Centre for Risk Studies **Research Showcase**
23 January 2014

A Research Framework for Complex Risks

Example of Cyber Catastrophe Risk

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Simon Ruffle
Director of Technology Research

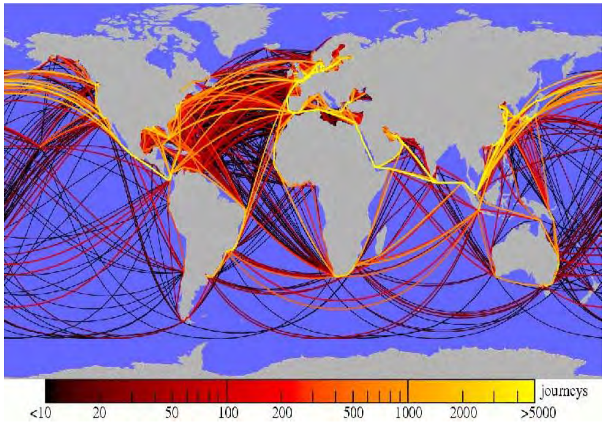
Catastrophe Modelling Meets Complex Systems

- The System Shock project arises from shared interests by the participants in exploring areas of intersection between
  - Catastrophe modelling and extreme risk analytics
  - Complex systems and networks failures
- Advance the scientific understanding of how systems can be made more resilient to the threat of catastrophic failures

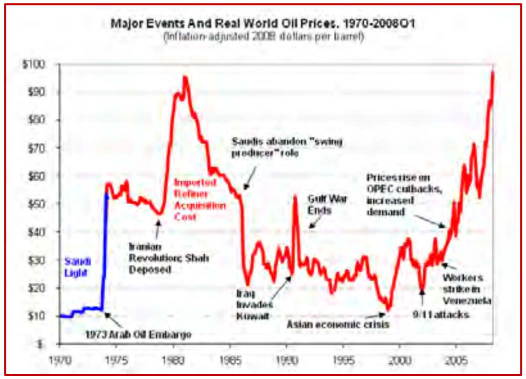
To answer questions such as:
'What would be the impact of
a [War in Taiwan] on the [Cargo Shipping Network] and how would this impact the [Oil Price]?

Regional Conflict

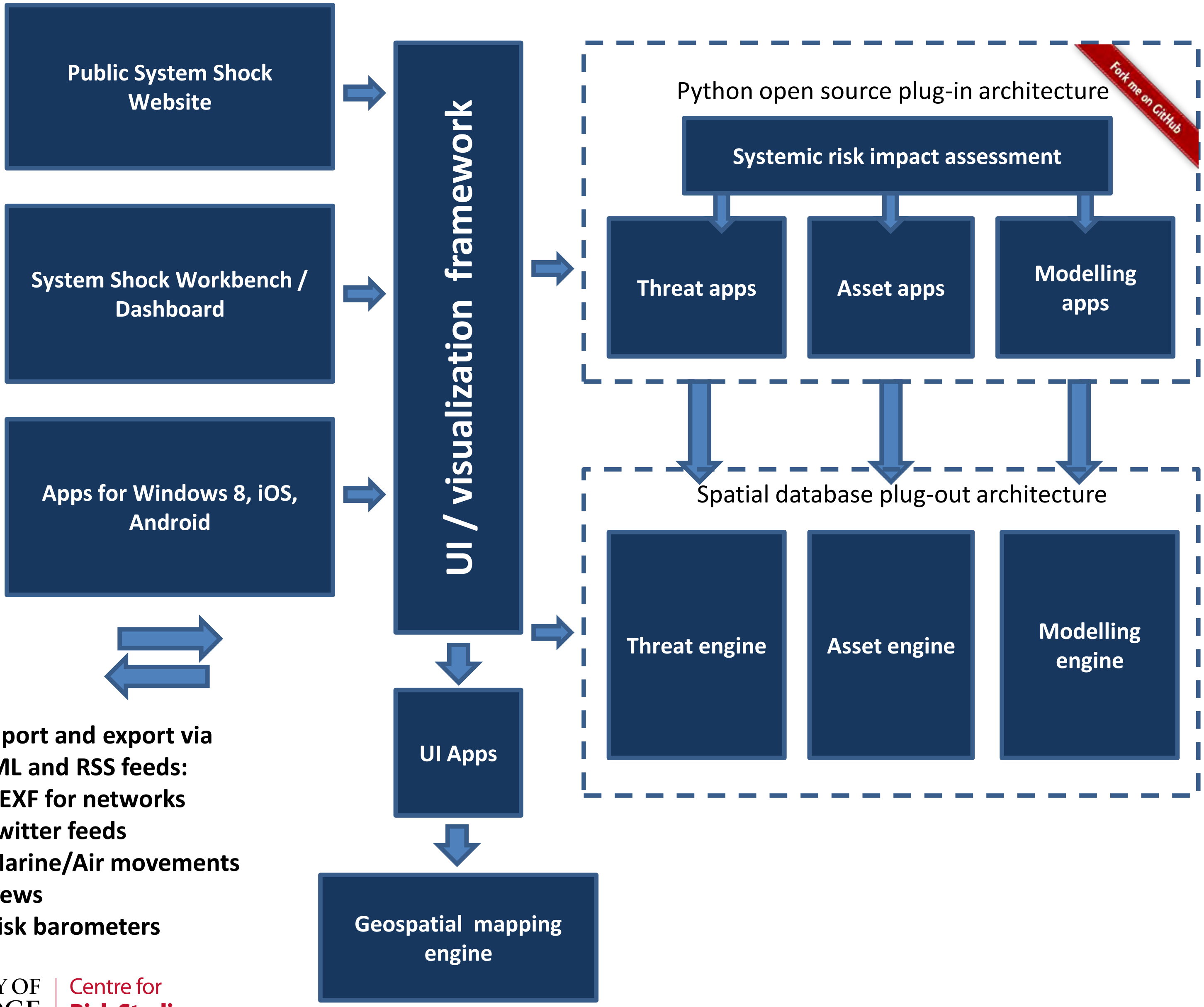
Cargo Shipping Network



Global Economy



The Cambridge Risk Framework



Public System Shock Website

System Shock Workbench / Dashboard

Apps for Windows 8, iOS, Android

UI / visualization framework

UI Apps

Geospatial mapping engine

Python open source plug-in architecture

Fork me on GitHub

Systemic risk impact assessment

Threat apps

Asset apps

Modelling apps

Spatial database plug-out architecture

Threat engine

Asset engine

Modelling engine

Import and export via XML and RSS feeds:
•GEXF for networks
•Twitter feeds
•Marine/Air movements
•News
•Risk barometers

