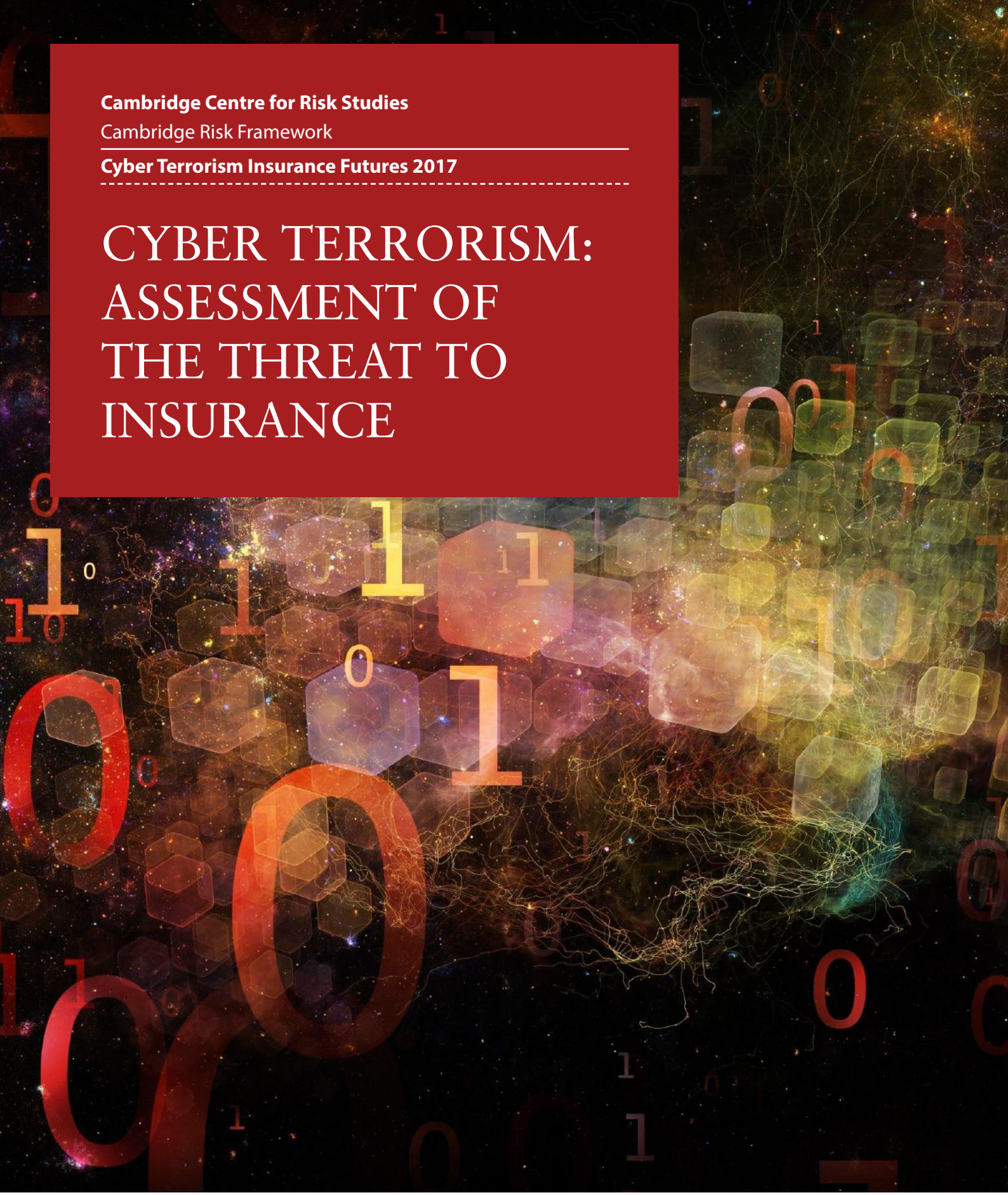
Cambridge Centre for Risk Studies

Cambridge Risk Framework

Cyber Terrorism Insurance Futures 2017

CYBER TERRORISM: ASSESSMENT OF THE THREAT TO INSURANCE



Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

POOL RE
REINSURING TERRORISM RISK

Cambridge Centre for Risk Studies
University of Cambridge Judge Business School
Trumpington Street
Cambridge, CB2 1AG
United Kingdom
enquiries.risk@jbs.cam.ac.uk
https://www.jbs.cam.ac.uk/risk

November 2017

The Cambridge Centre for Risk Studies acknowledges the generous support provided for this research by the following organisation:

Sections of this public report have been redacted for reasons of security.

The views contained in this report are entirely those of the research team of the Cambridge Centre for Risk Studies, and do not imply any endorsement of these views by the organisations supporting the research, or our consultants and collaborators.

This report is available online at **cambridgeriskframework.com/downloads**

Cambridge Centre for Risk Studies
Website and Research Platform

https://www.jbs.cam.ac.uk/risk

Report citation:

Evan, T.; Leverett, E.; Ruffle, S. J.; Coburn, A. W.; Bourdeau, J.; Gunaratna, R.; Ralph, D.; 2017. ***Cyber Terrorism: Assessment of the Threat to Insurance***; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.

Appendix 1: UK Cyber Blackout Scenario cites text and findings from the following report:

Kelly, S.; Leverett, E.; Oughton, E. J.; Copic, J.; Thacker, S.; Pant, R.; Pryor, L.; Kassara, G.; Evan, T.; Ruffle, S. J.; Tuveson, M.; Coburn, A. W.; Ralph, D. & Hall, J. W.; 2016; ***Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy***; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.

