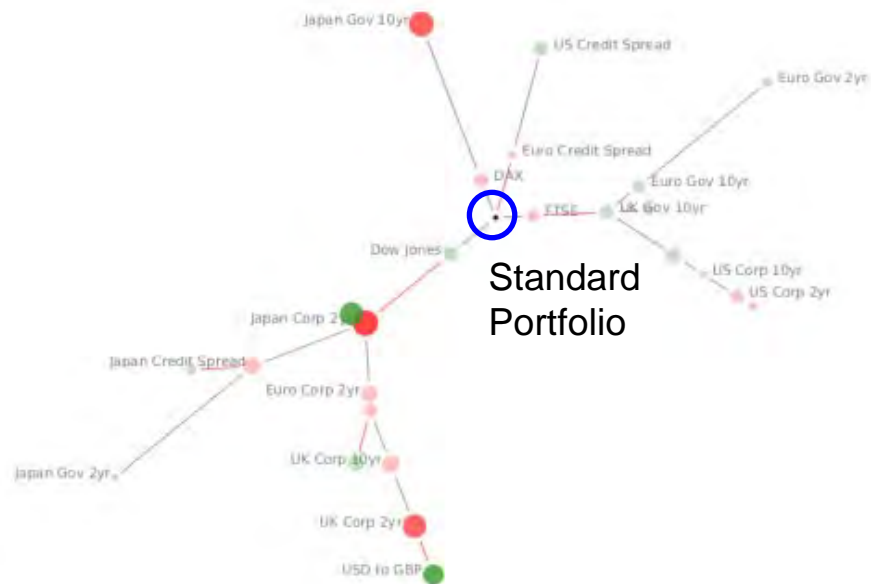
Global Property Crash: Impact on Investment Portfolio



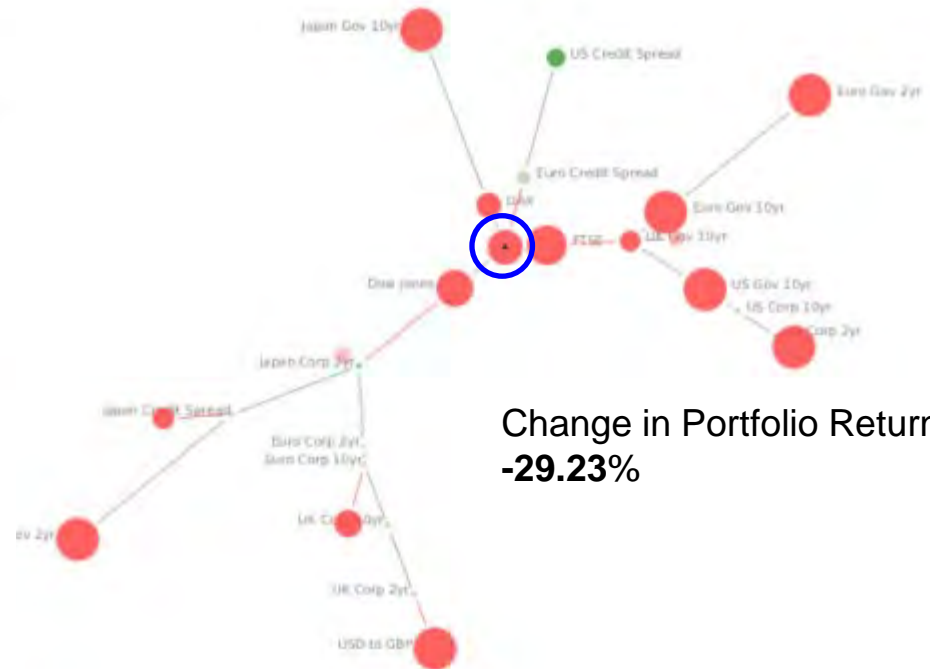
Impact on the assets in a standardized investment portfolio of the hypothetical stress test scenario

