Cambridge Judge Business School

Cambridge Centre for Risk Studies 2017 Risk Summit

ASSESSING THE FUTURE THREAT OF CYBER TERRORISM

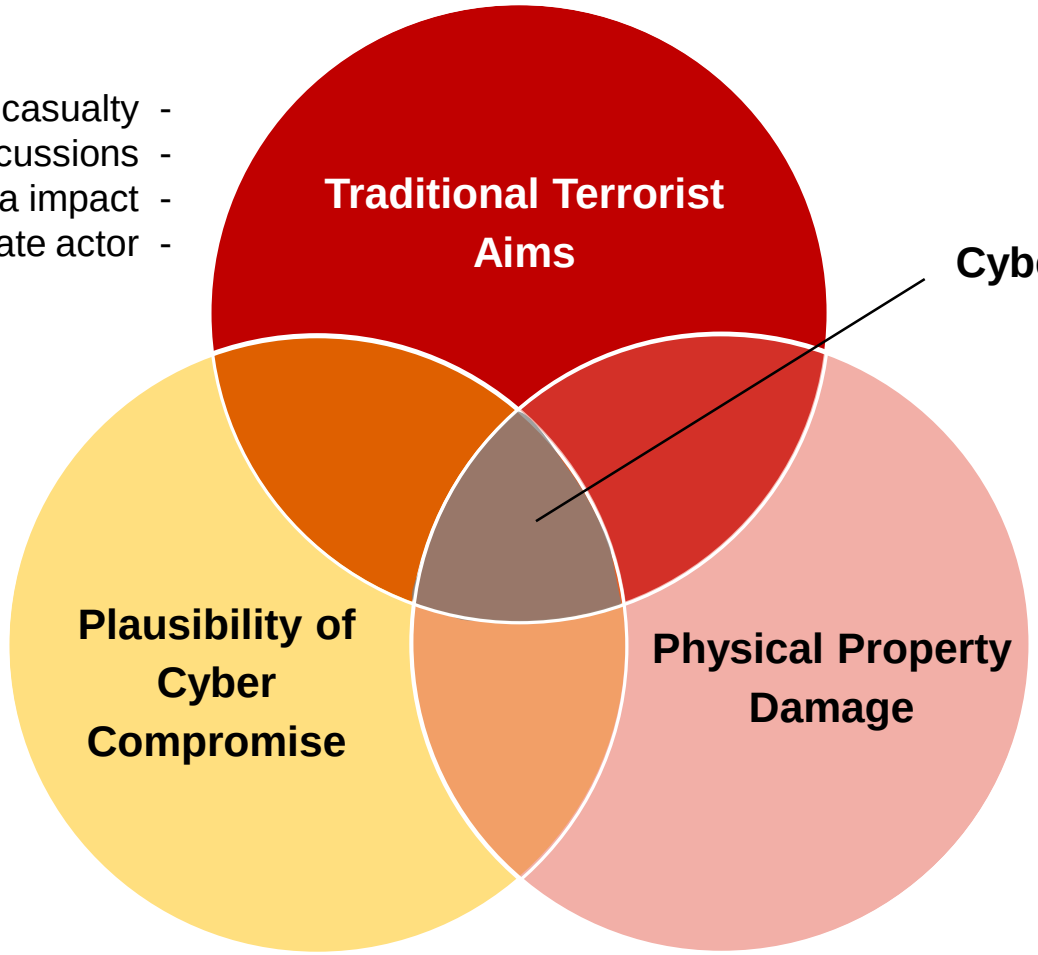
Tamara Evan, Research Assistant
Centre for Risk Studies

Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

Defining Cyber Terrorism

Mass casualty -
Political repercussions -
High media impact -
Non-state actor -



- Fire and explosion
- Significant business interruption
- Detrimental impact on critical services

The Cyber Terrorism Threat in 2017

- To date, there have been no known instances of cyber terrorism fitting this definition
- Terrorism in the West during 2017 has been largely characterised by lone-wolf attackers linked via securitised cyber communications to a radicalised network

- The indication that counterterrorism and coalition military efforts have placed IS under increased organisational pressure suggest little movement in terms of IS' development of destructive cyber capabilities
- While the group has reinforced its online communications strategies and increased utilisation of disruptive cyber capabilities, its future mandates look to prioritise frequent attacks in the West as a means of spreading fear, rather than diverting capital and energy towards establishing a strong cyber arm

The Cyber Terrorism Threat in 2017

IS is pursuing a new communications strategy

- Increased securitisation of terrorist messaging
- Highly dependent upon end-to-end encryption chat apps and private blogging platforms to pursue a personalised messages, depicting the caliphate as relatable and stable