Research Project Team

Cyber Terrorism Insurance Futures Project Lead
Simon Ruffle, *Director of Research and Innovation*
Tamara Evan, *Research Assistant and Coordinating Editor*

Cyber Terrorism Insurance Futures Project Contributors
Dr Andrew Coburn, *Director of Advisory Board*
Professor Daniel Ralph, *Academic Director*
Eireann Leverett, *Senior Risk Researcher*
James Bourdeau, *Research Assistant*

Cambridge Centre for Risk Studies Research Team
Dr Michelle Tuveson, *Executive Director*
Jennifer Copic, *Research Associate*
Dr Jennifer Daffron, *Research Associate*
Dr Edward Oughton, *Research Associate*
Dr Andrew Skelton, *Research Associate*
Dr Jay Chan Do Jung, *Risk Researcher*
Dr Duncan Needham, *Senior Risk Researcher*
Jennifer Copic, *Research Assistant*
Arjun Mahalingam, *Research Assistant*
Andrew Smith, *Research Assistant*
Kayla Strong, *Research Assistant*
Jessica Tsang, *Research Assistant*

Consultants and Collaborators
Professor Rohan Gunaratna, Head of the International Centre for Political Violence and Terrorism Research and Professor of Security Studies at the S. Rajaratnam School of International Studies, *Nanyang Technological University, Singapore*
Nur Azlin Mohamed Yasin, Chief of Security Informatics at the International Centre for Political Violence and Terrorism, Research and Associate Research Fellow at the S. Rajaratnam School of International Studies, *Nanyang Technological University, Singapore*
Dr Madan M. Oberoi, Director, Cyber Innovation & Outreach, *INTERPOL Global Complex for Innovation*
Dr Gordon Woo, Catastrophist, *RMS Inc.*

Our appreciation to **Rathore Shahzeb Ali**, Research Analyst, *International Centre for Political Violence and Terrorism Research, Singapore,* for editing the article which provided the basis of the chapter **Cyber Capabilities of Terrorist Groups**.

Cyber Terrorism: Assessment of the Threat to Insurance

Report Contents

Foreword

Dear Member,

I am very pleased to write the foreword to this joint Pool Re/Cambridge Centre for Risk Studies report entitled *Cyber Terrorism: Assessment of the Threat to Insurance*. This report marks the extension of Pool Re's coverage to include cyber terrorism.

The proliferation of the Internet of Things, Big Data and Quantum Computing has created new and diverse security challenges; increased networking of facilities management and industrial control systems has exposed new attack vectors and made it possible to destroy both lives and property through remote digital interference. Recent events have demonstrated that the peril is no longer hypothetical, and industries ranging from aviation, retail and healthcare have all proved to be vulnerable. While terrorist groups have yet to successfully weaponize computer systems, the broadening of attack surfaces and the growing technical capabilities of threat actors suggest that the arrival of a physical cyber terrorist attack is only a matter of time. Just as improvements have been made through protective security measures, such as Hostile Vehicle Measures (HVM), we now need to build resilience into our information systems and technology platforms.

Pool Re must be prepared for this contingency, and is therefore extending its coverage with effect from April 2018. We have partnered with the Cambridge Centre for Risk Studies to examine how the cyber terrorism threat could develop and to generate attack scenarios which could affect vulnerable UK industry sectors.

In the next year we will build on the work we have done with the Centre as we develop a modelling toolkit that will help us quantify the loss scenarios as we develop them.

The research has already enabled us to educate and advise on the realities of cyber terrorism and better understand Pool Re's and our Members' exposure to the threat. We very much hope that this will help the market respond to the emerging risk and ultimately build greater resilience against all forms of cyber terrorism.

Julian Enoizi

Chief Executive, Pool Re

1 Introduction

Changing tactics of terrorism

Terrorism – the application of politically-motivated violence to resist or influence the policies of governing regimes – has been a spectre of organised governments for millennia.[1] Almost by definition, terrorism is 'asymmetrical': the state is always more powerful than the antagonists seeking to undermine it. In employing a technique of changing violent tactics, a less well-resourced terror group can use the element of surprise to achieve success against a less agile state security apparatus.

Terror tactics have changed over time as the genus of groups perpetrating the violence and the security measures in place to prevent them has advanced and evolved. As known targets are hardened and securitised, terrorist groups typically shift to softer, more vulnerable targets. This praxis is shown in the changing terrorist practices of the last hundred years, from political assassination in the early 20th century, to plane hijacking and hostage taking by Middle Eastern terrorist groups in 1970s, attacks on police and army units and mainland car bombs preceded by warnings by the IRA in 1990s, and a shift toward maximising civilian casualties with suicide attacks by jihadists in the past 15 years. Perhaps the most radical innovation in terror tactics in the 21st century to date has been the weaponisation of passenger aircraft by al-Qaeda in 2001.

Could cyber terrorism be the next tactical shift?

With this history of advancing tactical techniques, commentators have speculated on myriad futures for global terrorism, including terrorist acquisition of weapons of mass destruction through to all-out economic and psychological warfare, or the repeated use of insurgency tactics to undermine the political tolerance of Western populations.

The spectre of cyber terrorism looms large over such speculation. Practices and predictions of terrorists acquiring destructive cyber capabilities date back many years. The National Academy of Sciences first warned of a 'digital Pearl Harbor' as early as 1990.[2] The imminent acquisition of cyber capabilities by terrorist groups has been long expected but has so far failed to materialise and there have been no known terrorist attacks using cyber means to trigger physical damage and destruction. However, concerns over the potential movement of terrorism into the cyber sphere endure, and, with the broadening of attack surfaces and growing technical capabilities of threat actors, the arrival of cyber terrorism seems ever more likely.

This report examines the possibility of this emergent threat and the potential risks it poses for the UK property insurance market over the next three years, using an analysis of the state of global terrorism and technological vulnerability at the close of 2017.

Cyber and insurance

The possibility of cyber crime developing the potential to cause physical damage is a major concern for the insurance industry. Property insurance and many other types of policies in use today were developed to protect insureds against traditional perils and causes of loss that are understood, priced, and underwritten on the basis of historical claims experience. If new losses were to occur resulting from cyber attacks – whether perpetrated by terrorists or other individuals – then this would add the new dimension of a nascent risk, which is difficult to measure and quantify, to pre-existing coverage. Some policy terms and conditions now explicitly exclude cyber as a cause of loss, particularly as a cause of legal liabilities and compensation for loss of privacy or data, in order to side-step this complication. There is a growing industry of 'affirmative' cyber insurance which provides corporate coverage for breaches of IT security but, at this time, there are only a handful of insurance products that offer protection for physical damage or human injury resulting from cyber attacks.[3]

The potential scope of physical damage that may result from a cyber attack is difficult to estimate, as most cyber criminal attacks to date are motivated by theft or information compromise, which may be financially or politically beneficial for the attacker. If physical damage were to result from a cyber attack, there is uncertainty in many insurance policy standard terms and conditions about whether such a loss would be covered. This ambiguous 'silent' potential exposure is an area of significant concern for the industry in light of the high profile of cyber threats. In the London market, Lloyd's regulators now require greater clarity of cyber

[1] The history of terrorism, dating back as far as the 'Zealots' terror campaign against the Roman regime in AD 66-73, is well described in Hoffman (2006); *Inside Terrorism*; Columbia University Press.

[2] Weimann, Gabriel; 2004; 'Cyberterrorism: How Real Is the Threat?' United States Institute of Peace Special Report.

[3] In our review of 26 affirmative cyber insurance products on the market in 2015, 12% of them offered cover for cyber terrorism, 19% offered coverage for physical damage, and 15% for human injury. CCRS and RMS, Inc. (2016) Managing Cyber Insurance Accumulation Risk, Cyber Accumulation Risk Management; 2015.

coverage. Insurance markets elsewhere, notably in the United States and Europe, are in a similar process of attempting to clarify cyber coverages and exposure in their insurance policy terms.

Cyber terrorism and insurance

Difficulty in attributing cyber attacks adds a degree of complexity to expanding insurance policies to cover losses caused by them. It can take a long time for forensic investigators to determine how a cyber attack was carried out, and some never confidently establish the identity of the perpetrators. Physically destructive cyber attacks could be difficult to trace and identify as an act of terrorism. It may be evident from the nature of the act that it has been carried out as an act of terrorism, but there is potential for considerable ambiguity. These issues are important to consider in understanding the potential exposure to insurers from cyber terrorism.

Case Study: WannaCry, 12 May 2017

WannaCry has proved something of a turning point in the public awareness of disruptive and global cyber crime. The ransomware spread rapidly, affecting public and private services on every continent. Up to 300,000 computers in 150 countries are thought to have been affected. In the UK, up to 60 NHS Trusts experienced some sort of disruption. Overall, the ransomware was deemed highly virulent, but poorly designed, and ultimately netted relatively little profit (approximately $128,424 out of potential millions).

WannaCry's successes can be directly attributed to the April 2017 data dump by the group known as the ShadowBrokers. The group had previously attempted to auction what was characterised as stolen NSA cyber weapons in August 2016, and these were included in the tools made available on 14 April. WannaCry primarily utilised two powerful exploits found within this data dump: ETERNALBLUE and DOUBLEPULSAR, which affected Windows operating systems. The exploits were patched by Windows on 14 March in response to the release by ShadowBrokers, and the malware impacted vulnerable machines that either did not install the update in time, or that ran versions of Windows software that was incompatible with the patch, such as Windows XP.

As of June 2017 most major security firms and government agencies agree that the Lazarus Group, an APT affiliated with the North Korean government, was responsible for the WannaCry release.

Perceived increased threat of cyber terrorism

The recent growth in the sophistication of cyber crimes and the advent of cyber attack causing physical damage means that insurers are expressing greater concern about the future appearance and rise of cyber terrorism. Several are using accumulation scenarios of hypothetical destructive cyber attacks, including those developed by Cambridge Centre for Risk Studies, as potential scenarios of cyber terrorism.[4] Active terrorist groups make periodic public announcements about their own advances in cyber capability and their increasing focus on developing these capabilities, which, if taken at face value, is a cause of concern for insurers.[5]

The 2015 decision by UK Government to announce the National Cyber Security Programme was a major initiative to protect national systems against cyber attacks and officials cited the threat of destructive cyber attacks by terrorist groups as a key justification for this. The then Chancellor George Osborne claimed at the time that the so-called Islamic State's 'murderous brutality has a strong digital element… [If] our electricity supply, or our air traffic control, or our hospitals were successfully attacked online, the impact could be measured not just in terms of economic damage but of lives lost.'[6] In November 2016, the government laid out plans for a five-year National Cyber Security Strategy, aiming to build UK cyber resilience and security through to 2021.[7]

Aims of the research

This report assesses the threat of cyber terrorism to the UK at the time of publication and examines how such a threat may develop over the next three years. The report proposes a variety of cyber terrorism attack scenarios which could affect vulnerable UK industry sectors which comprise the exposure of the Pool Re membership. It provides qualitative insight into the likelihood, possibility and potential direct and indirect impacts of each scenario type. It presents a review of evidence for the operational capabilities of active terrorist groups who might potentially pose a threat

[4] The Cambridge Centre for Risk Studies has worked with insurers who have adapted our Lloyd's Business Blackout scenario of a cyber attack on the US power grid, as a cyber terrorism risk management scenario.

[5] For example, a Twitter announcement on 4 April 2016 announced the formation of 'United Cyber Caliphate' merging three IS-related cyber teams to increase the cyber terrorism capabilities of Islamic State.

[6] The ex-Chancellor's speech to GCHQ on cyber security, 17 November 2015; Spending Review and Autumn Statement 2015. The chancellor's statement, announcing a £1.9 billion budget for cyber security came four days after terrorist attacks in Paris on 13 November.

[7] Chancellor Philip Hammond made the strategy documents available online; National Cyber Security Strategy 2016 to 2021, 1 November 2016.

of cyber terrorism to UK, and proposes a structured scale of 'cyber capability' against which to map and monitor the evidence of capability.

Above all, the report seeks to both educate and advise on the realities of cyber terrorism and the industry's exposure to the threat.

Defining cyber terrorism

For the purposes of this report, we define 'cyber terrorism' as *an act of politically-motivated violence involving physical damage or personal injury caused by a remote digital interference with technology systems*. We do not seek to suppose the political motivations for such actions as the official certification of terrorism for the purposes of Pool Re's coverage would be a matter of government intelligence and sanction.

Report structure

This report sets out to provide useful insight on the developing threat of cyber terrorism as it pertains to the interests of the broader (re)insurance industry. It presents a series of unlikely but plausible cyber terrorism scenarios which may impact insurance portfolios, organised by exposure categories, in order to create an informed view of the scope of possible risk as of Q3 2017. Per publication of the report, the details of these scenarios have been removed and are discussed at a distance.

The report then presents an analysis of modern terrorist groups and their current cyber capabilities. The historical pattern of extremism in the Middle East would suggest that the groups which currently pose the greatest threat to the security of the UK Mainland (namely, the Islamic State, also referred to as Daesh), will likely retain some power and influence in the region for the foreseeable future. For the purposes of this report, therefore, we consider that extremist groups operating presently will be the main threat actors responsible in any cyber terrorist development in the next three years.

Following this, the report focuses on the susceptibility of the UK Mainland to future cyber terrorist activity and the defences available. While active plots to compromise UK cyberspace may not come into fruition in the next three years, this does not negate the inherent vulnerabilities in national infrastructure and industry. Identifying at-risk systems, high profile targets and indicators for increased cyber vulnerability is crucial to the responsible provision of cyber terrorism cover in the future.

Various real-world case studies are presented throughout the report. Although none of these scenarios represent examples of known destructive cyber terrorism, these case studies provide further insight into susceptible facilities and the insurance losses associated with significant industrial accidents that could be ultimately engineered by cyber terrorists or actors in cyber warfare.

The report also includes a summary of the Cambridge Centre for Risk Studies' 2016 analysis of a hypothetical blackout catastrophe in the United Kingdom caused directly by a nation-state cyber assault on South Eastern substation networks in Appendix 1: UK Cyber Blackout Scenario. Appendix 2: Major ICS cyber events to 2017 presents a catalogue of notable industrial control systems (ICS) cyber events that have occurred since 1999 and provides information on their attackers, attack methods and motivation.

Conclusions

The key conclusion of this report is that, while various types of cyber attack are becoming more commonplace, the most relevant cyber terrorist actors currently pose a low likelihood of inflicting severe physical destruction through digital means before 2020. At present, the major terrorist groups posing a threat to the West are motivated by mass casualty attacks; the cyber tools available to these actors currently provide far less chance of major injury than a traditional explosive, knife or vehicle attack.

The onus of developing an informed and well-funded hacking team or otherwise acquiring a sophisticated cyber weapon capable of achieving success in physically destructive and damaging cyber attacks requires a significant investment of both time and money for terrorist groups, who are simultaneously combating international counterterrorism efforts and pursuing options for immediate political returns on traditional acts of terror in the face of significant territory loss.

This conclusion must be tempered by recognition that cyber terrorism, and cyber crime in general, remains an emerging threat. The number of vulnerabilities embedded within digital devices ubiquitous to Western society is constantly growing, and the added development of the 'Internet of Things' adds layers of additional vulnerability to many existing physical systems, from manufacturing and other industrial facilities to biological security systems. The protean nature of the digital economy provides ample attack surfaces for any agents of cyber terrorism or cyber war that may appear. While monitoring the cast of potential threat actors, this attack surface also requires constant evaluation and continuing securing on behalf of businesses and governments. The development and provision of cyber terrorism insurance policies may form a part of this security effort.

2 Defining the Scenarios

The following chapters propose a series of unlikely, though plausible, cyber terrorism scenarios which may impact a UK terrorism insurance portfolio, and establishes an informed picture of the range of vulnerability to acts of cyber terrorism in the UK economy over the next three years. Rather than speculate on hypothetical attack perpetrators, timings or motivations, this analysis focuses on highlighting UK industrial systems which may be liable to compromise and exploitation by cyber terrorists depending on their latent destructive qualities and their situation in the growing 'Internet of Things'. This provides insight into the shape that cyber terrorism may assume if and when terrorists groups develop the digital capabilities to remotely manipulate and take control of vital aspects of UK infrastructure.

The type of terrorist activity that has characterised the early 21st century has typically been oriented towards plotting high-mortality events in order to achieve the aims of extremist groups, and to demonstrate both the strength of the attackers and the fragility of the community under fire. These plots also serve to draw attention to and goad politicians into actions that may be used to enhance the reputation of the group, and are used to recruit new members to extremist causes. The emotional and political effectiveness of such campaigns has only reinforced the practice in the post-9/11 world.

Though physical property damage could be incurred in the pursuit of mass casualties and may create a lasting impact on a national psyche, it is not the primary aim of contemporary Islamist extremists. Attacks or incidents in which physical property, industrial systems, or operational machinery is targeted and badly damaged are far costlier, in economic terms, to national industries and governments, but generally fail to register the same emotional impact—i.e. 'terror'—as a significant loss-of-life event.

A workshop held at the University of Cambridge Judge Business School in February 2016 brought together terrorism and cyber experts along with the project team from the Centre of Risk Studies to establish a candidate-list of feasible scenarios for cyber terrorism presented in a truncated form in Chapter 3. These scenarios were reviewed and revised again in February 2017.

Defining the likely scenarios for this report requires examining the overlap of traditional terrorist aims (loss of life/mass casualty), with the purview of the Pool Re scheme (physical damage to property) as well as considering what cyber capabilities are likely to develop in the next three years that will pose a threat to both arenas (plausibility). Participants at the workshop used these criteria in to establish the definition of 'cyber terrorism' for the uses of this report and the intersection between these three areas provides our primary framework of focus for the proposed list of scenarios, as illustrated in Figure 1.

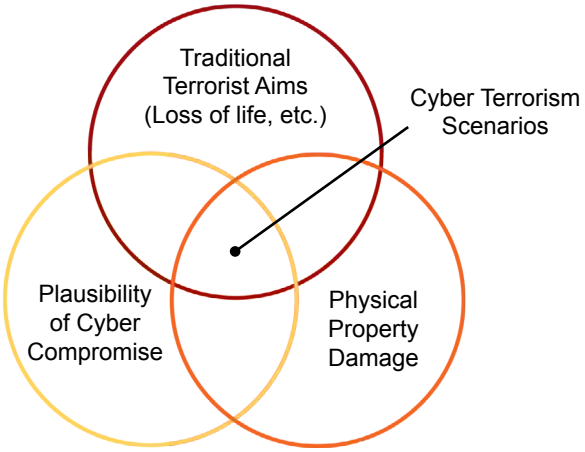


Figure 1: Strategic focus for defining realistic cyber terrorism scenarios affecting Pool Re's property portfolio

Physical exposure

These scenarios were categorised by their area of impact in one of the ten exposure categories provided by Pool Re and then qualitatively ranked on various interest criteria, listed below, in order to establish their likelihood and plausibility as attack vectors for potential cyber terrorism. They are listed with their breakdown for Material Damage expressed as a percentage of Pool Re's portfolio. The list does not include Housing or Miscellaneous coverages as listed in Pool Re's own data schemes.

1. **Real Estate & Property (70%)**
2. **Aviation (1.5%)**
3. **Retail (2%)**
4. **Construction (1%)**
5. **Transport (15%)**
6. **Power & Energy (1.5%)**
7. **Healthcare (1%)**
8. **Pharmaceutical (1%)**
9. **Chemical (1%)**
10. **Aerospace (1.5%)**

The total insured value (TIV) of these properties across the UK Mainland is shown in Figure 2. While TIV is most concentrated in the London area and along commuter lines to the UK's industrial centres, roughly 33% of Pool Re's Material Damage exposure

is located in urban areas (Zones A and B), compared with 66% in non-city areas (Zones C and D).

It is reasonable to assume that London would be the area most at risk in any future cyber terrorism plots, and that insured companies located in the City and the E14 district would be most susceptible to malicious compromise and viewed as high value targets. However, cyber risk is rarely limited or circumvented by geography. A piece of malware that is designed to infect a particular industrial system may put all systems using a certain exploitable technology at risk, and any physical damage caused may be indiscriminate in terms of location. The most sophisticated and costly acts of cyber terrorism are likely to impact multiple systems at the national level.

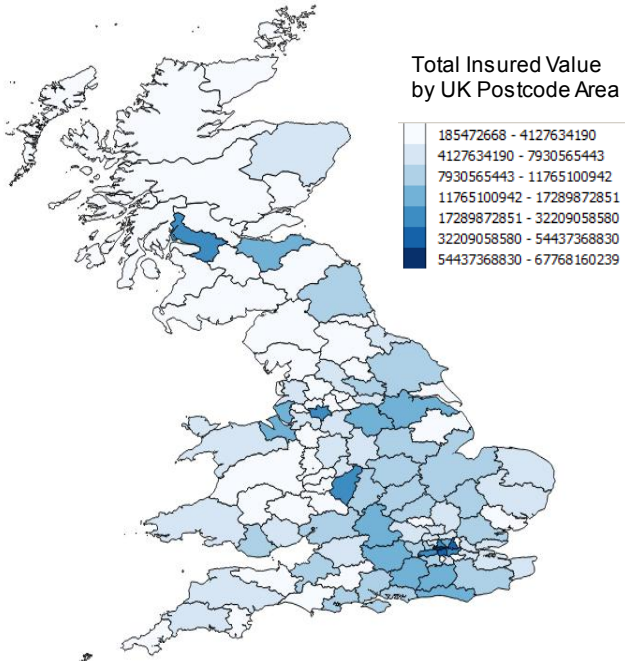


Figure 2: Geographic Total Insured Value (TIV) Distribution) in the UK Mainland

Proposed Scenarios

A long-list of forty scenarios across ten exposure categories provided by Pool Re was generated in collaboration with several industry and cyber experts. Each scenario was ultimately rated across several variables. Due to their sensitive nature, the scenario descriptions have been simplified for this publication.

1. Real Estate & Property

Between 55-60% of Pool Re's exposures lie in its real estate coverage. This portfolio incorporates many major London buildings as well as industrial parks, stadia, arenas and major shopping centres throughout the UK. The Real Estate & Property category contained the highest number of potential cyber terrorism scenarios.

Case Study: Stuxnet, 2009

The Stuxnet worm was a game changer. Although financial losses were not large, it made headlines because malicious code was seen deliberately targeting physical critical infrastructure. Stuxnet targeted industrial systems under control of the Siemens PCS7 SCADA system by exploiting four zero-day vulnerabilities. The specific target was the Natanz Nuclear Facility in Iran, where 1000 nuclear centrifuges (roughly a fifth of Iran's then-operating supply) were spun faster than their operating limits and ultimately destroyed. It also caused damage to other industrial systems under control of the Siemens system, particularly in the oil industry. In 2012, it was reported that the Stuxnet worm was developed by joint US and Israeli forces in order to sabotage Iran's nuclear programme by creating a series of events which would present as apparent industrial accidents.

The scenarios in this category involve the direct exploitation of evacuation and safety mechanisms and HVAC systems to create physically damaging effects impacting a building's structural integrity, its contents and any individuals inside it. These scenarios are typically time sensitive in their nature, and would need to be organised with sufficient intelligence to be fully destructive. The proposed cyber terrorism scenarios for Real Estate are generally also applicable to all other categories of exposure and could be carried out against facilities insured under other categories.

2. Aviation

Airports and commercial airliners have been targets for terrorism and extremists since the mid-twentieth century. Pool Re's coverage extends to many of the UK's largest airports, as well as NATS air traffic control facilities. The scheme's coverage does not extend to carrier jets or planes, nor their contents.

The scenarios in this category demonstrate how traditional aviation terrorist attacks can be achieved through digital means.

3. Retail

A number of large retailers are covered by the Pool Re scheme. The scenarios in the Real Estate & Property category may be similarly applied to these facilities and threaten members of the public.

The cyber terrorism scenarios specific to this category lead to significant business interruption due to the loss or compromise of stock.

4. Construction

Though construction sites may be inherently vulnerable to physical attacks or infiltration in dense urban areas, there is currently relatively little explosive or damaging cyber risk associated with the technology present on sites. In October 2015, the CECE-CEMA political summit petitioned the EU to enact legislation to speed and promote the transition to digitised construction work-sites in Europe, with an aim to increasing precision and fuel efficiency; ensuring the security of digitised industrial machinery on construction sites in the future is a matter of some concern. In 2017, the Committee for European Construction Equipment re-emphasised its ambitions to digitise work-sites for greater fuel and personnel efficiency.

5. Transport

The scheme covers various transport depots (stations, docks, links, major motorways and toll), though not the vessels themselves, including the undersea rail connections

Considering its international status and symbolic value, we would expect major rail routes to be a likely target for future terrorist disruption; cyber represents a feasible avenue by which to compromise this rail service. Other scenarios in this category involve deliberate cargo and signal tampering to create explosive collisions with major impacts on public health.

6. Power & Energy

The Centre for Risk Studies has published two reports which examine the wider economic impact of cyber attacks against national power grids in both the US and the UK. Lloyd's *Business Blackout* report (2015) and Lockheed Martin's *Integrated Infrastructure: Cyber Resiliency in Society* (2016) propose scenarios in which attackers are able to target power transformers and power distribution. These attack scenarios would likely be considered acts of 'cyber war', rather than cyber terrorism, as they require a level of sophistication that would be uncharacteristic of the terrorist groups currently operating against the West. However, due to Pool Re's insurance of many UK non-nuclear power stations, we consider these scenarios as part of the analysis on vulnerable systems.

Most other scenarios in this category involve the weaponisation of plant computer systems interacting either with chemical substances or plant furnaces to cause major explosions and structural damage.

7. Healthcare

Healthcare represents one area where cyber attacks may be used to incur human casualties in the near future. The development of smart medical devices and assistive technologies expose a new domain of digital vulnerability potentially physically embedded into members of the public.

Not counted in this list of scenarios is the possibility that disruptive cyber attacks such as DDoS and the use of ransomware may have real-world impacts if used against particularly critical systems. Such disruptive cyber attacks affecting healthcare facilities pose a real threat to the health and continued care of medical patients, and the sophistication of modern hacking tools in this arena means that attacks are not difficult to carry out. Similarly, DDoS attacks against poorly secured systems may cause significant physical and personal damage in particular circumstances.

Throughout 2017, instances of ransomware have locked down hospitals and other healthcare facilities, placing patient health at risk. The May 2017 WannaCry attack first appeared in NHS computer systems in the UK, prompting initial assumptions

Case Study: the Ivano-Frankivsk (Ukraine) blackout, 23 December 2015

In the lead up to 23 December 2015, three energy companies in the Ukraine failed to detect the reconnaissance stage of a cyber attack. The attackers had very likely been present in their network for six months or more, having compromised the system using a spear-phishing campaign which targeted a number of employees without detection. This allowed them to move through the three companies, installing key loggers, stealing credentials to various systems, and developing custom firmware modules for selected network equipment. The cyber attack caused a blackout that lasted eight hours, impacting three regions and 225,000 customers. Meanwhile, power companies were bombarded with bogus phone calls such that they couldn't receive legitimate customer calls reporting the outage. Firmware images were installed and the legitimate use of 27 or so infected substations was actively thwarted by the attackers.

The attack remains unattributed though may, in hindsight, come to be considered an act of cyber warfare, or perhaps an early instance of cyber terrorism, given the Ukraine's current geopolitical climate. The blackout was followed a year later by a similar malware attack against Ukrenergo, which deprived Kiev and the surrounding area of power from 17-18 December 2016 (see page 20).

Case Study: NotPetya, 27 June 2017

On 27 June 2017, a pseudo ransomware termed NotPetya quickly infected 12,500 machines in up to 64 countries in its first day loose in the wild. The supposed ransomware disproportionately affected Eastern European companies and institutions. These spanned the spectrum of critical infrastructure including: banking and financial centres; energy exploration and production; shipping; terminal operators and other support companies; power generation facilities; and, companies who overall had a broad presence and exposure in Eastern Europe. It is widely asserted that an Eastern European software company's source code was compromised and infected further systems that were undergoing update.

NotPetya's true intent as a disk wiper, designed to maliciously erase and destroy data by corrupting the Master File Table and Master Boot Record, leaving systems inoperable. When applied to critical infrastructure systems, this process can be highly disruptive and has the potential to become highly destructive. The utilisation of previous ransomware exploits such as GOLDENEYE and ETERNALBLUE of WannaCry fame, is widely thought of as an example of misdirection. The use of ETERNALBLUE as a means of spreading the malware laterally through organisations explains the speed and intensity of the attack.

A.P. Moller-Maersk, the world's largest shipping and terminal operator, has publicly estimated accumulated losses of $200 to $300 million, primarily due to business interruption. As these attacks of this type mature, the combined shocks of failing critical infrastructure and economic output put at risk through the unpredictability of international trade and business interruption will have far reaching ramifications.

that the ransomware was a direct attack against the national healthcare network; later communications revealed the ransomware was indiscriminately spreading through industrial, education and business networks worldwide. Disruptive attacks which directly impacted human health and physical integrity of critical infrastructure or in the industries listed above would be classified as Destructive in the cyber threat capability chart.

8. Pharmaceutical

Similar to retail exposure, Pool Re's pharmaceutical coverages represent an area where cyber terrorism would lead to significant business disruption, due to product recall, health and safety standards or reputational harm, rather than physical damage. With pharmaceuticals, as with healthcare, there is an increased risk of public injury or loss or life resulting from any cyber compromise.

9. Chemical

The volatile nature of chemical manufacturing and treatment makes it vulnerable to potential malicious, terrorist interference. The scenarios affecting this category are particularly concerned with cyber interference in the security measures taken in manufacturing and transporting chemical compounds, when substances would be in greater proximity to densely populated areas or public resources such as reservoirs or groundwater supplies

10. Aerospace

Scenarios in this exposure group include deliberate interference with blueprint commands, leading to costly recalls, repairs, massive public injury, and a major compromise of SCADA systems. In 2016, an international study brought to light potential security issues regarding 3D print technologies used by manufacturers, demonstrating the plausible sabotage and subsequent rapid deterioration of 3D printed machine parts. As additive manufacturing becomes more integral to a myriad of industries, including aerospace, auto, and healthcare, the risk of introducing deliberate and scalable compromises into 3D-printed parts causing serious damage, injury, or loss of stock will increase unless made more secure.

3 Scenario Impact Assessments

All scenarios assessments are considered on the basis of an 'extreme-case-scenario' based on contributing factors that would cause extreme losses and then scored in terms of the following impacts:

- **Mortality Rate:** (ranked 0 to 10) Scenarios logarithmically ranked for their worst-case-scenario death toll where 0 indicates no deaths linked to the effects of the cyber attack, 1 indicates fewer than 10 deaths and 10 indicates a thousand or more.
- **Physical Damage:** (ranked 0 to 10) In terms of economic costs of physical damage rendered by cyber terrorism activities, 0 indicates no physical damage whatsoever, and 10 indicates billions of pounds.
- **Media Impact:** (ranked 0 to 10) On the understanding that terrorist groups aim to attract attention and sway world affairs in their actions, we include a ranking for 'spectacle' or Media Impact in our analysis. Media impact rankings were informed by scores for both Mortality Rate and Physical Damage, on the basis of understanding that events which cause a high number of causalities will automatically be headline news in the UK media. Attacks that cause negligible physical damage, however, will likely inspire less or perhaps no media interest, regardless of the nature of cyber compromise – these are ranked a 1 or 0 on the scale.

  Attacks which lead to significant number of casualties and incur serious physical damage will make international headlines, and are ranked a 10. In this category, attacks which successfully target and undermine public confidence in particularly noteworthy or famous elements of critical infrastructure – such as airports or the National Grid – will also warrant a higher ranking, regardless of external physical impact.
- **Plausibility:** (ranked 0 to 10) Plausibility is defined as a combination of cyber capability (or developing cyber capability within a three-year period) and motivation. Motivation is understood as the worth of 'return', or 'utility' to attacker, compared to an organisation's financial or time investment; though an attack may be relatively easy to carry out, without the surety of significant impact in terms of death toll, public disruption or spectacular damage, it is implausible to consider it as a viable cyber terrorist threat for the current age.

  A ranking of 1 indicates a scenario in which there are both poorly established cyber capabilities, as well as little motivation to develop cyber skills in order to carry out such an attack due to its low 'return' on investment. Scenarios ranked 9 or 10 are those in which system vulnerabilities are either well-understood or available for purchase, and potential physical impacts are significant enough to warrant terrorist motivation.
- **Scalability:** (ranked 0 to 10) Scalability relates to the number of systems that can be hit at the same time. In the case of the 'Pathogen Release' scenario, a highly secure biochemical facility is likely to have a uniquely tailored security system, meaning than a successful compromise of one facility will not be easily replicated in another. However, commonly used yet vulnerable system such as a fire alarm or sprinkler system will provide a broader scale of attack.

  A ranking of 1 indicates a bespoke computer system and a low scalability factor whereas a 10 indicates a system that may be used, and compromised, in 100,000s of locations.
- **Direct BI Potential:** (ranked 0 to 3) Insurers provide cover for business interruption losses resulting directly from property damage and terrorist activity. This ranking, therefore, does not factor in disruption to supply chains or costs to downstream industries.

  A ranking of 0 indicates no interruption to business proceedings; 1 indicates up to one week of interruption; 2, a week to a month; and 3, six months to a year of direct BI losses.
- **Overall Economic Impact:** (ranked 0 to 3) Overall Economic Impact is ranked on the basis of estimated total work-weeks of productivity lost or disrupted by an attack.

  A 0 ranking indicates no work-weeks lost to 10,000 weeks lost; 1 indicates 10,000-100,000 work-weeks lost; 2 indicates 100,000-1 million weeks impacted; and 3 is indicative of 1 million or more work-weeks lost or negatively affected.

Plotting the scenarios on a variable scale of both personal and property damage helps in visualising the threat of future cyber terrorism, as shown in Figure 3. The four scenarios deemed most damaging are spread across the upper right corner and bracketed in red.

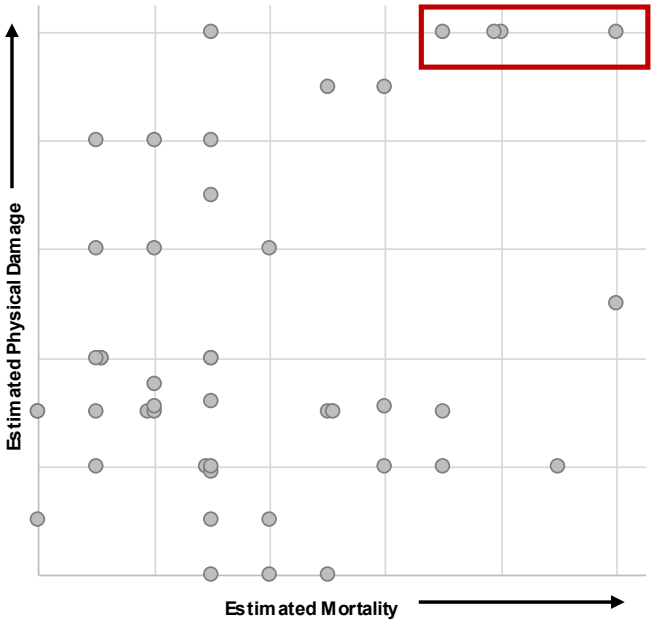


Figure 3: Distribution of long-listed scenarios across a personal injury impact grading against direct property damage grading.

The majority of scenarios rank low on both scales, clustering in the lower left-hand quadrant of the chart; while incidents of this kind may be plausible as acts of cyber terrorism they would likely not compare with the loss of life that might be achievable through conventional terrorist attacks, nor are they expected to lead to large liability insurance payouts.

The scenarios which appear on the right-hand side of the chart – incurring higher casualty rates – are those that would typically appeal to terrorist groups motivated by achieving high death counts. Scenarios towards the top of the chart, which would be the most outwardly destructive and expensive, are in the remit for the type of industrial cyber attacks that have been so far observed (see Appendices and Case Studies).

The overlap between these two traditional domains contains the four scenarios of most concern regarding future cyber terrorism threats. When the high rankings for Mortality Rate and Physical Damage are compared to their Plausibility scores (see Table 1 below), we see that the potential impact of carrying out such attacks could be considered by terrorists as a potentially worthwhile investment of time and funds.

Table 1: Isolated rankings for the top four cyber terrorism risks

	Mortality Rate	Physical Damage	Plausibility
Airplane Target	8	10	6
Rail Infrastructure Target	7	10	7
Chemical Reactor Target	10	10	9
Ordnance Target	8	10	5

As these scenarios fall into the remit of traditional terrorist activity, their plausibility is largely affected by the efficacy of pre-existing methods to achieve the same results. It is not currently easier for terrorists to hack into a plane's control systems than it is to place a man on board and have him take control by force. If security measures become more stringent and counterterrorism surveillance limits the ability to physically access targets, the terrorist motivation to invest in advanced computer security teams in order to carry out highly destructive acts through the cyber domain will very likely increase.

Conclusions

The 40 cyber terrorism scenarios referred to in this section provide key qualitative insight into what types of attacks may be possible in the next three years which have the potential to directly impact Pool Re's insured portfolio. The systems described are vulnerable and will develop additional vulnerabilities as technology develops if not rigorously tested and safeguarded against cyber compromise. Information and operational technology is not yet at the stage where any digital system can be considered completely impenetrable.

It should be noted that, given the rate of technological development and difficulty in foreseeing new breakthrough techniques, this list may quickly fall out of date as new aspects of the national infrastructure are given digital features and new technical advancements occur. New scenarios for cyber terrorism may emerge quickly due to leaps in technological innovation. While the scenarios described are unlikely to occur in a three-year period, they are practically possible and this list provides a starting place in which to examine vulnerability to cyber terrorism in physical and critical areas of UK infrastructure and industry.

4 Cyber Capabilities of Terrorist Groups

The capabilities and preferred tactics of terrorist groups evolve over time. Terrorism is asymmetrical in nature and its history is one of repeated shifts in attack strategy to outwit security forces. We should not expect the terrorist attack modes of the past to be sustained as their preferred mode of operation in the future. Hoffman's assessment of '*Terrorism Today and Tomorrow*' identifies a number of potential future trends that may shape the landscape of terrorism in the coming decades, including the emergence of state-sponsored terrorism, the persistence and adaptation by terror groups to avoid annihilation, the use of non-conventional weapons, and technological progress.

Western powers do not fear the rise of destructive cyber attacks because of their potential human impact but because of the threat posed to critical national infrastructures, physical property and national security; these exposures do not align with the motivations of most major terrorist groups known to us today. It is far more difficult to achieve a high death count with through digital than with other traditional destructive attack modes. Developing the capabilities required to carry out physically destructive cyber attacks, therefore, is very likely not as high a motivation for terrorist groups as the continued development of conventional or other novel attack methods.

Potential perpetrators

Potential perpetrators of acts of cyber terrorism can be separated into several principal groups of which the most relevant and significant to this study are Non-State Terrorist Organisations and Nation State Cyber Teams. For additional context we also include brief comparisons to three other groups, Organised Criminals, Hacktivists and 'Lone Wolf' Cyber Attackers. An in-depth analysis of Daesh's cyber capabilities is included in Chapter 5.

The capabilities and threats posed by these groups are assessed as characterised by different motivations, capabilities, and targeting priorities.

Capability scale

We differentiate between three phases of progressively more sophisticated terrorist cyber capability:

a) **Enabling** – online activities that support the operations of terrorist groups, such as publicity and propaganda, 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, including pro-active cyber breaches of networks; dissemination of malware; exfiltration of digital information; financial theft and fraud; denial of service attacks; phishing and other information technology (IT) hacking activities.

c) **Destructive** – cyber attacks that trigger physical damage or injury through spoofing operation technology (OT) and digital control systems; attacks on Supervisory Control and Data Acquisition (SCADA) systems; disabling control and safety systems;

In Figure 5 on page 15, we divide these three main capability phases into four further subdivisions, providing a 12-point scale of progressive capability development. Our review of capabilities plots evidence for attainment of each level of capability for each of the main threat actors of concern.

Almost all terrorist organisations operating today exhibit 'Enabling' cyber capability – they have their own websites, social media accounts, and use Internet technologies to communicate and facilitate operation.[1] In the following section, the 'Disruptive' capabilities of terrorist groups are detailed with examples and evidence of technical accomplishment.

From this assessment it may be concluded that the terrorist organisations with the highest motivations to damage the UK have so far failed to demonstrate advanced skills in 'Disruptive' capabilities and may be some way short of the skills required for 'Destructive' capability.

The attack scenarios which this report would consider acts of cyber terrorism require 'Destructive' cyber capability. Destructive cyber capability would likely require a group to possess a more advanced set of skills that are specific to the understanding of OT systems and the way they interact with the physical world. Typically, gaining this level of cyber skill would require engineering knowledge, such as process engineering or control systems science, and computing and hacking experience. We examine the evidence that these threat actors may be poised to invest in or achieve 'Destructive' cyber capability.

[1] See the classic textbook Hoffman (2006) '*Inside Terrorism*' which includes a chapter 'The New Media' detailing the adoption of internet technology by terrorist groups since 9/11; and also Weimann (2006) '*Terror on the Internet*' which outlines an eight-year study of the use of the World Wide Web by terrorist groups.

In the security community, capability is typically assessed in terms of a quadrant threat intelligence model. Our assessment places the threat actors in these various quadrants, as shown in Figure 4.

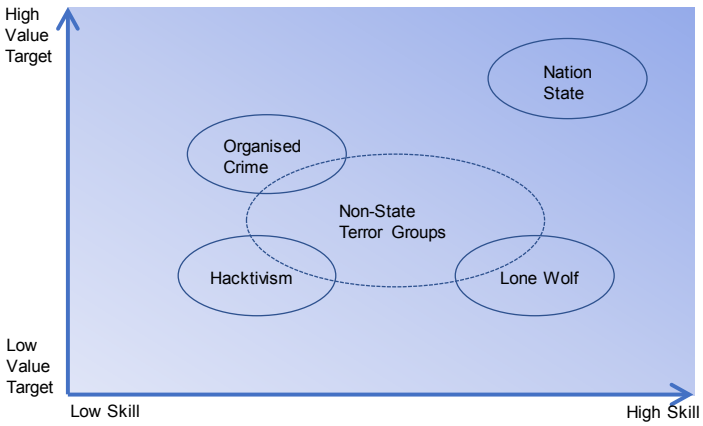


Figure 4: Quadrant threat intelligence model of cyber capabilities

It is difficult to estimate how rapidly terrorist groups could acquire the necessary skills to implement destructive cyber attacks in the future. National security operations in many countries devote significant resources to preventing terrorist groups acquiring new offensive capabilities and aggressively disrupting their advances and leadership. Private corporations, such as Facebook, Twitter, Telegram and YouTube, have also expanded their anti-terror measures to reduce the proliferation of extremist content available online. In addition to these efforts, various vigilante groups have also publicised their intent to disrupt Daesh's cyber capacity building.[2] Left to their own devices and without disruption from counterterrorism operations terrorist groups may, if motivated to do so, graduate from relatively unskilled 'Enabling' (A) capability to more skilled 'Disruptive' (B) and then on to acquire 'Destructive' (C) capability.

An organisation that is highly motivated to acquire 'Destructive' capability would advance its 'Disruptive' capabilities by adding personnel with advanced computer science and hacking skills and would then complement this development by recruiting people with experienced control engineering skills. This process could take several years of planning, recruitment, education, team integration, practice and testing before it could deliver operational capability. It is likely to require a relatively advanced technical facility and a stable and supportive environment within which to develop these capabilities.

Case Study: German steel mill, 2014

The German government's Bundesamt für Sicherheit in der Informationstechnik (Known as BSI) released a report in December 2014 detailing a past cyber attack on a German steel mill. The hackers compromised the facility using a spear-phishing procedure which initially only provided employee access details to the corporate network. After some additional reconnaissance, the hackers also compromised the plant control network. They demonstrated some familiarity of industrial control system components and caused a number of them, including blast furnaces, to fail, leading to an unregulated shutdown and 'massive' physical damage. Further specifics of the attack were not disclosed.

This is only the second cyber attack to cause confirmed physical damage after the Stuxnet worm in 2011, though, in comparison, the mode of compromise employed at the German steel mill was not as advanced or sophisticated. There is some speculation that the massive physical damage to the plant was not intended. However, evidence has not been presented that adequately supports or disproves this speculation. The incident, however, underscores that not all intrusions into critical infrastructure systems have to be carefully designed or, indeed, intended to cause harm to the system, in order to create significant physical damage.

From the evidence to date, even if these development processes were uninterrupted and fostered by a supportive environment and a technically advanced facility, there remains a relatively low likelihood that the terrorist groups currently pursuing a degree of in-house cyber expansion would develop a 'