

Cambridge Judge Business School

Cambridge Centre for Risk Studies 2018 Risk Summit

# CYBER TERRORISM THREAT INTELLIGENCE AND LOSS MODELLING

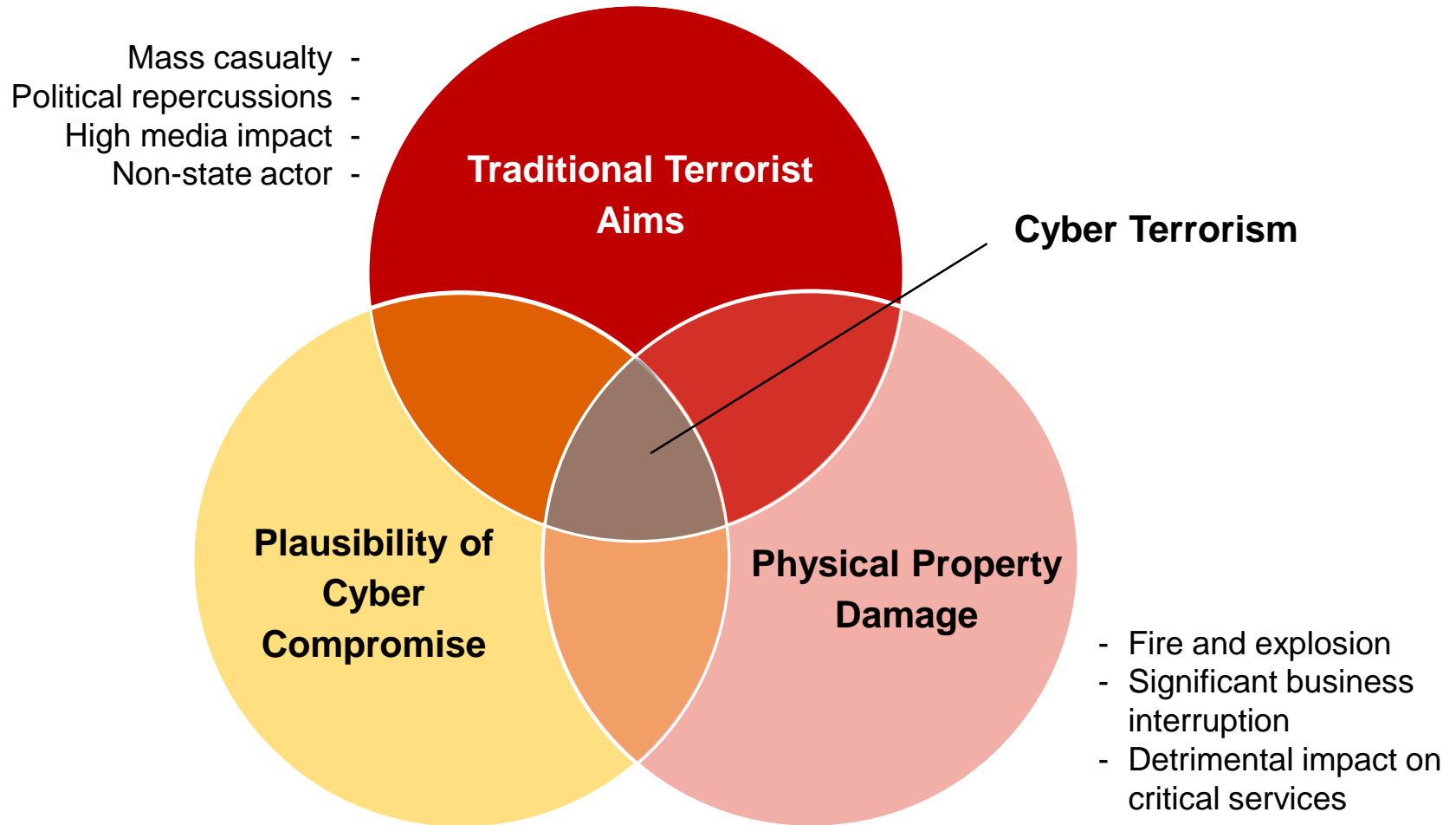
**Tamara Evan**, Research Assistant  
Centre for Risk Studies