New message is to decentralise IS resources

- There is an aim to usher recruits into developing *wilayahs* (administrative centres) elsewhere in the Muslim world as IS fighters lose territory in the Levant
- IS is also encouraging radicalised contacts *not* to travel and instead perpetrate attacks towards their homelands with little direct planning
- These messages are being distributed via enabled cyber means

The Cyber Terrorism Threat in 2017

United Cyber Caliphate has released their first official statement

- In October 2016, they announced plans to attack the West both “in technology and militarily”.
- The group has made attempts to merge pro-IS hacking cells and embark on an online defacement campaign which also involves an aspect of data exfiltration and financial theft

The Cyber Terrorism Threat in 2017

However, incidents of cyber crime remain newsworthy and frequent

Disruptive attacks

- **Dyn**: 21 October 2016, a internet traffic management product experienced two two-hour outages due to a massive DDoS attacks
- **Shadowbrokers**: 13 August 2016, anonymous auctioneering of packaged cyber weaponry sourced from the US National Security Agency
- **Bangladesh Bank Heist**: February 2016, weaknesses in the SWIFT network were exploited to achieve the largest cyber bank heist in history, with $951 million stolen
- **Tesco Bank**: 6 November 2016, 40,000 bank accounts were attacked in the largest cyber bank robberies in UK history
- **WannaCrypt0r**: 12 May 2017, 250,000 computers in 150 countries were locked by a virulent strain of ransomware, derived from exploits contained in the Shadowbrokers release

Destructive attacks

- **Fidelix BMS**: 3 November 2016, a DDoS attack on an unprotected building management system in Finland caused a loss of heat distribution, ventilation and hot water in two apartment buildings for 24 hours
- **Ukrainian substation attack**: 17 December 2016, suspicious hardware was found to have caused a 75 minute power outage in sub-zero temperatures affected Kiev and the surrounding area

Assessing the Future Threat

Monitoring group capability and identifying industry-specific cyber vulnerabilities

1. Monitoring of two key areas of capability development

- Capabilities of attributed terrorist threat groups
  - Tracking against the capability development matrix
- Evidence of destructive terrorism intent by unattributed threat actors
  - Successful or unsuccessful attempts to cause physical damage or human injury by remote digital attacks
  - From any threat actor, whatever attribution or unattributed

2. Creation with expert review of a longlist of low-probability scenarios

- Severities of outcome (damage impact, lives lost, spectacle grade)
- Difficulty of execution (logistical burden, plausibility)
- Ability to scale attack across multiple insureds
- Direct BI potential and overall economic impact

Hierarchy of Cyber Capability

A. Enabling

- online activities that support the operations of terrorist groups
- e.g.:
  - publicity and propaganda, fund-raising, recruitment, reconnaissance, clandestine communications between members, and disseminating manuals and know-how to incite and facilitate attacks by others.