UNIVERSITY OF CAMBRIDGE
Judge Business School

Centre for **Risk Studies**

Basic structure of Cambridge Risk Framework

- Scenario
- At-risk networked asset
- Model

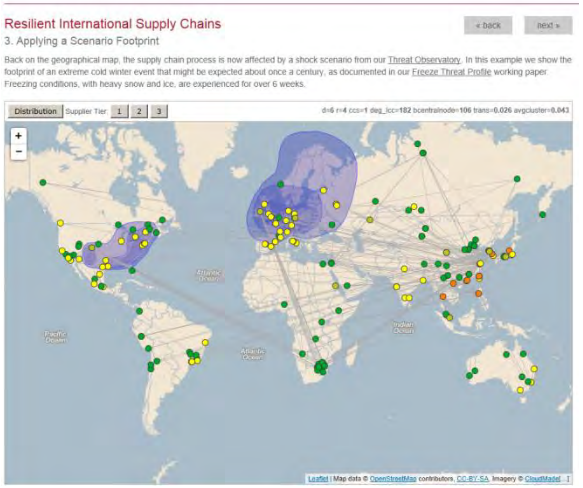
```
n = Network ( )
s = Scenario ( )
p = [parameters]
m = Model (s, p)
results = m.run_model(n)
```

Cambridge Risk Framework 2014

- Server side development
  - make more generic to give better support for modellers
  - “Risknode” standardisation
  - better mapping facilities
  - risk dashboard
  - support for multiple users
  - move to new server with VCS integration
- Client side development
  - improvements to user interface for network management and model use
  - user accounts & social networking
  - design of info-graphics for network and map visualisation

Network models 2013

- Resilient International Supply Chains (RISC)
  - Scenario: Freeze
  - At-risk networked asset: Consumer electronics supply chain
  - Model: Supply chain health


Resilient International Supply Chains

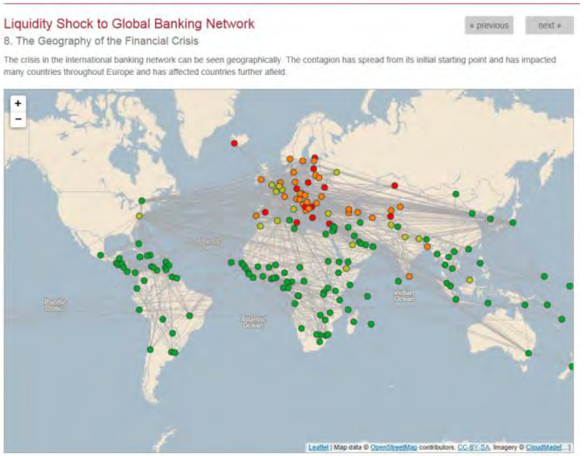
3. Applying a Scenario Footprint

Back on the geographical map, the supply chain process is now affected by a shock scenario from our Threat Observatory. In this example we show the footprint of an extreme cold winter event that might be expected about once a century, as documented in our Freeze Threat Profile working paper. Freezing conditions, with heavy snow and ice, are experienced for over 6 weeks.

d=6 r=4 ccs=1 deg_lcc=182 bcentralnode=106 trans=0.026 avgcluster=0.043

Leaflet | Map data © OpenStreetMap contributors, CC-BY-SA, Imagery © CloudMade

- Liquidity shock to global banking network (FinCat)
  - Scenario: Greece and Cyprus default
  - At-risk networked asset: Global interbank network
  - Model: Liquidity


Liquidity Shock to Global Banking Network

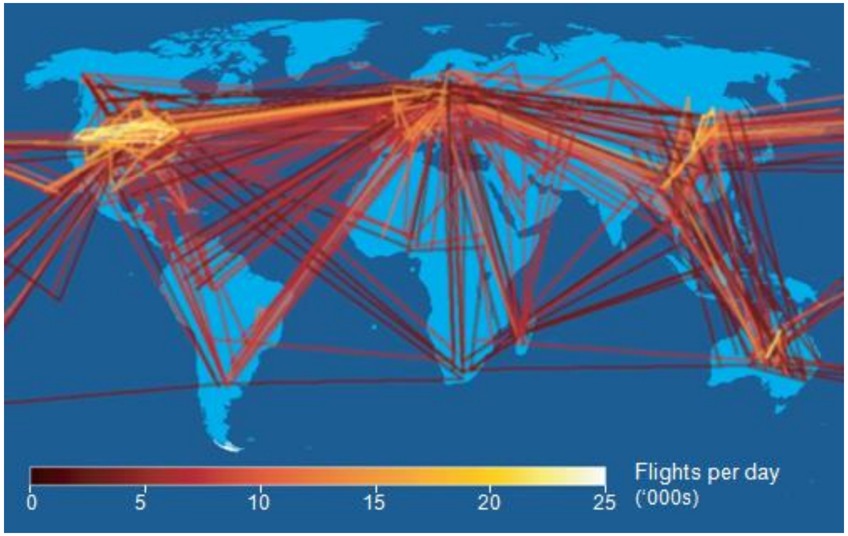
8. The Geography of the Financial Crisis

The crisis in the international banking network can be seen geographically. The contagion has spread from its initial starting point and has impacted many countries throughout Europe and has affected countries further afield.

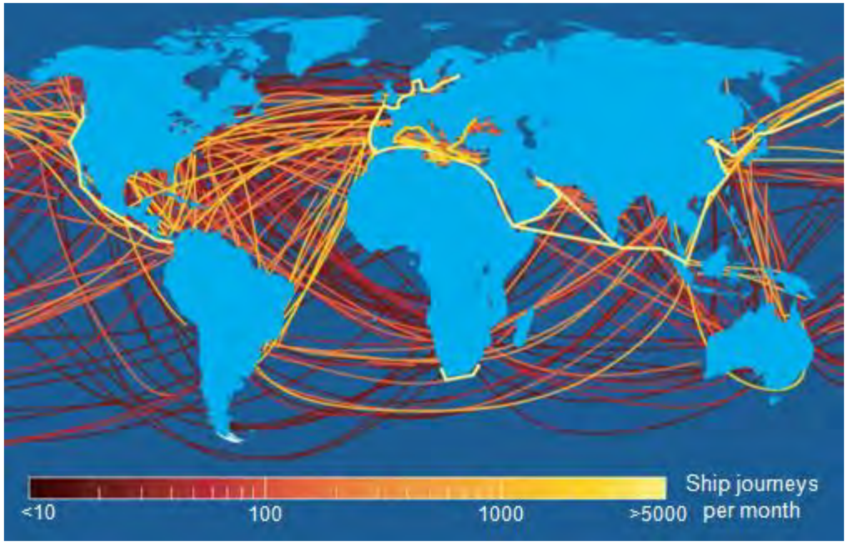
Leaflet | Map data © OpenStreetMap contributors, CC-BY-SA, Imagery © CloudMade

Business Activity as a System of Systems

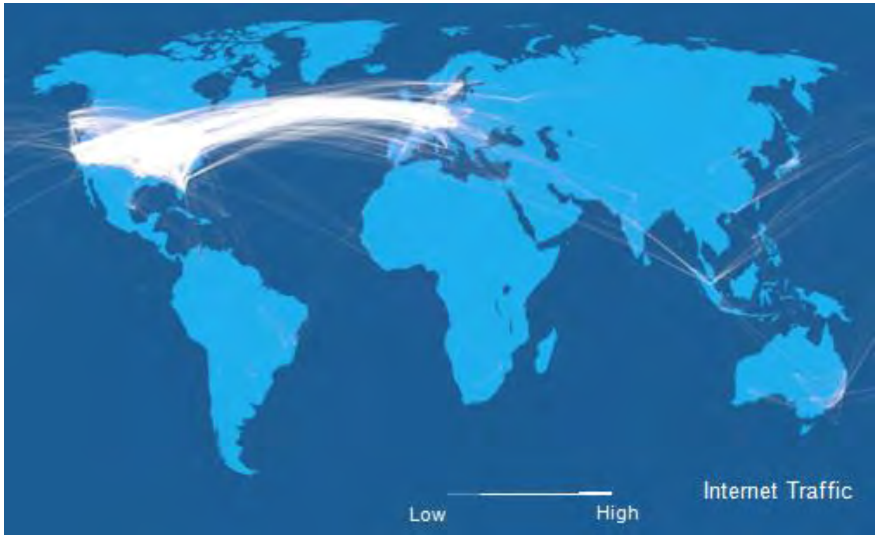
Air Travel Network



Cargo Shipping Networks



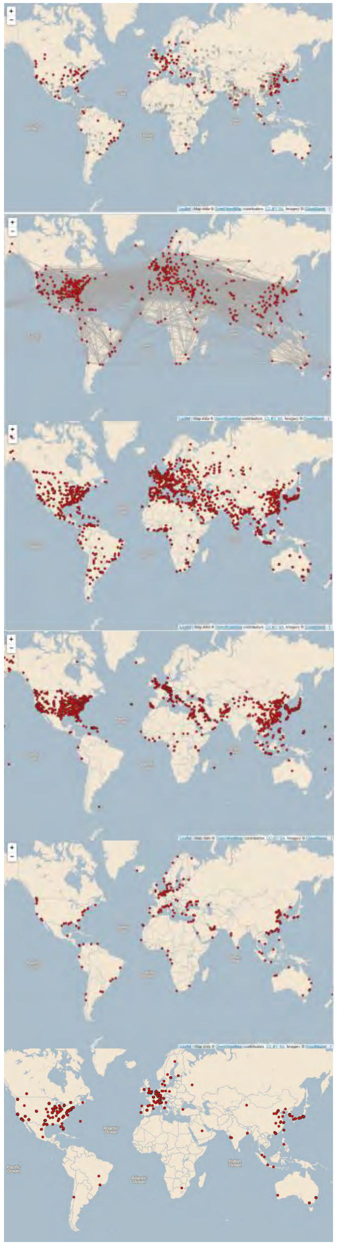
Communications Networks



UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

Global Substrate Data

Utilities	🔴	Water & sewerage
Energy	🟡	Electricity
	🟡	Gas
	🟡	Oil
Transportation	🔴	Roads
	🟡	River & sea
	🔴	Rail
	🟢	Air
Telecommunications	🟡	Data
	🟡	Telephony
	🔴	Broadcasting
Geography	🟡	Countries
	🟢	Cities
	🟡	Military power structure
Trade	🟡	Inter country
	🟡	Inter enterprise
Finance	🟡	Inter bank



- *continuing data gathering, validation and curatorship needed*

Enterprise Model of the Global Economy

- GICS Sectors and Industry Groups
- 600 Companies from Bloomberg Industry Leaderboard
- Data sourced electronically from Bloomberg Data Service.
- Includes inter-enterprise relationship value
- Will be known as **Cambridge Global Enterprise Network**

GICS: Global Industry Classification Standard

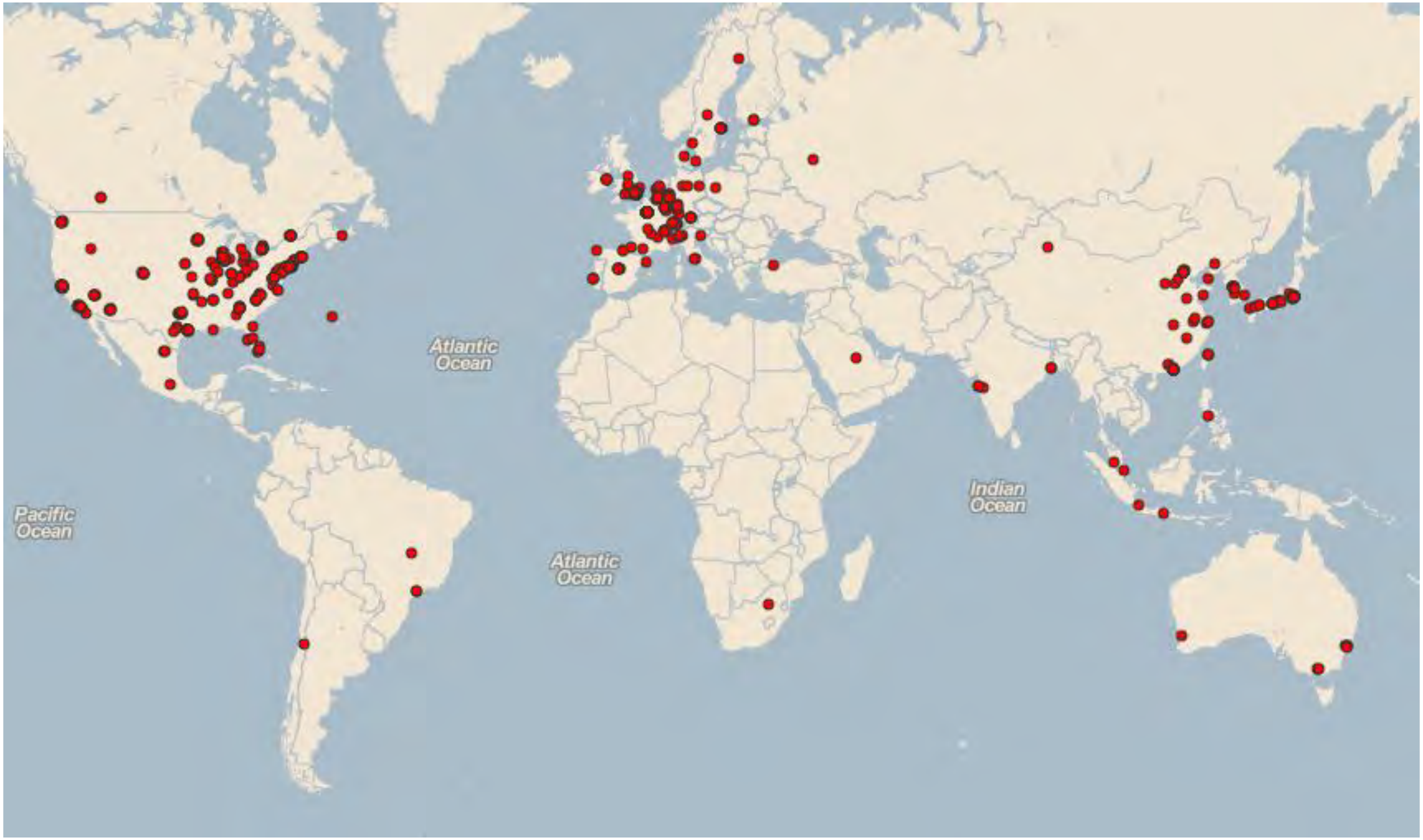
Code	Sector	Sub-code	Industry Groups
10	Energy	1010	Energy
15	Materials	1510	Materials
20	Industrials	2010	Capital Goods
		2020	Commercial & Professional Services
		2030	Transportation
25	Consumer Discretionary	2510	Automobiles & Components
		2520	Consumer Durables & Apparel
		2530	Hotels Restaurants & Leisure
		2540	Media
		2550	Retailing
30	Consumer Staples	3010	Food & Drug Retailing
		3020	Food, Beverage & Tobacco
		3030	Household & Personal Products
35	Health Care	3510	Health Care Equipment & Services
		3520	Pharmaceuticals & Biotechnology
40	Financials	4010	Banks
		4020	Diversified Financials
		4030	Insurance
		4040	Real Estate
45	Information Technology	4510	Software & Services
		4520	Technology Hardware & Equipment
		4530	Semiconductors & Semiconductor Equipment
50	Telecommunication Services	5010	Telecommunication Services
55	Utilities	5510	Utilities

Group Overview of Global Enterprise Network

GICS Industry group	Revenue $M	Market capitalization $M	Total Assets $M	Total net income $M	Group count	Largest company in group by revenue
Energy	3,488,146	2,103,734	2,782,799	199,111	26	Royal Dutch Shell
Capital Goods	1,809,936	1,696,063	2,720,030	83,475	51	GE
Automobiles & Components	1,650,500	1,047,564	2,174,869	93,683	20	Volkswagen
Food & Staples Retailing	1,589,257	718,066	845,492	37,153	32	Wal Mart
Materials	1,247,870	1,124,244	1,832,520	30,866	51	BASF
Insurance	1,021,092	633,572	6,935,800	35,164	15	AXA
Banks	1,001,307	1,417,398	21,904,310	171,605	11	Ind & Comm Bank of China
Utilities	921,225	616,360	2,195,734	38,609	20	E.ON
Telecommunication Services	878,367	1,146,448	1,781,938	49,058	13	AT&T
Food Beverage & Tobacco	859,389	1,771,726	1,201,074	91,147	28	Nestle
Retailing	812,430	915,998	504,457	27,069	50	Home Depot
Diversified Financials	803,811	1,493,539	15,197,549	74,560	17	Berkshire Hathaway
Transportation	633,843	587,901	772,813	19,936	30	Deutsche Post
Pharmaceuticals, Biotechnology	570,966	2,150,694	1,178,017	98,014	22	Johnson & Johnson
Technology Hardware & Equipment	540,277	831,777	591,372	56,047	11	Apple
Software & Services	480,629	2,013,484	741,814	90,516	23	IBM
Consumer Durables & Apparel	382,640	375,870	463,597	2,279	34	Panasonic
Media	381,723	669,312	711,340	28,112	37	Comcast
Health Care Equipment & Services	358,884	323,586	388,328	18,749	12	United Health
Semiconductors & Semiconductor	247,781	440,648	311,741	25,719	12	Samsung
Household & Personal Products	226,135	591,998	301,053	26,829	9	Proctor & Gamble
Consumer Services	217,895	528,309	293,487	11,918	40	McDonalds
Real Estate	155,119	455,507	763,517	25,061	30	Brookfield
Commercial & Professional Services	2,065	3,349	2,160	118	1	Regus

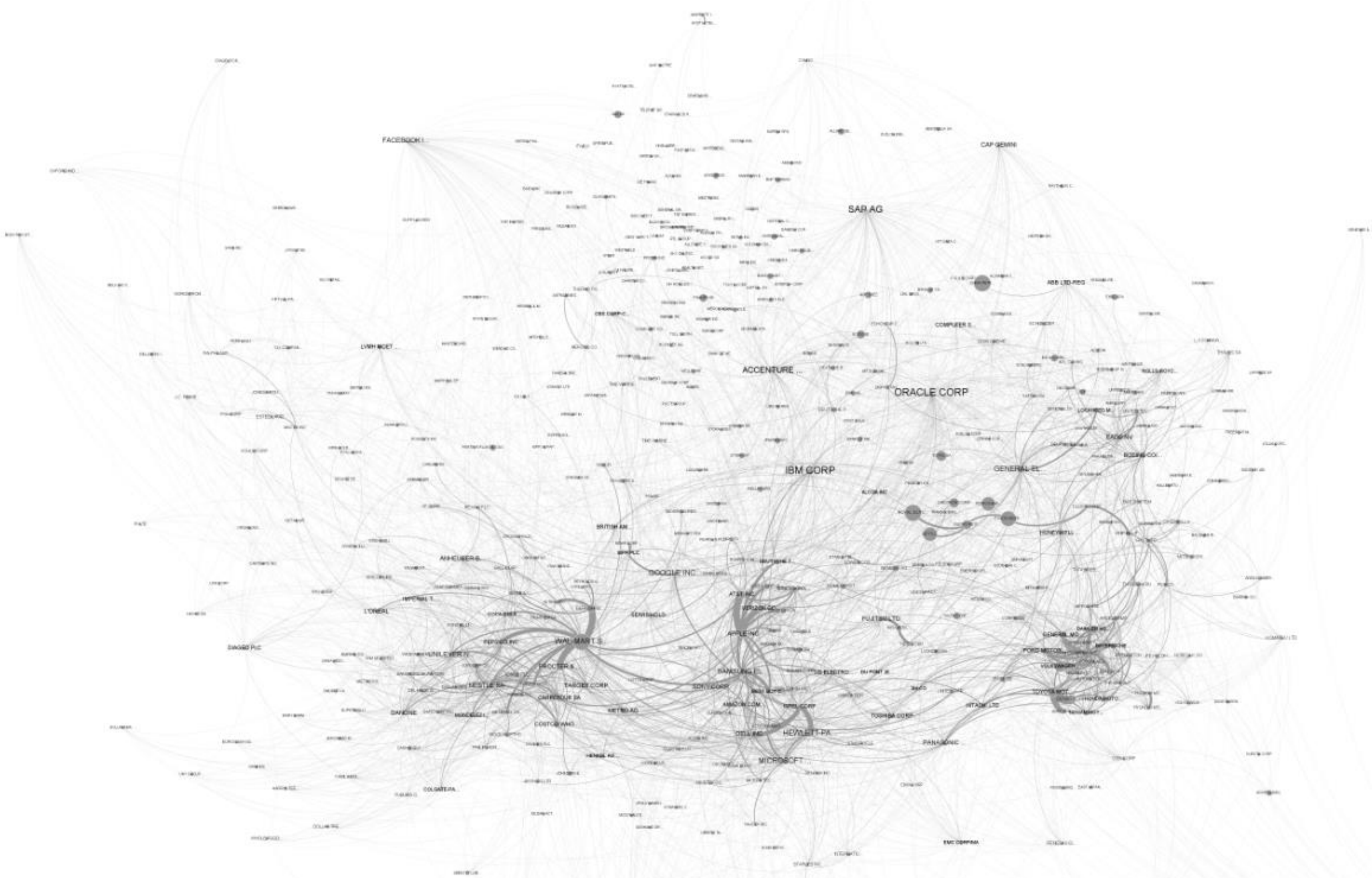
Using GICS (Global Industry Classification Standard) Industry Groups. Source: Bloomberg, retrieved 3rd January 2014. Ranked by revenue. N=595.

Global Enterprise Network



The 600 enterprises with the location of their corporate HQs mapped

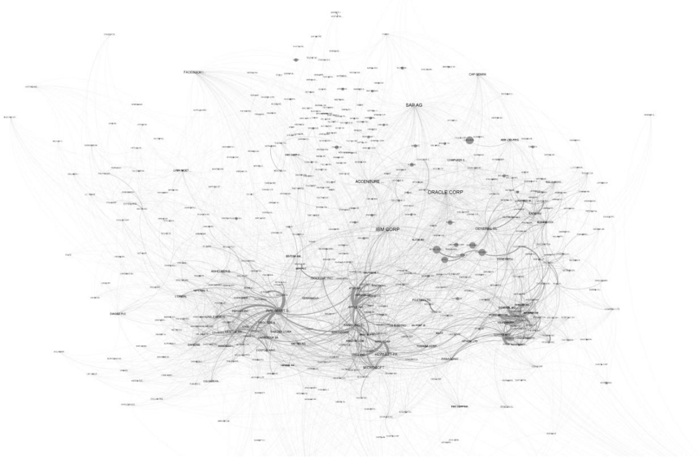
Global Enterprise Network



475 out of 600 enterprises that have relationships shown on a force-directed graph, node radius = revenue; label size = degree

Network models 2014

- Cambridge Global Enterprise Network
  - driven forward by LMCO Cyber
  - subsume supply chain?
- Financial Catastrophe
- Other scenario specific
  - which?
- The Cartography of Finance
- Sea container cargo
  - in collaboration with Jasmine Lee, NTU



J.S.L. Lam / Journal of Transport Geography 19 (2011) 366–374

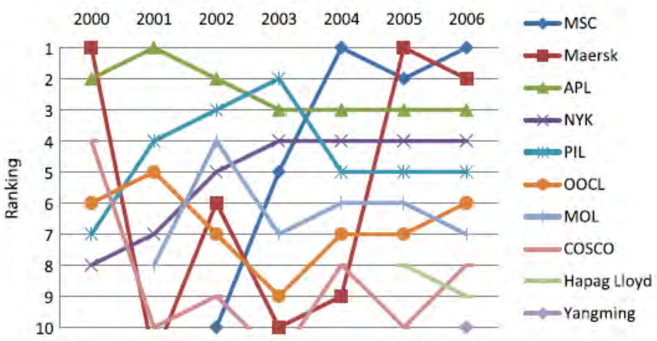


Fig. 1. The top 10 lines connected to the port of Singapore in terms of slot capacity deployed (2000–2006).

Cyber Catastrophe

Subject Matter Editors

IOActive™

Éireann Leverett

Security Researcher, IOActive

Works in the Industrial Systems Security team at IOActive, Studied Advanced Computer Science in Cambridge's computer security group. Specialises in industrial system security incidents and cyber risk management in the corporate sector.

UNIVERSITY OF CAMBRIDGE

Dr. Rob Watson

Security Research Group, University of Cambridge Computer Laboratory

University Lecturer in Systems, Security, and Architecture in the Security Research Group at the University of Cambridge Computer Laboratory. Specialist in operating system security extensibility.

Dr. Richard Clayton

Security Research Group, University of Cambridge Computer Laboratory

Software developer who specialises in digital crime, with research into email spam, fake bank "phishing" websites, and other Internet wickedness. As an expert in these areas, he is a regular speaker and media commentator.

Dr. Frank Stajano

Senior Lecturer, University of Cambridge Computer Laboratory

Specialist in systems security with particular interest in the human aspects of systems security. Frank is the author of the book *Security for Ubiquitous Computing*.

Cyber Event catalogue

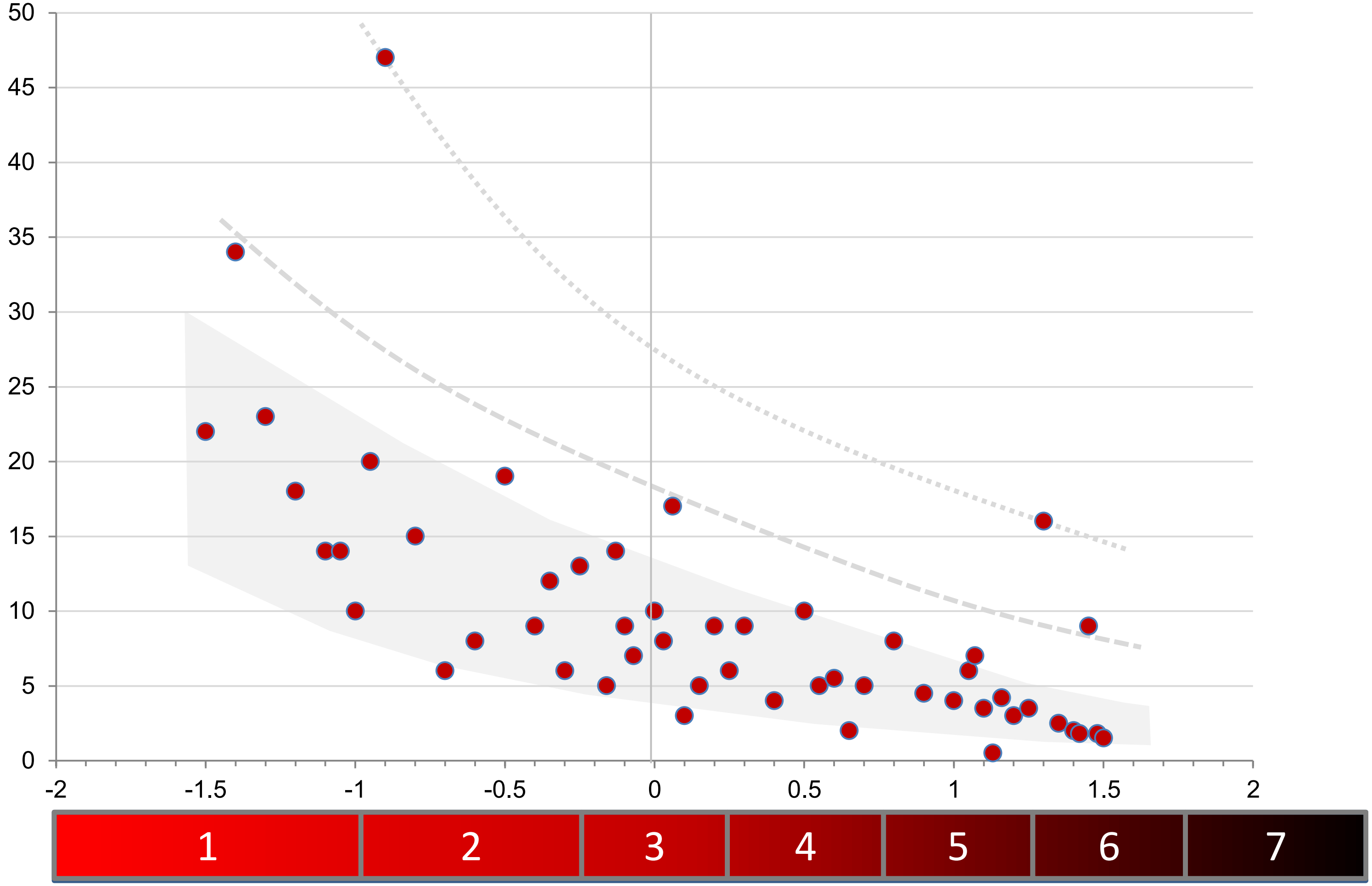
			Theft	Disruption	Damage
ILOVEYOU	2000	2 🟨🟨			🟦
MafiaBoy	2000	1 🟨			🟦
Code Red	2001	2 🟨🟨			🟦
SQL Slammer	2003	1 🟨			🟦
MyDoom	2004	2 🟨🟨		🟦	
Sasser	2004	1 🟨		🟦	
Titan Rain	2004	3 🟨🟨🟨	🟦		
TJX	2005	3 🟨🟨🟨	🟦		
APT1	2006	4 🟨🟨🟨🟨	🟦		
Conficker	2007	2 🟨🟨		🟦	
Zeus	2007	3 🟨🟨🟨	🟦		
Estonian Cyber attack	2007	3 🟨🟨🟨		🟦	
Heartland	2008	2 🟨🟨	🟦		
RBS WorldPay	2008	3 🟨🟨🟨	🟦		
Stuxnet	2010	4 🟨🟨🟨🟨			🟦
Operation Aurora	2010	4 🟨🟨🟨🟨	🟦		
Epsilon	2011	3 🟨🟨🟨	🟦		
Sony Playstation	2011	2 🟨🟨	🟦		
Citigroup	2011	3 🟨🟨🟨	🟦		
RSA	2011	4 🟨🟨🟨🟨	🟦		
Operation Ababil	2012	2 🟨🟨		🟦	
Shamoon	2012	1 🟨			🟦
Flame / Skywiper	2012	4 🟨🟨🟨🟨	🟦		
The Unlimited Operation	2012	3 🟨🟨🟨	🟦		
CloudFlare	2013	2 🟨🟨		🟦	
ObamaTwitter Scare	2013	4 🟨🟨🟨🟨		🟦	

Cyber Event Magnitude Scale

Magnitude Scale Value	Threat profile	Typical perpetrator profile	Motivation	Time scale	Covert-ness	Resources	Historic precedents
Magnitude **1** Cyber Hazard	Undirected attack using a single cyber attack technique	Lone bedroom hacker; "script kiddie"	Curiosity; notoriety	Short	Low	Low	SQL Slammer, Mafia Boy
Magnitude **2** Cyber Hazard	Directed attack on defined targets using single cyber attack technique	Group of hackers; online buddies; hacktivists	Notoriety; activism; political	Short	Medium	Low	Sony Playstation, Conficker
Magnitude **3** Cyber Hazard	Directed attack using mix of cyber attack techniques, kinetics and social engineering	Malicious insider; organised crime; "hacker-backer-casher"	Revenge; political; financial	Medium	Medium	Medium	Unlimited Operation
Magnitude **4** Cyber Hazard	As 3 but with addition of more development resources, testing facilities, increased covertness and kinetics. Systemic impact.	Security agency in peacetime mode; Mafia grade criminal organisation	Financial; political	Long	High	High	APT1, Stuxnet
Magnitude **5** Cyber Hazard	As 4 but with military grade resources and intensity of attack. Systemic impact.	Electronic army; nation state	Political; military	Long	High	High	

Vulnerability to Cyber Attack with Security Score

Losses from Cyber Attacks
Annualized
$ million



Cyber Security Index

The Security Effectiveness Score (SES) has been developed by PGP Corporation and Ponemon Institute in its annual encryption trends survey to define the security posture of responding organizations. The SES is derived from the rating of 24 security features or practices. This method has been validated from more than 30 independent studies conducted since June 2005. The SES provides a range of +2 (most favorable) to -2 (least favorable). Hence, a result greater than zero is viewed as net favorable.

Ponemon INSTITUTE

UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for **Risk Studies**

Vulnerability : Cyber Security Index (CSI)

Magnitude Scale Value	Typical security posture	SES Score
1 Cyber Vulnerability	(Most vulnerable) No security posture: Old operating system; no regular updates; no firewalls; no antivirus; no restrictions on websites visited; email attachments regularly opened.	-2
2 Cyber Vulnerability	Average domestic security posture: Modern operating system; automatic updates; antivirus; firewall; average email and website hygiene. Weak passwords, poor backup strategy.	-1
3 Cyber Vulnerability	Average organization security posture: Add regular backups; strong passwords;	0
4 Cyber Vulnerability	Average corporate IT security posture: Add thin clients; remote workstation management; strict restriction on which websites can be visited; strict email spam filtering;	1
5 Cyber Vulnerability	Above average corporate IT security posture: Add board level commitment to security; published corporate security guidelines; regular staff training; strict BYOD rules; removable media bans.	1,2
6 Cyber Vulnerability	E-service supplier security posture: Add wide use of encryption; use of security intelligence consultants; testing of updates; extensive cyber threat monitoring; mirror servers; duplicate data centres;	2
7 Cyber Vulnerability	(Least vulnerable) Military grade security posture: Add air gaps; decoy systems; cyber retaliation	Above 2

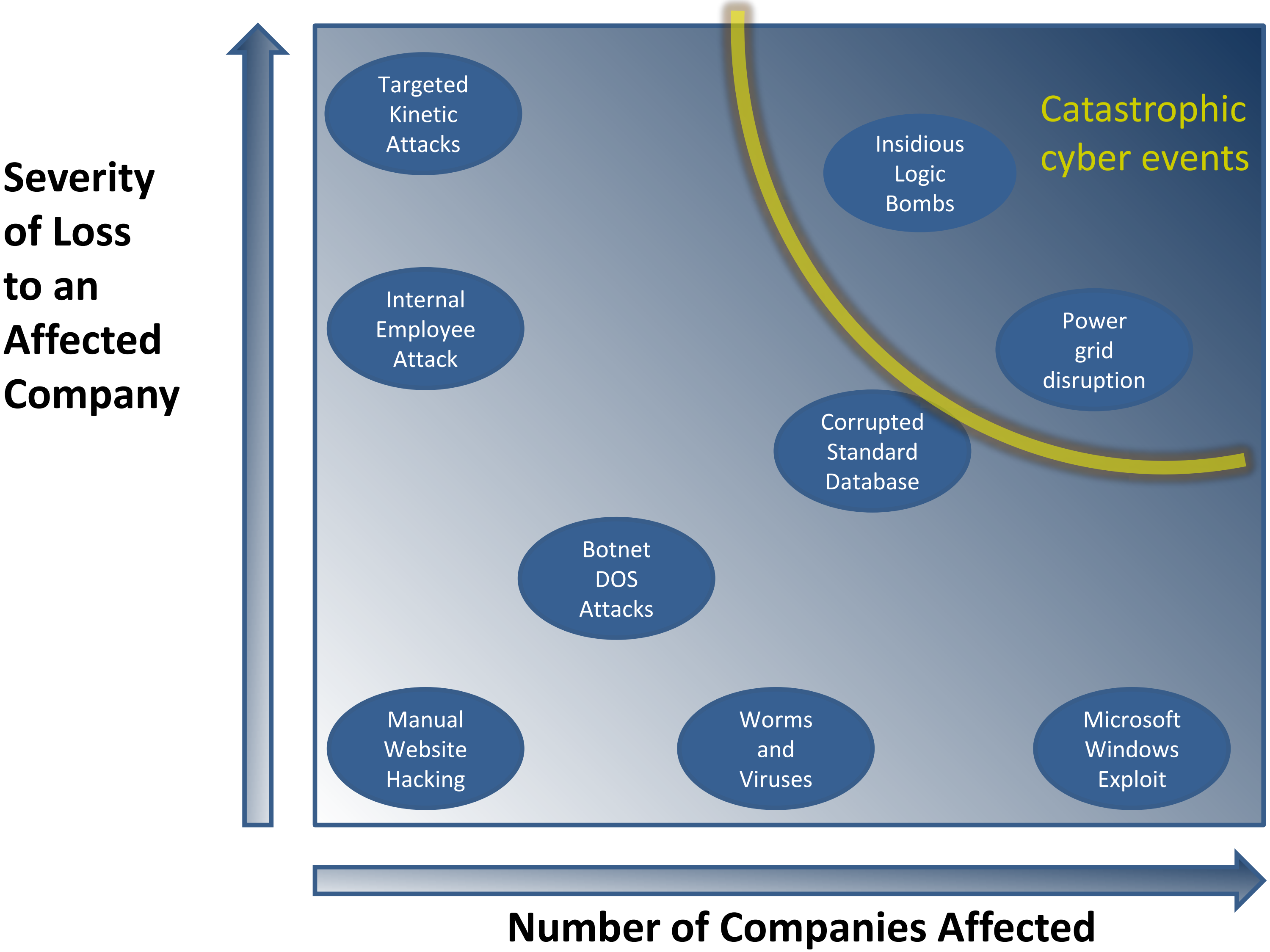
Average vulnerability by industry

GICS Industry Group	Vulnerability	Average vulnerability: Cyber Security Index (CSI)	Rationale
Utilities	HIGH	3	Average SME organization security posture: Regular backups; strong passwords.
Diversified financials	MEDIUM	4	Average corporate IT security posture: Thin clients; remote workstation management; strict restriction on which websites can be visited; strict email spam filtering;
Insurance	MEDIUM	5	Above average corporate IT security posture: Board level commitment to security; published corporate security guidelines; regular staff training; strict BYOD rules; removable media bans.
Banks	LOW	6	E-service supplier security posture: Wide use of encryption; use of security intelligence consultants; testing of updates; extensive cyber threat monitoring; mirror servers; duplicate data centres;

Catalogue of IT failures

GICS Industry group	Type of failure	Real life precedents
Automobiles & Components	**Robotic manufacturing failure causes loss of production**	"Ping Sweep": Robotic arm out of control
Banks	**Bad data leads to write-down**	National Australia Bank, 2001:HomeSide write-downs, $2.2Bn loss
Insurance	**Corruption of scanned paper based customer records**	Xerox WorkCentre Document Scanning Flaw
Diversified financials	**Algorithmic trading losses**	Flash Crash, Knight Capital $450m loss, AXA Rosenberg $250m loss
Semiconductors	**Losses to high value items in production**	Semiconductor fabrication production line failure: $50,000 damage
Pharmaceuticals & Biotechnology	**Financial forecasts and reports wrong**	AstraZenica spread sheet error sends wrong data to sell side analyst community, 2012.
Media	**Event overbooking, loss of consumer confidence**	Locog spread sheet error causes Olympic ticket overselling, 2011
Energy	**Unable to send gas through pipeline**	Penetration test locks up SCADA system of gas utility for 4 hours.
Utilities	**Contractual errors lead to losses**	Transalta: $25m charge due to wrong transmission hedging contracts
Utilities	**Environmental Damage lead to liability claims and fines.**	Maroochy Shire Incident, 2000: 800,000L raw sewage spill in 47 separate incidents

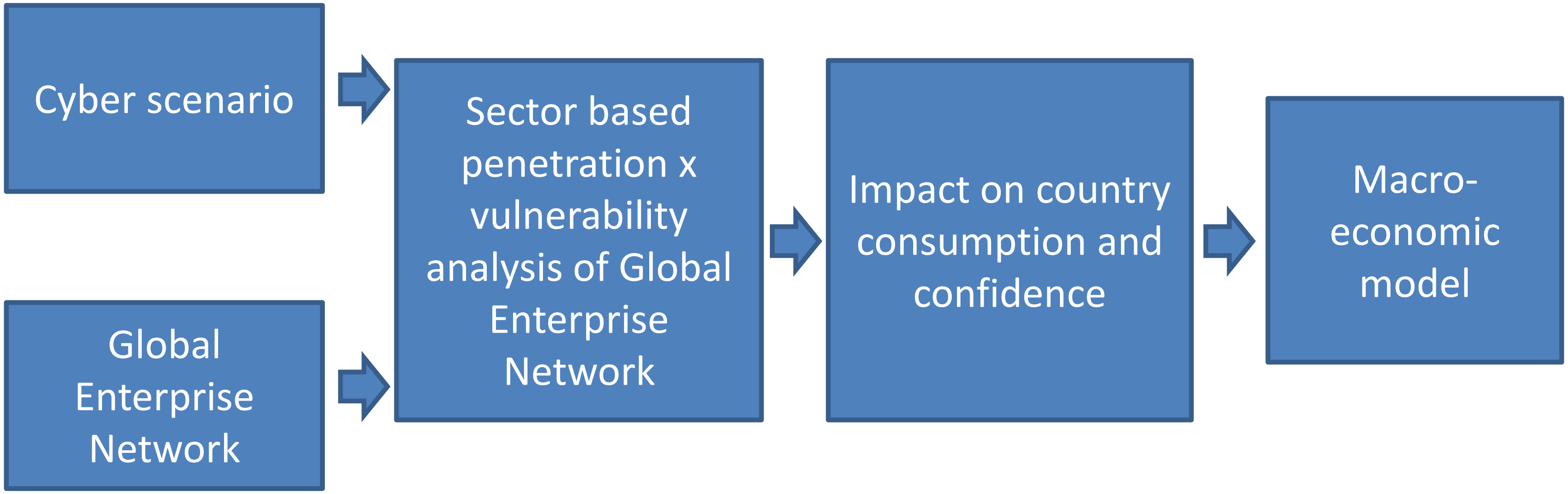
Scenario definition



Mapping the Cyber Economy: The Cambridge Global Enterprise Network

- Can we construct a model of the inputs and outputs of large corporations, in a similar way to classic Input/Outputs models of countries?
- ‘Multi-Enterprise, Multi-Regional Input Output Model’ (MEMRIO)
- Construct analysis tables from economic data produced by governments, blended with financial and other data on individual enterprises
- Assume each enterprise behaves according to its sector average until specific data is available about them
- Reflect the scale and structure of the world’s largest enterprises across regions and sectors
  - Take into account the full complexity of global supply chains
  - Remove any double-counting caused by the fact that the enterprises included in the analysis may fall within one another’s supply chains
  - deal with the uncertainty faced by an outside observer who may be under-informed about the detailed purchasing and sales structure of the enterprise in question

Cyber catastrophe macro-economic impact modelling



Cyber scenario

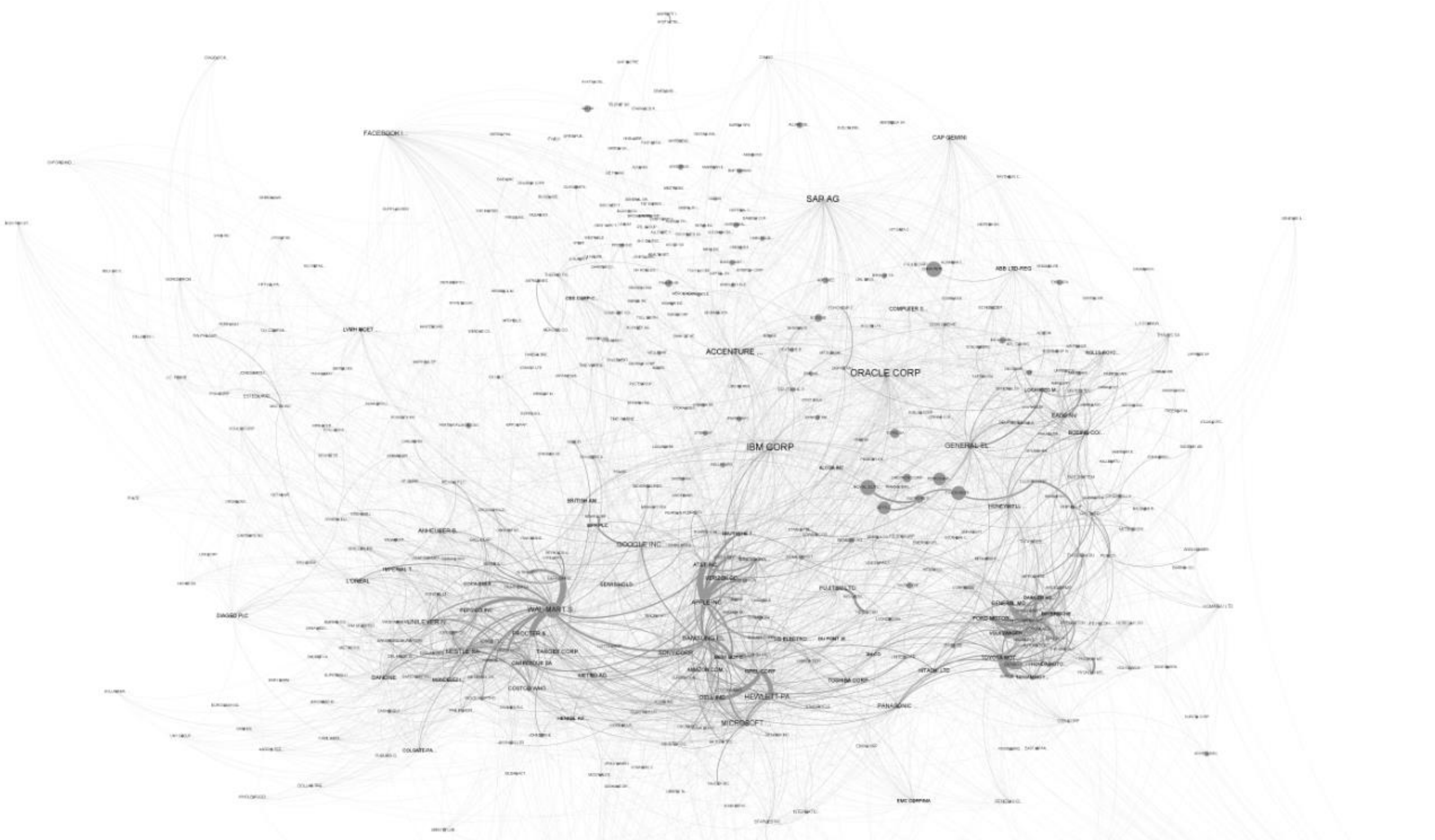
Global Enterprise Network

Sector based penetration x vulnerability analysis of Global Enterprise Network

Impact on country consumption and confidence

Macro-economic model

Global Enterprise Network



475 out of 600 enterprises that have relationships shown on a force-directed graph, node radius = revenue; label size = degree

UNIVERSITY OF CAMBRIDGE
Judge Business School

Centre for
Risk Studies

Cyber Catastrophe Risk 2014

- Meet Subject Matter Experts
- More detailed historic catalogue
- Calibration through precedence studies of past IT failures
- Cambridge Global Enterprise Network as basis of "Enterprise Model of the Cyber Economy"
- Meet industrial sector experts?
- Cyber scenario complete with macro-economic modelling
- Completion of Cyber Threat Monograph
- Partnerships? Priorities?