Asset Correlation Structure

Before Shock



Portfolio After Crisis



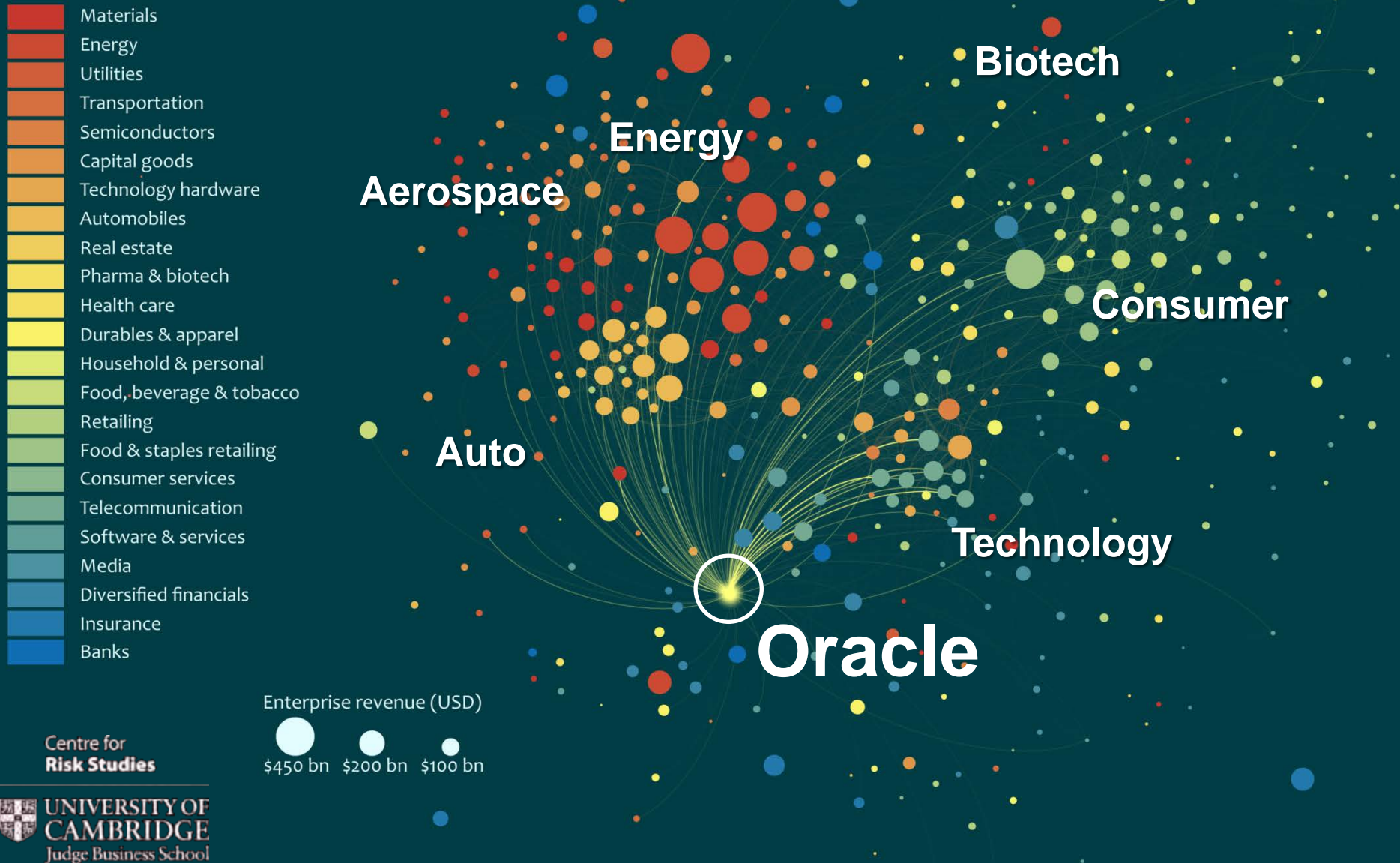
Change in Portfolio Return:
-29.23%

Cyber Catastrophe

Cyber Economy and 'SITES'

- Emerging threat of cyber disruption
 - Pillar of our research since 2013
 - Focus has been on cyber catastrophe, ie, systemic, correlated impact
 - 'Systemically Important Technology Enterprises' (SITEs)
- In 2014 we developed model of the cyber economy
 - Quantify impacts using standard industrial classes
 - Consequences for public sector critical infrastructure
 - SITEs concept increasingly cited for systemic correlation
 - Insurance industry increasingly interested
 - Accumulation techniques and exposure management

SITEs and the Cyber Economy



Our Cyber Research in the Media

The Actuary Dec 2014

Risk Technology

Andrew Coburn, Simon Ruffie and Louise Pryor are developing frameworks for cyber catastrophe analysis. They explain how mapping the cyber economy enables risk modelling of systemically important IT providers

Cyber attacks are featured in one of the top 100 stories in the World Economic Forum's Global Risks Report, but understanding the full scale of cyber-related damage to businesses and economies is still in its infancy.

The benefits of investing in increased levels of IT security cannot be disputed, neither can the risk of a major cyber attack being avoided. Cyber risk management needs a proper risk framework.

However, it is difficult to find a consistent cyber attack coverage because the risk is not well understood. What concerns insurers most is how the level of individual loss varies, such as the impact of a single company, such as a pharmaceutical company, or a single company, such as a pharmaceutical company, or a single company, such as a pharmaceutical company.

The fundamental concern is a single company could be a major loss, but the risk is not well understood. What concerns insurers most is how the level of individual loss varies, such as the impact of a single company, such as a pharmaceutical company, or a single company, such as a pharmaceutical company.

However, while a similar framework can be applied to model cyber catastrophe risk, developing an overall risk framework for assessing cyber threats is not easy, due to the challenges of the limited data on cyber loss experience.

A lack of understanding and communication of businesses and government organisations. The lack of awareness of cyber catastrophe risk means that the potential for cyber catastrophe is not well understood. What concerns insurers most is how the level of individual loss varies, such as the impact of a single company, such as a pharmaceutical company, or a single company, such as a pharmaceutical company.

The lack of understanding and communication of businesses and government organisations. The lack of awareness of cyber catastrophe risk means that the potential for cyber catastrophe is not well understood. What concerns insurers most is how the level of individual loss varies, such as the impact of a single company, such as a pharmaceutical company, or a single company, such as a pharmaceutical company.



A vulnerability in the Microsoft Windows operating system that is used by over 90% of corporate computers. Just IT Department reported on this security issue, however, it is the head of the IT department who would be most likely to be affected by the security issue. The head of the IT department would be most likely to be affected by the security issue. The head of the IT department would be most likely to be affected by the security issue.

A vulnerability in the Microsoft Windows operating system that is used by over 90% of corporate computers. Just IT Department reported on this security issue, however, it is the head of the IT department who would be most likely to be affected by the security issue. The head of the IT department would be most likely to be affected by the security issue. The head of the IT department would be most likely to be affected by the security issue.

A vulnerability in the Microsoft Windows operating system that is used by over 90% of corporate computers. Just IT Department reported on this security issue, however, it is the head of the IT department who would be most likely to be affected by the security issue. The head of the IT department would be most likely to be affected by the security issue. The head of the IT department would be most likely to be affected by the security issue.

The size of the attack. The size of the attack is dependent on how many companies are connected to the attacked company. The size of the attack is dependent on how many companies are connected to the attacked company. The size of the attack is dependent on how many companies are connected to the attacked company.

The size of the attack. The size of the attack is dependent on how many companies are connected to the attacked company. The size of the attack is dependent on how many companies are connected to the attacked company. The size of the attack is dependent on how many companies are connected to the attacked company.

The size of the attack. The size of the attack is dependent on how many companies are connected to the attacked company. The size of the attack is dependent on how many companies are connected to the attacked company. The size of the attack is dependent on how many companies are connected to the attacked company.

Financial Times Apr 2014

Diversity is the way to avoid cyber collapse

Viewpoint

MICHELLE TUVESON
and SIMON RUFFIE

Regulatory consciousness has increasingly focused on the reduction of systemic risk to ward off another financial crisis.

Regulators have poured vast amounts of intellectual capital into formulating the best measures for preventing taxpayer bailouts of collapsing institutions.

As a result, they created the "Systemically Important Financial Institutions" (SIFIs) brand to indicate a bank that may need rescuing.

In a recent discussion at a Cambridge Chief Risk Officer Council event, one bank official asked: "Why should a bank be worried about systemic risk? Its own risk should be its only focus." The remark captures the tension between the micro and macro risk perspectives.



error in its high-frequency trading algorithm resulted in losses of \$40m in less than an hour – 38 per cent of annual revenue – and led to its takeover.

One could argue these breaches were confined to two businesses and did not affect the global economy.

But what is worrying is the potential for a global system-wide IT failure occurring simultaneously across many organisations – a "correlated loss" event that affects a vast number of companies, or an entire sector.

As businesses get more interconnected, this type of threat becomes a real possibility.

A number of technology companies have become so deeply embedded in business productivity that they are systemically

important to the overall economy. Like the SIFIs, they and their products are so intertwined their failure would cause problems on a very large scale. We refer to these companies as Systemically Important Technology Enterprises (SITEs).

Mapping of the cyber economy identifies the technology enterprises vital to international corporate productivity. The mappings

also show the centrality of a cluster of companies and provide a visual representation of how potential failures may spread.

Could the economic effects of such a global cyber catastrophe be estimated? Any type of failure or attack that exploits vulnerabilities in products and applications of SITEs could permeate the world economy.

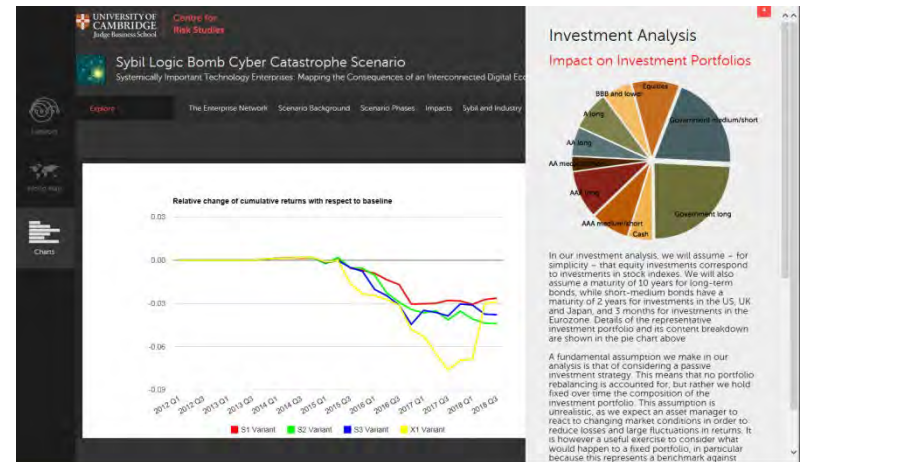
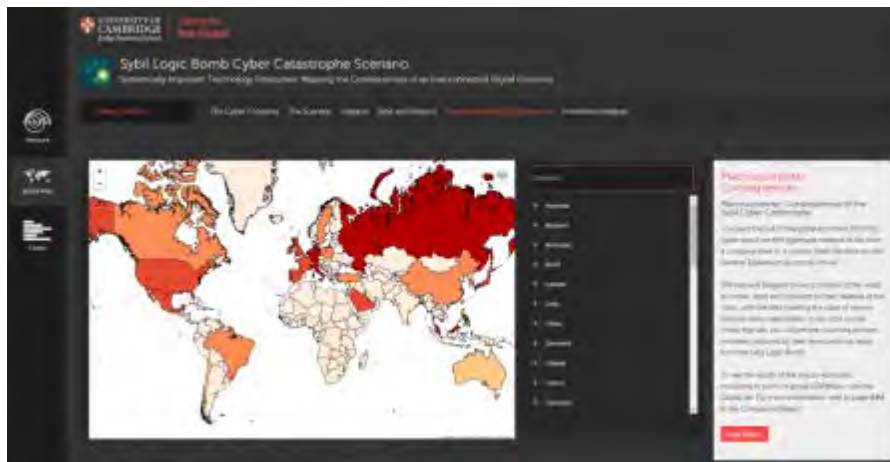
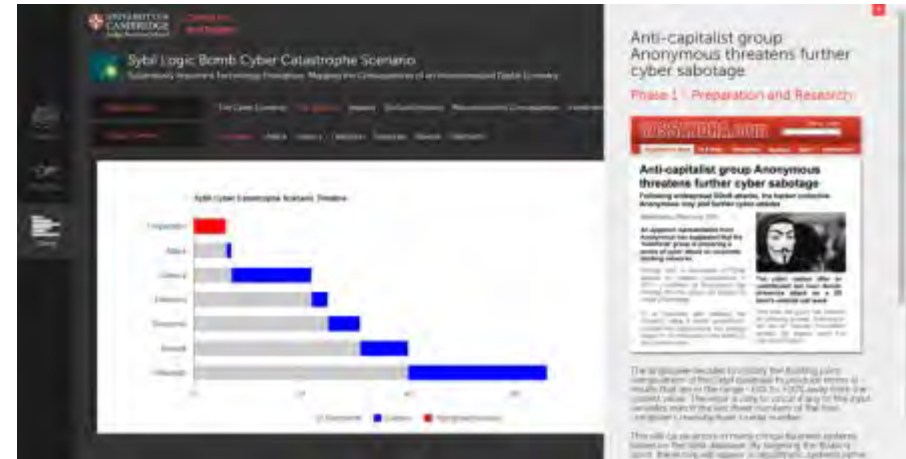
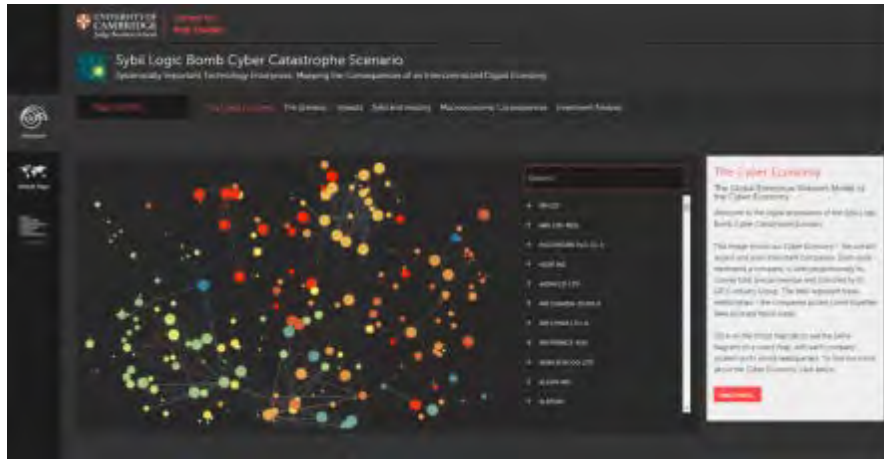
CYBER CATASTROPHE

HOW BAD COULD IT GET?

Cyber Catastrophe

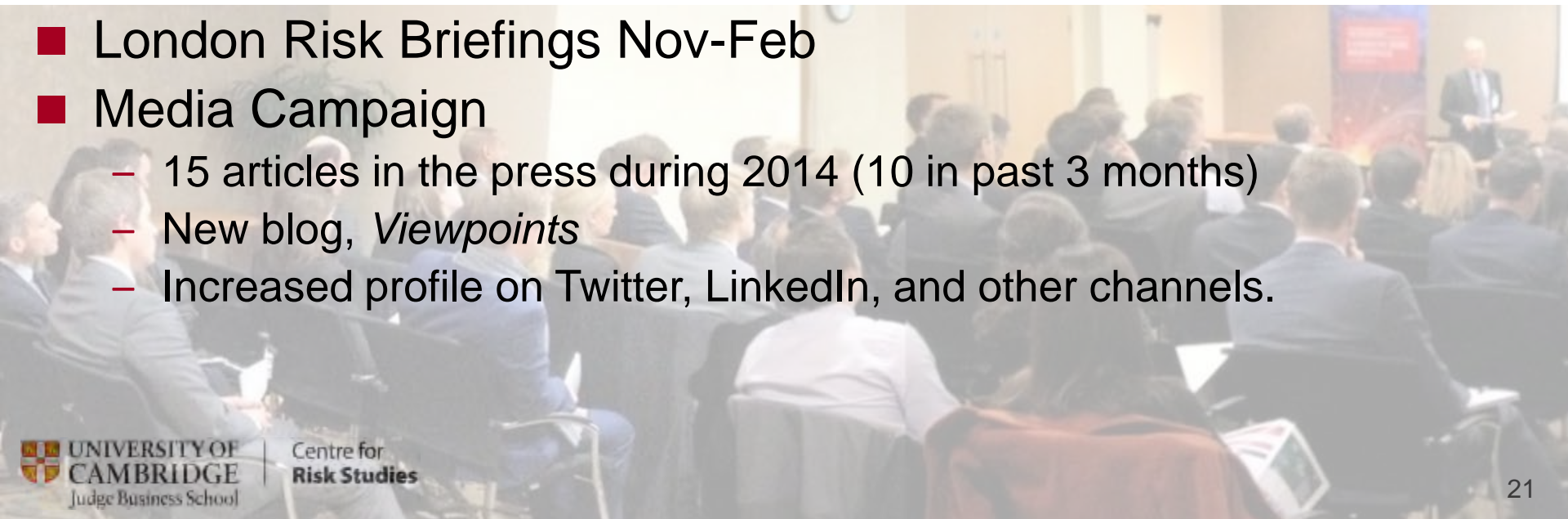
Online Digital Exploration of Sybil Logic Bomb

sybil.cambridgeriskframework.com



Broader Engagement & Dissemination in 2014

- *5th Annual Risk Summit* in June
 - Prefaced by Special Topics Seminar of work done in Centre
 - Attended by 150 senior executives and decision-makers
- Seminars, all fully subscribed
 - *Emerging Risks Scenarios* in March
 - *Insurability of Supply Chain Risk* in April
 - *Financial Risk and Networks* in September
- *Aspen Crisis and Risk Forum* in July
- London Risk Briefings Nov-Feb
- Media Campaign
 - 15 articles in the press during 2014 (10 in past 3 months)
 - New blog, *Viewpoints*
 - Increased profile on Twitter, LinkedIn, and other channels.



Research Programme 2015

■ Centre for Risk Studies'

- Research focuses on risk management in organisations
- 'Cambridge Risk Framework' provides common approach
 - Taxonomy: Range of threats, scenarios, and consequences
 - Range of systems at risk: firms, cities, regions, nations, infrastructure
 - Networks of relationships: trade, finance, information etc

■ Our research is built with and on our IT infrastructure

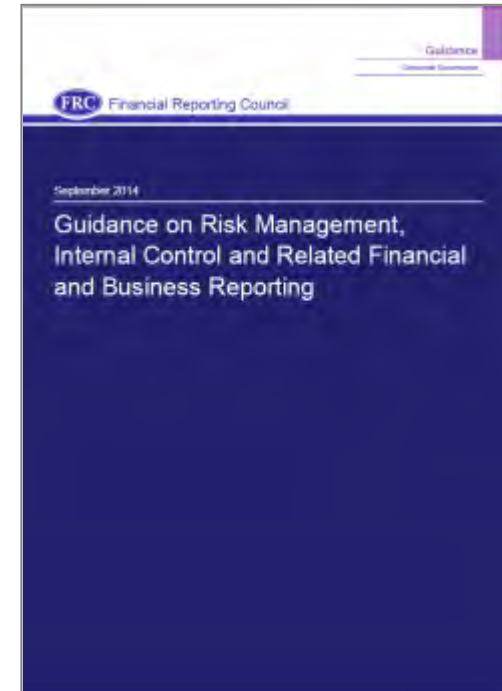
- Data, Maps, Networks, Analytics and Web Engines

■ Research Applications Areas for 2015

- Multi-Threat Economic Risk:** Understanding and quantifying the risk to the global economy from all threat types in taxonomy
- Financial Catastrophe Risk:** Managing tail risk of financial shocks in financial services & investment
- Cyber Catastrophe Risk:** A more rigorous framework for threats to critical and invisible infrastructure

Growing Pressure for Corporate Risk Reporting

- New UK regulations require annual reports to include explicit risk identification as part of strategic report
- Other moves towards 'balance sheet risk reporting'
 - Integrating Natural Disaster Risks & Resilience into the Financial System (Willis & Rowan Douglas, Capital, Science & Policy)
 - '1-in-100 movement' – standardized risk tests at 1% annual probability
- Potential drivers of external momentum:
 - UN Hyogo Framework renewal March 2015
 - R!SE
 - Financial Sector Initiative, UN Climate Action
 - UN Millennium & Sustainable Development Goals



Multi-Threat Economic Risk

What Threats do Corporate Executives Worry About?

Economic	Fiscal crises in key economies
	Failure of a major financial mechanism or institution
	Liquidity crises
	Structurally high unemployment/underemployment
	Oil-price shock to the global economy
	Failure/shortfall of critical infrastructure
	Decline of importance of the US dollar as a major currency
Environmental	Greater incidence of extreme weather events (e.g. floods, storms, fires)
	Greater incidence of natural catastrophes (e.g. earthquakes, tsunamis, volcanic eruptions, geomagnetic storms)
	Greater incidence of man-made environmental catastrophes (e.g. oil spills, nuclear accidents)
	Major biodiversity loss and ecosystem collapse (land and ocean)
	Water crises
	Failure of climate change mitigation and adaptation

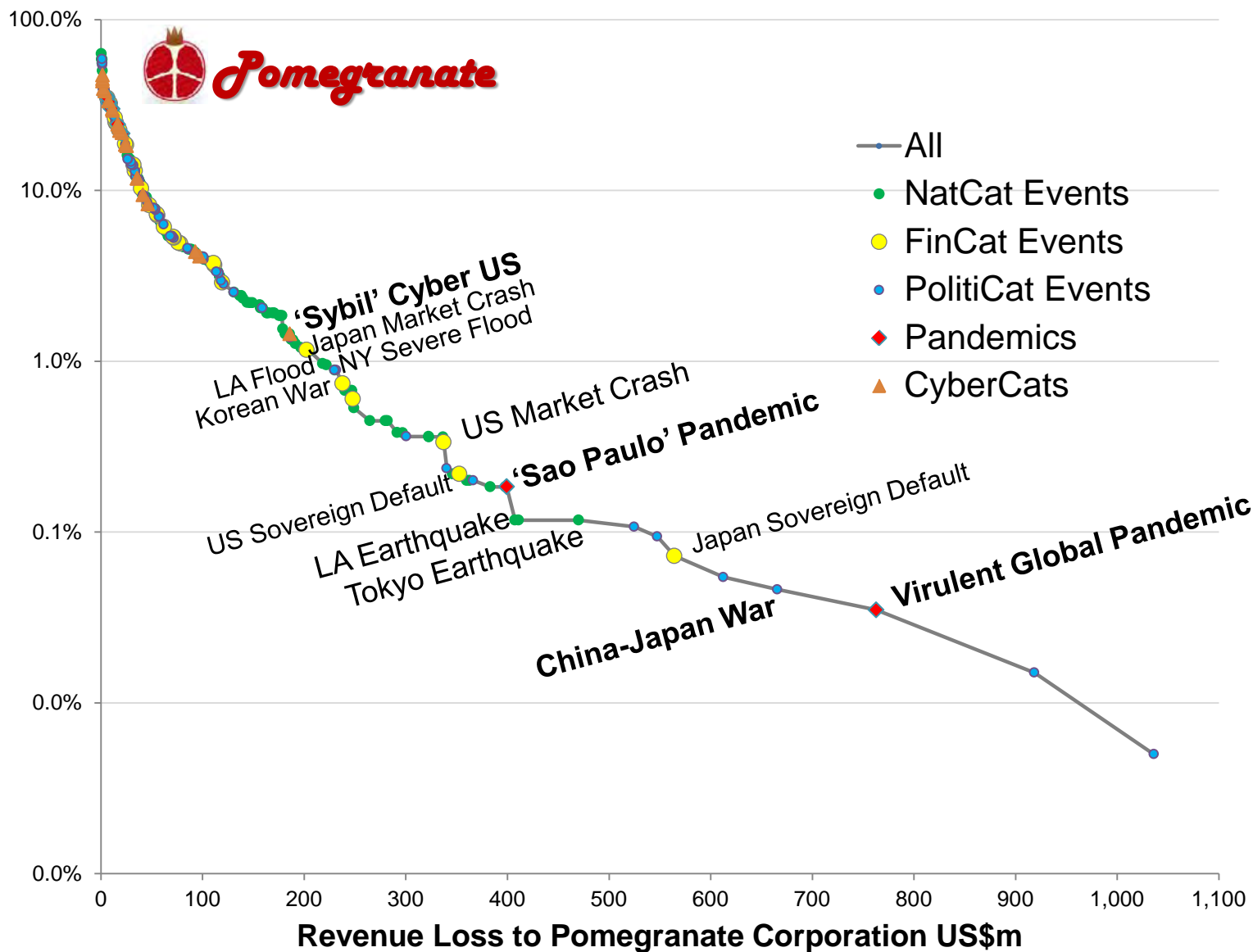
Geopolitical	Global governance failure
	Political collapse of a nation of geopolitical importance
	Increasing corruption
	Major escalation in organized crime and illicit trade
	Large-scale terrorist attacks
	Deployment of weapons of mass destruction
	Violent inter-state conflict with regional consequences
	Escalation of economic and resource nationalization
Societal	Food crises
	Pandemic outbreak
	Unmanageable burden of chronic disease
	Severe income disparity
	Antibiotic-resistant bacteria
	Mismanaged urbanization (e.g. planning failures, inadequate infrastructure and supply chains)
	Profound political and social instability
Technological	Breakdown of critical information infrastructure and networks
	Escalation in large-scale cyber attacks
	Massive incident of data fraud/theft



WEF Global Risks Perception Survey
Annual survey of current concerns and fears of 4,500 influential opinion-makers

Pomegranate 'Exceedance Probability' Curve

(Multi-Threat Economic Tail Risk on Log Scale)



Centre for
Risk Studies



UNIVERSITY OF
CAMBRIDGE
Judge Business School