Centre for  
**Risk Studies**

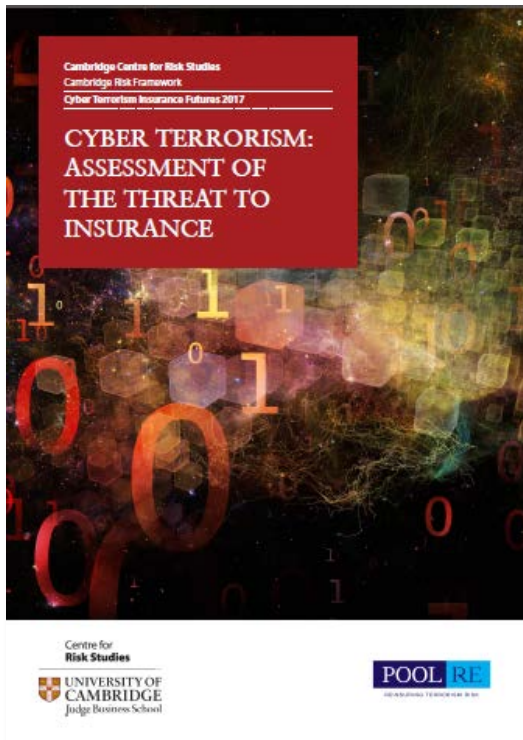


UNIVERSITY OF  
CAMBRIDGE  
Judge Business School

# Defining cyber terrorism



# Pool Re extends cover for losses from cyber terrorism



- 2016 -2017 Cyber Terrorism Insurance Futures methodology
  - Expert revision schemes for proposed scenario long-lists
  - Monitoring capabilities of terrorist threat groups
    - Quarterly updates on threat development and thematic changes
  - Creation of low-probability cyber terrorism scenarios
  - In-depth study of key loss processes
  - Treasury granted permission to Pool Re's extension of retrocession cover for losses from acts of cyber terror in August 2017
- 2017 Report: **Cyber Terrorism: Assessment of the Threat to Insurance**, launched November 2017



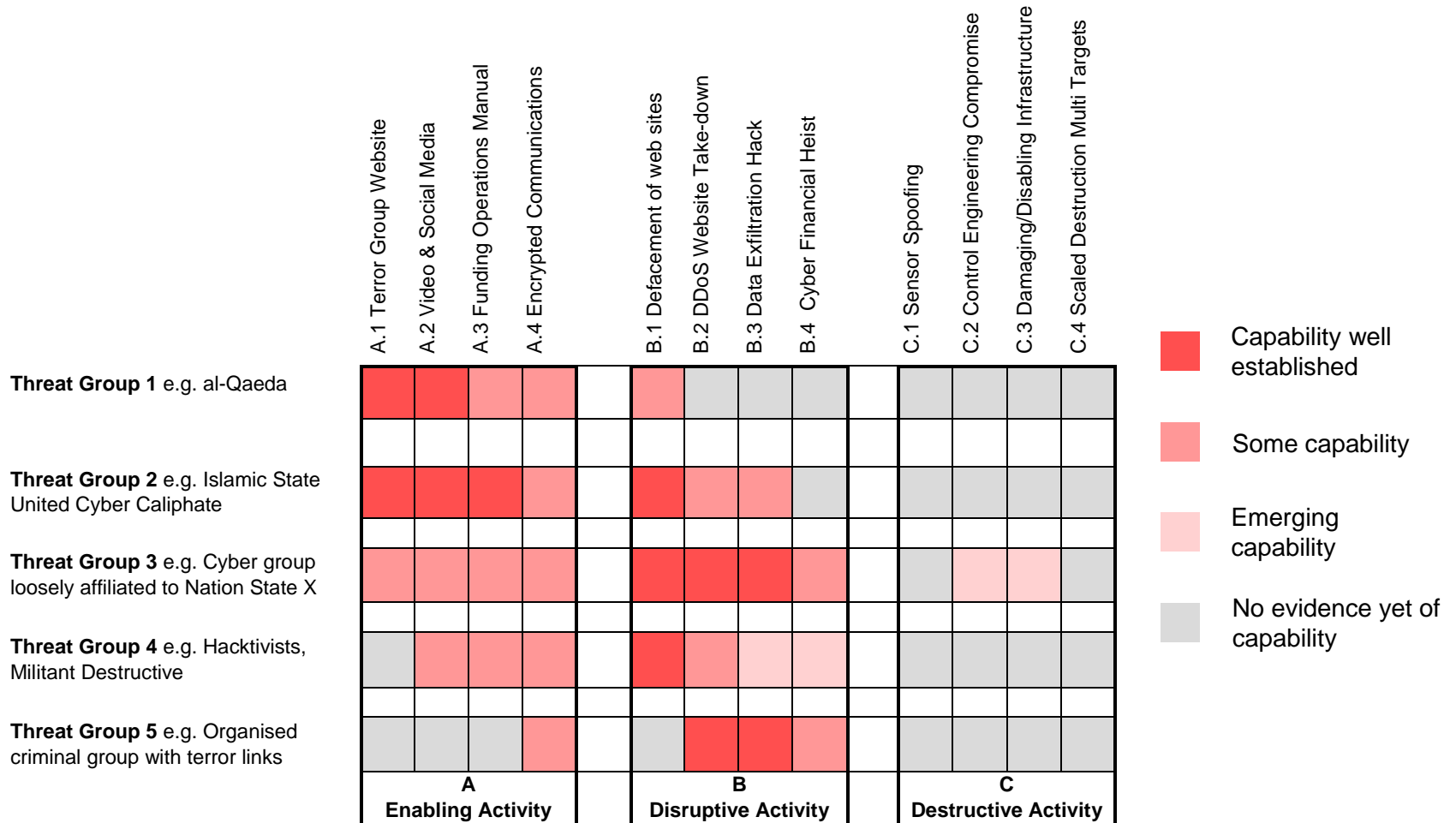
# November 28 Report and Schema Launch



# The cyber terrorism threat in 2018

- To date, there have been no known instances of cyber terrorism fitting this definition
- There is little evidence to suggest that current terrorist groups have invested significant time or capital into the development of sophisticated physical cyber attacks
- Several groups have proclaimed their intentions to attack the West digitally
  - Statements of intent do not necessarily suggest capability
- Given the generational lifetime of dominant terrorist threats, we would expect that any imminent development of destructive cyber capabilities would be carried out by currently active group
  - The most relevant groups pose a low-likelihood of inflicting severe physical damage through digital means

# Tracking capability across cyber actor groups





# Threat assessment and structure analytical techniques

Literature Search  
Mendeley Suggest

My Library  
All Documents  
Recently Added  
Recently Read  
Favorites  
My Publications  
Unsorted  
Pool Re Q1+Q2 2018 Sources  
Create Folder...

Groups  
Create Group...

Trash  
All Deleted Documents

Authors	Title
BBC	Tumblr deletes 'Russian troll' accounts
Stephen Tankel, R. Kim Cragin, Daveed Gartenstein...	Policy Roundtable: What Is the Future of the Jihadist Movement?
FBI	Iranian Mabna Hackers: Conspiracy To Commit Compu Intrusions; Conspiracy To Commit Wire Fraud; Compu
Healey, Jason	The Attacker Has the Advantage in Cyberspace. Can Fix That?
DeYoung, Ellen Nakashima and Karen	Trump administration hits Iranian hacker network with sanctions, indictments in vast global campaign
Institute, Mabna	Mabna Institute
BBC	Iran angered at US imposition of cyber sanctions
Schmitt, Dedan Walsh and Eric	U.S. Strikes Qaeda Target in Southern Libya, Expanding Shadow War There
FireEye	Looking Ahead: Cyber Security in 2018
Rowlatt, Justin	Russia 'arming the Afghan Taliban' says US
BBC	France hostage taking: 'One dead' in Trebes supernat
Mansour, Renvad, Al-Hasham	ISIS Inc.
Welle, Deutsche	Deadly 'Islamic State' hostage situation in France
Carr, Stuart Dacis and Nick	APT33: New Insights into Iranian Cyber Espionage Gr
Team, Security Response Attack Investigation	Chafar: Latest Attacks Reveal Heightened Ambitions
Sheany	Police Arrest Core Members of 'Muslim Cyber Army'
Vigl, Michael	Domestic Terrorism: The Threat in Our Backyard
O'Neill, Chris Bing and Patrick Howell	Kaspersky's 'Slingshot' report burned an ISIS-focused intelligence operation
Lapowsky, Issie	Voice Chat App Zello Turned A Blind Eye To Jihadis For Years
Symantec	Internet Security Threat Report ISTR
Movantia, Ambaranie Nadia Kemala	Poli Bongkar group The Family MCA, Syndicate Sprea Provocative Issues
Baranski, Chris	Surgeon David Nott: Hack led to Syria air strike
FireEye	Suspected Chinese Cyber Espionage Group (TEMP-Perscope) Targeting U.S. Engineering and Mar
Lancaster, Jennifer Blouiz and Hannah Benninger and Ala	Exploiting the Prophet's Authority: How Islamic State Propaganda Uses Hadith Quotation to Assert Legitima

Details Notes Contents

Type: Report

**Worldwide Threat Assessment of the US Intelligence Community**

Authors: ODNI

View research catalog entry for this paper

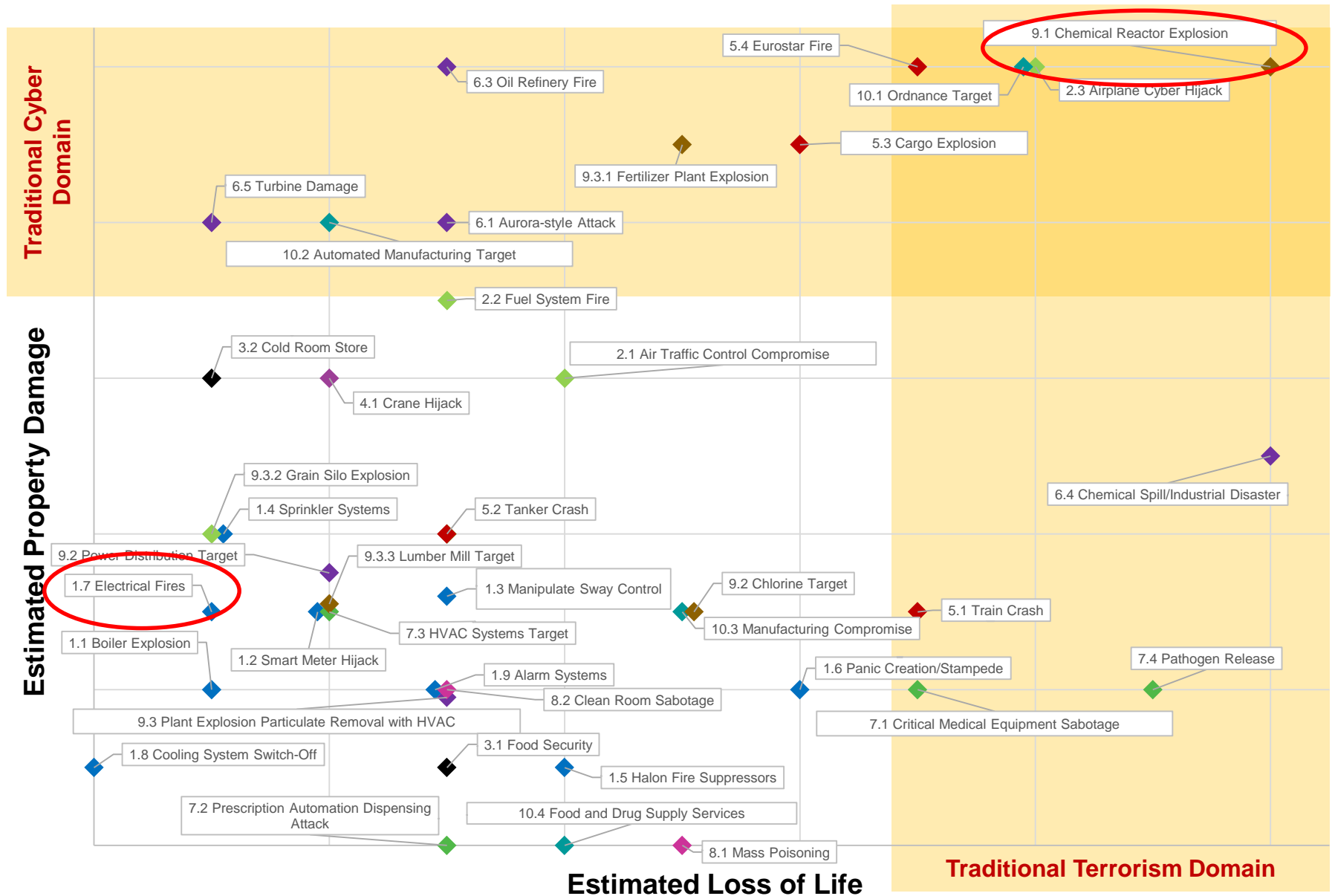
Year: 2018

Pages:

Abstract:

Date	Type	Details	Attribution	Actor	Class
06/07/2017	Malware	Multiple Western ICS Breaches	Dragonfly 2.0	Nation State APT	Destructive
07/07/2017	Malware	Western ICS in Energy Sector	Most Likely Russian APT	Nation State APT	Destructive
15/07/2017	Malware	British ICS in Energy Sector	Most Likely Russian APT	Nation State APT	Destructive
16-Jul-17	Malware	South Carolina Election Breaches	Most Likely Russian APT	Nation State APT	Disruptive
17/07/2017	Malware	UK Energy Sector GCHQ-ICS	Most Likely Russian APT	Nation State APT	Destructive
27/07/2017	Malware/	DarkWeb Marketplace Claiming T	Cyber Criminal	Cyber Criminals	Destructive
27/07/2017	Malware	Macron Campain Breach	Most Likely Russian APT	Nation State APT	Disruptive
28/07/2017	Exploits	WikiLeaks Vault 7 Dump	Hacktivists or APT	Hacktivist	Disruptive
01/08/2017	Destructive	IsraBye Diskwiper That Functions	Cyber Terrorists/Hacktivis	Cyber Terrorists	Destructive
07/08/2017	Defaceme	Defacements Advocating The Ove	The Binary Guards	Cyber Terrorists	Disruptive
12/08/2017	DDoS	Coordinated Attack on City of Cha	Anon	Hacktivists	Disruptive
15/08/2017	Brut Force	Brute Force Attack on Scottish Par	Likely Nation State APT	Nation State APT	Disruptive
18/08/2017	Data Exfil	Hacktivists Release Info on GOP S	Anon	Hacktivists	Disruptive
18/08/2017	Data Exfil	1.2 Million NHS Records Stolen (D	Anon	Hacktivists	Disruptive
02/09/2017	Manipulat	Australian 1st Responder Comms	Pirate Broadcaster ?	Hacktivists	Disruptive
06/09/2017	Malware	Symantec Finds APTs in Western	Most Likely Russian APT	Nation State APT	Destructive
07/09/2017	Data Exfil	Equifax 143 Million Details Exfil	Cyber Criminal Organisati	Cyber Criminals	Disruptive
27/09/2017	DDoS	Danish Ministries Dealing With Ir	Cyber Terrorists/ Hacktivis	Cyber Terrorists	Disruptive
05/10/2017	Data Exfil	NSA Contractor Has NSA Exploits	Most Likely Russian APT	Nation State APT	Destructive
10/10/2017	Malware	North Korea Penetrates US ICS/Pc	North Korean APT	Nation State APT	Destructive
10/10/2017	Data Exfil	North Korean APT Steals OP Plan	North Korean APT	Nation State APT	Disruptive
11/10/2017	DDoS	Targeted DDoS Attack Against Swi	Most Likely Russian APT	Nation State APT	Destructive
12/10/2017	DDoS	Targeted DDoS Attack Against 3rd	Most Likely Russian APT	Nation State APT	Destructive
20/10/2017	Malware	APT Conducting R&D In Energy An	Likely Nation State APT	Nation State APT	Destructive
24/10/2017	Malware	Bad Rabbit Ransomware, Based O	Most Likely Russian APT	Nation State APT	Destructive
30/10/2017	Malware	Cybercriminal Group Targeting Int	Cyber Criminals	Cyber Criminals	Disruptive
31/10/2017	Ddos? Def	Hacktivists Bring Down Several Sp	Anonymous	Hacktivists	Disruptive
06/11/2017	Defaceme	Team System Dz Multiple Defacer	Team System Dz	Cyber Terrorists	Disruptive
14/12/2017	Malware	TRITON Malware Attacks ICS and S	Likely Nation State APT	Nation State APT	Destructive
	Hacktivists	Destructive	Cyber Criminals		
	Nation State APT	Disruptive	Cyber Terrorists		

# Scenario planning 2016-present





# Scenario: Cyber-Induced Explosion in a Major Chemical Processing Facility



**‘Fuel bomb’ leak at major chemical facility**  
(Chemical reactor explosion)



	Mortality Rate	Physical Damage	Media Impact	Plausibility	Scalability	Direct BI Potential	Overall Economic Impact
<b>9.1 Chemical Reactor Explosion</b>	10	10	10	9	2	3	1

	Standard Scenario (S1)	Scenario Variant (S2)	Extreme Variant (X1)
Variant Profile Description	A significant fire causes physical damage at the facility	A major explosion at the facility with blast radius with 2km debris scatter	Chemical explosion with blast radius impacts key facility operations with 2km debris scatter
Loss of Affected Site (Property)	50%	50%	Write-off (100%)
Loss of Affected Site (Contents)	50%	50%	50%
Surrounding Area of Business Affected	Facility only	2km radius	2km radius
Total Loss Value	<b>£ 507m</b>	<b>£ 625m</b>	<b>£ 1,132m</b>

# Scenario: Cyber-Induced Fires in Commercial Office Buildings



## Cyber-Induced Fires in Commercial Office Buildings (Lithium battery fire induction)

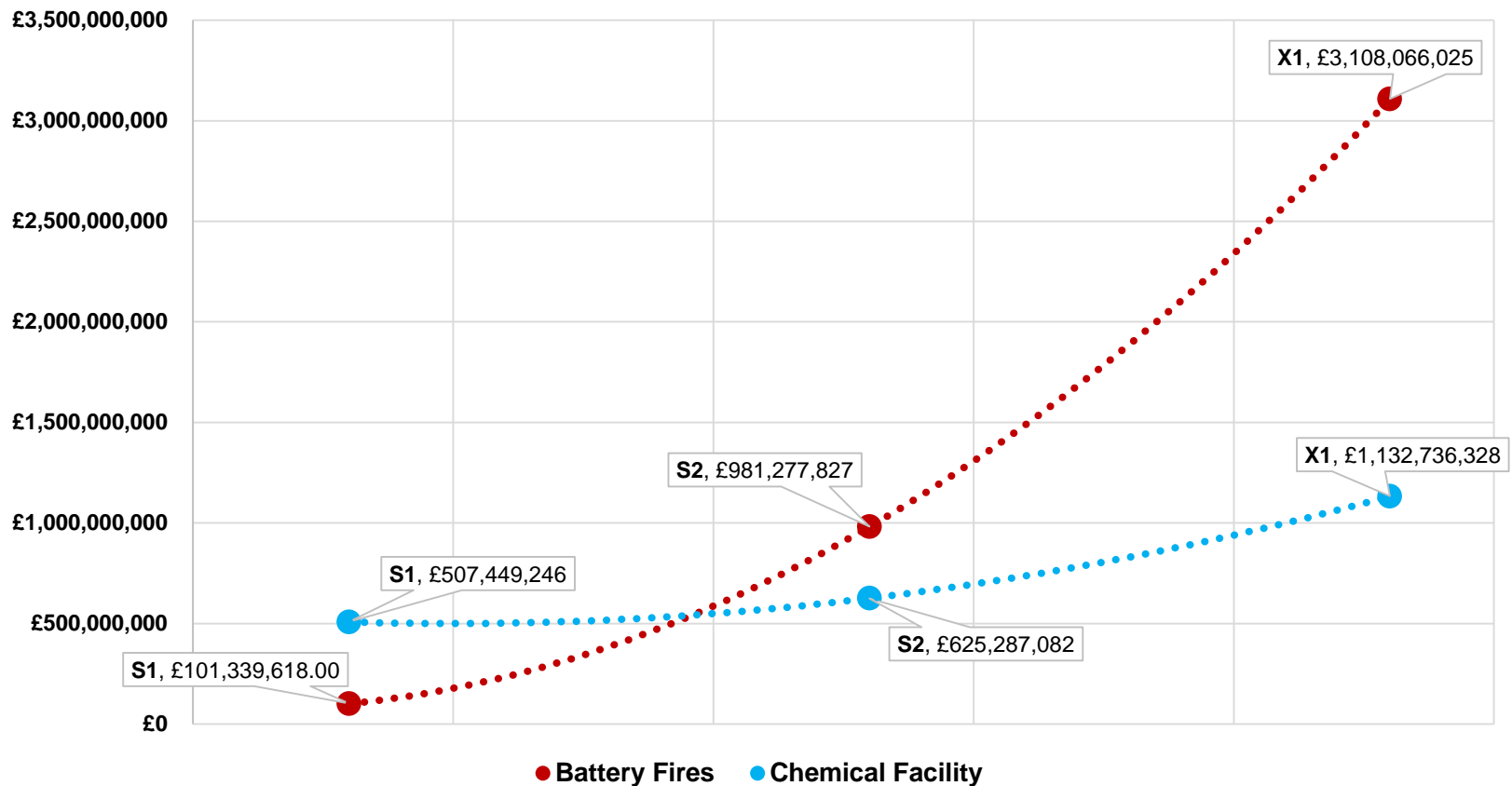


	Mortality Rate	Physical Damage	Media Impact	Plausibility	Scalability	Direct BI Potential	Overall Economic Impact
1.7 Electrical Fires	1	6	6	3	8	3	2

	Standard Scenario (S1)	Scenario Variant (S2)	Extreme Variant (X1)
Variant Profile Description	In cases of a single laptop's destruction (LFD), 20% of affected businesses claim BI for one day. Other Fire damage variations affect 50% of Businesses.	In cases of a single laptop's destruction (LFD), 50% of affected businesses claim BI for one day. Other fire damage variations affect 75% of Businesses.	In cases of a single laptop's destruction (LFD), 75% of affected businesses claim BI for one day. Other fire damage variations affect 100% of Businesses.
Business Interruption LF3 – LF5	50%	75%	100%
Rate of workplace device ignition	0.11%	1.04%	3.12%
Total Loss Value	£93m	£879m	£2,638m

# 2017 scenario comparison

Comparison of loss estimates highlights the significant threat of exponential losses resulting from a systemic cyber terrorism attack



# The next challenge

- Future acts of cyber terrorism are likely to fall into one of two categories
  - Explosive, damaging single attacks on major physical assets
  - High-frequency attacks on a large attack surface
- Cyber terrorism will be most impactful when focused on scalability and severity
  - Rather than large singular events that have limited systemic ramifications
- Determining **likelihood** for extreme loss and high impact scenarios
  - Collaboration with the intelligence community
  - Advise on setting risk appetite for insurers



# Cyber terrorism: strategic surprise

- Cyber terrorism is an emerging threat: a low-likelihood classification based on motivations and capabilities will not remain the norm
- Acts of cyber terrorism are possible, though the means to carry out attacks is currently unsupported
  - Shift from religiously motivated to politically subversive terrorism
  - Think in terms of strategic surprise
  - Generational divide in cyber knowledge will subside
  - Education in computer science will increase skills and capabilities while raising exposure to insider threats

Centre for  
**Risk Studies**

---



UNIVERSITY OF  
CAMBRIDGE  
Judge Business School