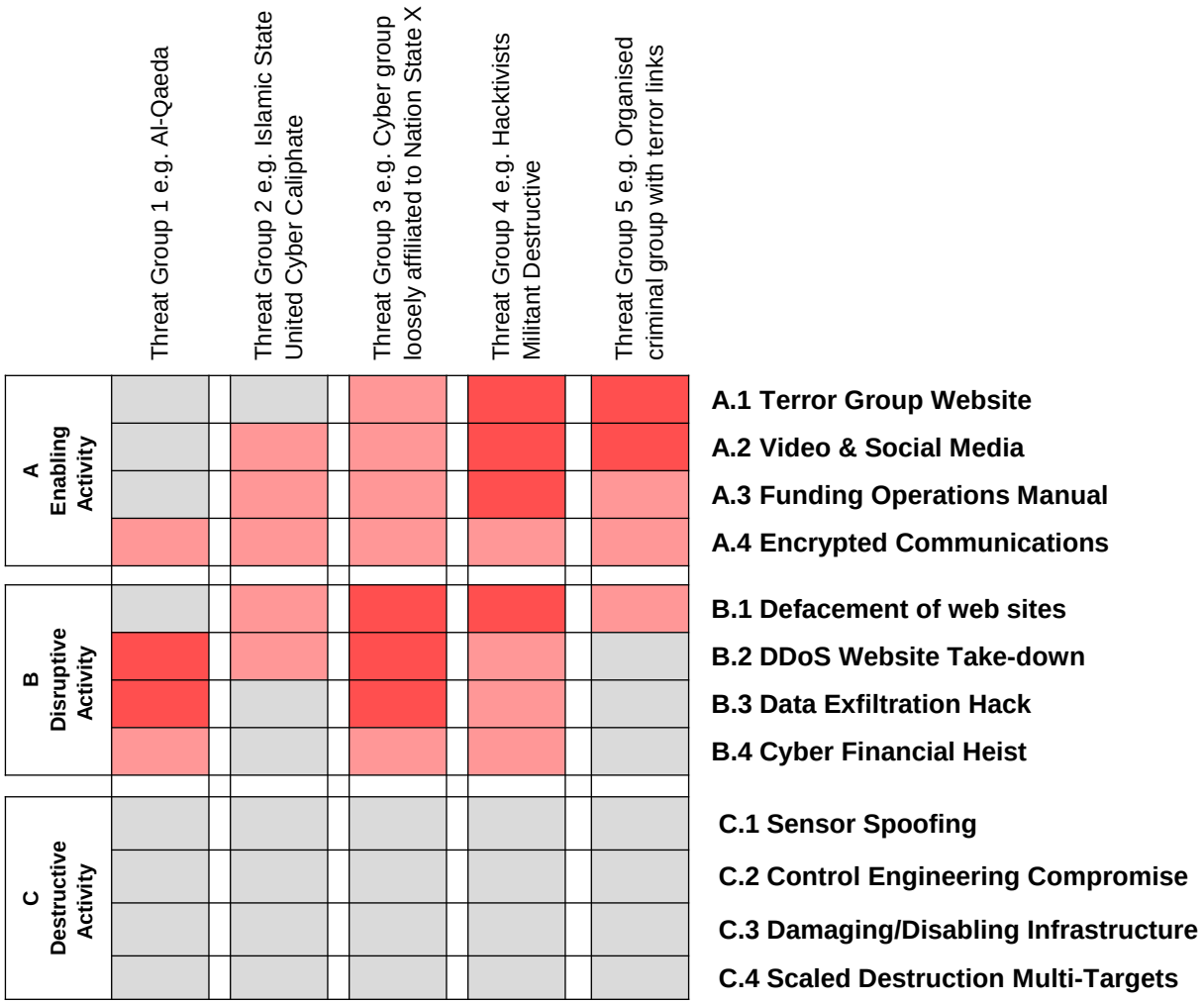
B. Disruptive

- online activities that disrupt the information technology of opponents
- e.g.:
  - hacking: cyber breaches of networks; dissemination of malware; exfiltration of digital information; financial theft and fraud; denial of service attacks; phishing and other IT hacking activities.

C. Destructive

- cyber attacks that trigger physical damage or injury through spoofing operation technology (OT) and digital control systems
- e.g.:
  - attacks on Supervisory Control and Data Acquisition (SCADA) systems; disabling control and safety systems;

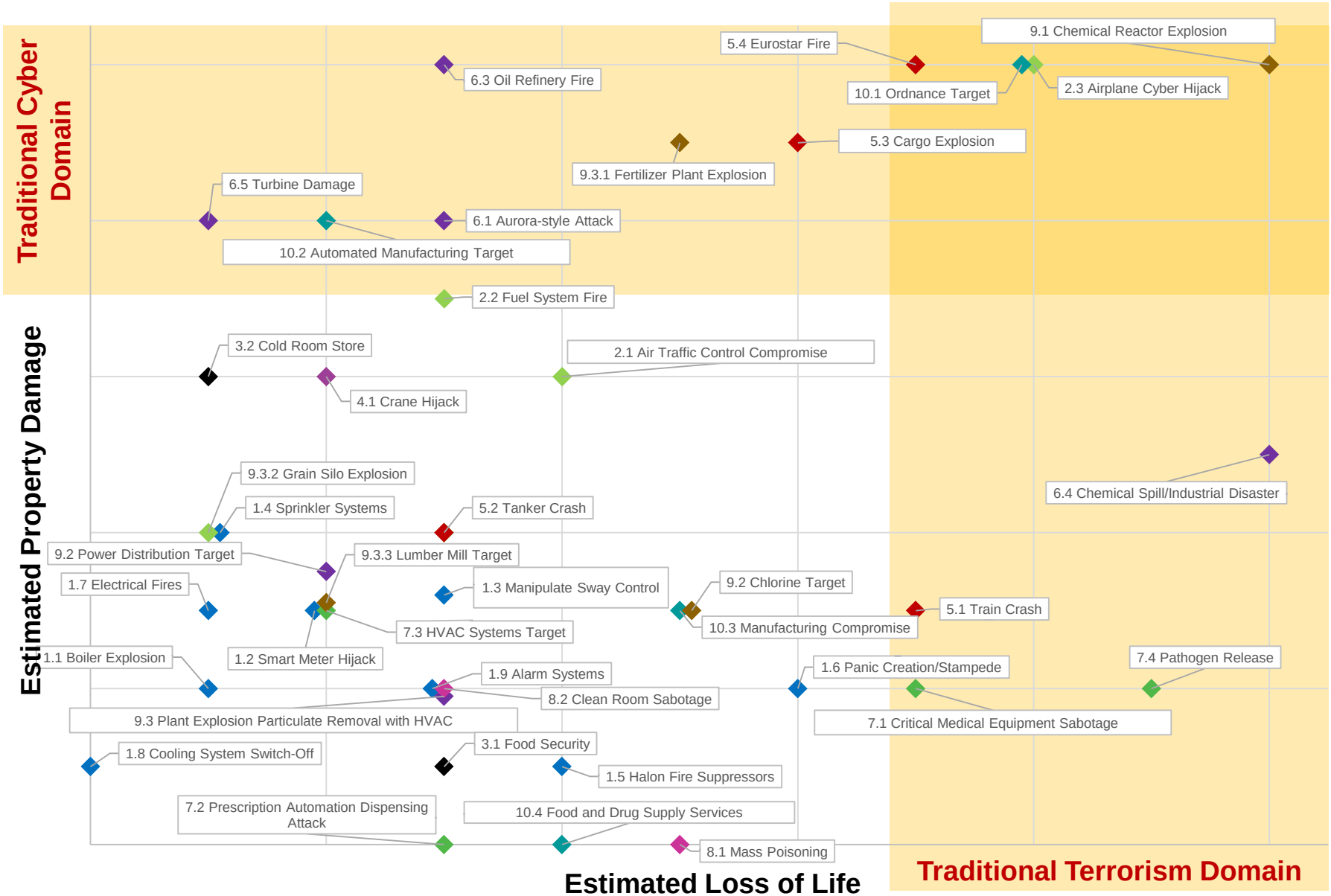
Standardized Capability Development Template



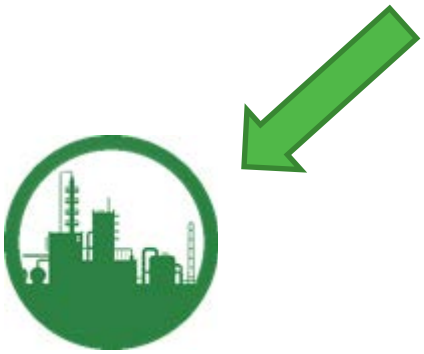
Candidate ‘Long-List’ of Cyber Terrorism Scenarios

- **Real Estate**
  - Boiler explosion, Smart Meter hijack, manipulation of building sway control, targeting of: sprinkler systems or Halon Fire suppressors, door locking, electrical fires caused by system overloads, shutting off cooling systems on server farms or data centre battery power UDS, spoofing backup generators, sabotage or manipulation of vital alarm systems.
- **Airports**
  - Air traffic spoof to create an airport crash, fuel store fire, airplane crash over City of London.
- **Construction projects**
  - Crane hijack
- **Transport**
  - Train crash, tanker crash, chemical cargo explosion, Eurostar fire.
- **Power/Energy**
  - Aurora style attack, causing oil refinery fires, chemical spill, Erebos-style UK outage.
- **Healthcare**
  - Critical medical equipment sabotage, prescription automation attack, targeting HVAC systems, uninterrupted power systems attack, pathogen release.
- **Aerospace**
  - Ordnance target, automated manufacturing target, manufacturing spoof/deadly sabotage of equipment, targeting food and drug supply services
- **Chemicals**
  - Cause a chemical reactor explosion, chlorine explosion or poisoning, fertilizer plant explosion, grain silo explosion, targeting lumber mill or particulate removal with HVAC
- **Pharmaceutical**
  - Mass poisoning
- **Retail**
  - Panic/stampede creation with spoof announcement or alarm, targeting food security

Long-List Qualitative Mapping

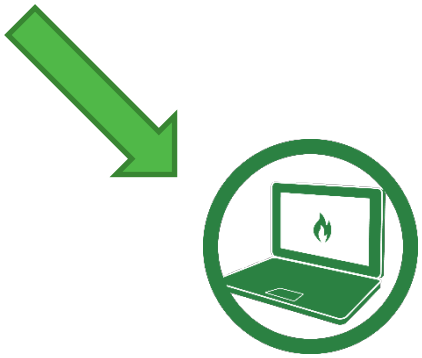


Forward Project Plan: Two Scenarios with Variants



Major bespoke cyber attack: Chemical explosion/fire at major facility

Proposed: A chemical fire is caused by a cyber attack at a major facility, causing wide-scale damage, evacuations and extended BI in surrounding areas



Systemic high-frequency cyber attack: Commercial property fires

Proposed: Lithium battery firmware hack causes a number of fires to break out overnight in office buildings, causing significant property damage

The Five Year View

Development path to ‘Destructive’ cyber capability entails advancing from ‘Disruptive’ capability

- Needs advanced computer science and hacking skills
- AND people with experienced control engineering skills

Process of capacity development requires several stages

- Planning; recruitment; education; team integration; practice & testing

Counter-terrorism operations are actively degrading their capabilities

- Slowing up capability building through pre-emptive disruption of leadership and attacks on cyber resources

We believe that there is a relatively low likelihood that the key terrorist threat groups will develop a ‘Destructive’ cyber capacity within the next five years

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School