CYBER TERRORISM THREAT INTELLIGENCE AND LOSS MODELLING

Tamara Evan, Research Assistant
Centre for Risk Studies
Defining cyber terrorism

Traditional Terrorist Aims
- Mass casualty
- Political repercussions
- High media impact
- Non-state actor

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

Plausibility of Cyber Compromise

Physical Property Damage
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

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

<table>
<thead>
<tr>
<th>Threat Group</th>
<th>Enabling Activity</th>
<th>Disruptive Activity</th>
<th>Destructive Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat Group 1</strong> e.g. al-Qaeda</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Threat Group 2</strong> e.g. Islamic State United Cyber Caliphate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Threat Group 3</strong> e.g. Cyber group loosely affiliated to Nation State X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Threat Group 4</strong> e.g. Hacktivists, Militant Destructive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Threat Group 5</strong> e.g. Organised criminal group with terror links</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**A.1 Terror Group Website**

**A.2 Video & Social Media**

**A.3 Funding Operations Manual**

**A.4 Encrypted Communications**

**B.1 Defacement of web sites**

**B.2 DDoS Website Take-down**

**B.3 Data Exfiltration Hack**

**B.4 Cyber Financial Heist**

**C.1 Sensor Spoofing**

**C.2 Control Engineering Compromise**

**C.3 Damaging/Disabling Infrastructure**

**C.4 Scaled Destruction Multi Targets**

- **A** Enabling Activity
- **B** Disruptive Activity
- **C** Destructive Activity

- **A.1** Terror Group Website
- **A.2** Video & Social Media
- **A.3** Funding Operations Manual
- **A.4** Encrypted Communications
- **B.1** Defacement of web sites
- **B.2** DDoS Website Take-down
- **B.3** Data Exfiltration Hack
- **B.4** Cyber Financial Heist
- **C.1** Sensor Spoofing
- **C.2** Control Engineering Compromise
- **C.3** Damaging/Disabling Infrastructure
- **C.4** Scaled Destruction Multi Targets

- **Capability well established**
- **Some capability**
- **Emerging capability**
- **No evidence yet of capability**
### Threat assessment and structure analytical techniques

<table>
<thead>
<tr>
<th>Date</th>
<th>Type</th>
<th>Details</th>
<th>Attribution</th>
<th>Actor</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/07/2017</td>
<td>Malware</td>
<td>Multiple Western ICS Breaches</td>
<td>Dragonfly 2.0</td>
<td>Nation State APT</td>
<td>Destructive</td>
</tr>
<tr>
<td>07/07/2017</td>
<td>Malware</td>
<td>Western ICS in Energy Sector</td>
<td>Most Likely Russian APT</td>
<td>Nation State APT</td>
<td>Destructive</td>
</tr>
<tr>
<td>13/07/2017</td>
<td>Malware</td>
<td>British ICS in Energy Sector</td>
<td>Most Likely Russian APT</td>
<td>Nation State APT</td>
<td>Destructive</td>
</tr>
<tr>
<td>16-Jul-17</td>
<td>Malware</td>
<td>South Carolina Election Breaches</td>
<td>Most Likely Russian APT</td>
<td>Nation State APT</td>
<td>Disruptive</td>
</tr>
<tr>
<td>17/07/2017</td>
<td>Malware</td>
<td>UK Energy Sector GCHQ-ICS</td>
<td>Most Likely Russian APT</td>
<td>Nation State APT</td>
<td>Disruptive</td>
</tr>
<tr>
<td>27/07/2017</td>
<td>Malware</td>
<td>DarkWeb Marketplace</td>
<td>Cyber Criminal</td>
<td>Cyber Criminals</td>
<td>Destructive</td>
</tr>
<tr>
<td>27/07/2017</td>
<td>Malware</td>
<td>Macron Campaign Breach</td>
<td>Most Likely Russian APT</td>
<td>Nation State APT</td>
<td>Destructive</td>
</tr>
<tr>
<td>20/08/2017</td>
<td>Malware</td>
<td>Exploits</td>
<td>WikiLeaks Vault 7 Dump</td>
<td>Hacktivists or APT</td>
<td>Disruptive</td>
</tr>
<tr>
<td>21/08/2017</td>
<td>Malware</td>
<td>Exploits</td>
<td>WikiLeaks Vault 7 Dump</td>
<td>Hacktivists or APT</td>
<td>Disruptive</td>
</tr>
<tr>
<td>22/08/2017</td>
<td>Malware</td>
<td>Exploits</td>
<td>WikiLeaks Vault 7 Dump</td>
<td>Hacktivists or APT</td>
<td>Disruptive</td>
</tr>
<tr>
<td>23/08/2017</td>
<td>Malware</td>
<td>Exploits</td>
<td>WikiLeaks Vault 7 Dump</td>
<td>Hacktivists or APT</td>
<td>Disruptive</td>
</tr>
<tr>
<td>24/08/2017</td>
<td>Malware</td>
<td>Exploits</td>
<td>WikiLeaks Vault 7 Dump</td>
<td>Hacktivists or APT</td>
<td>Disruptive</td>
</tr>
<tr>
<td>25/08/2017</td>
<td>Malware</td>
<td>Exploits</td>
<td>WikiLeaks Vault 7 Dump</td>
<td>Hacktivists or APT</td>
<td>Disruptive</td>
</tr>
</tbody>
</table>
Scenario: Cyber-Induced Explosion in a Major Chemical Processing Facility

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

<table>
<thead>
<tr>
<th>Variant Profile Description</th>
<th>Standard Scenario (S1)</th>
<th>Scenario Variant (S2)</th>
<th>Extreme Variant (X1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Affected Site (Property)</td>
<td>50%</td>
<td>50%</td>
<td>Write-off (100%)</td>
</tr>
<tr>
<td>Loss of Affected Site (Contents)</td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>Surrounding Area of Business Affected</td>
<td>Facility only</td>
<td>2km radius</td>
<td>2km radius</td>
</tr>
<tr>
<td>Total Loss Value</td>
<td>£ 507m</td>
<td>£ 625m</td>
<td>£ 1,132m</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9.1 Chemical Reactor Explosion</th>
<th>Mortality Rate</th>
<th>Physical Damage</th>
<th>Media Impact</th>
<th>Plausibility</th>
<th>Scalability</th>
<th>Direct BI Potential</th>
<th>Overall Economic Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>9</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>
Scenario: Cyber-Induced Fires in Commercial Office Buildings

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

<table>
<thead>
<tr>
<th>1.7 Electrical Fires</th>
<th>Mortality Rate</th>
<th>Physical Damage</th>
<th>Media Impact</th>
<th>Plausibility</th>
<th>Scalability</th>
<th>Direct BI Potential</th>
<th>Overall Economic Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Scenario (S1)</td>
<td>1</td>
<td>6</td>
<td>6</td>
<td>3</td>
<td>8</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Scenario Variant (S2)</td>
<td>50%</td>
<td>75%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extreme Variant (X1)</td>
<td>75%</td>
<td>100%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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**

- Standard Scenario (S1): 50%
- Scenario Variant (S2): 75%
- Extreme Variant (X1): 100%

**Rate of workplace device ignition**

- Standard Scenario (S1): 0.11%
- Scenario Variant (S2): 1.04%
- Extreme Variant (X1): 3.12%

**Total Loss Value**

- Standard Scenario (S1): £93m
- Scenario Variant (S2): £879m
- Extreme Variant (X1): £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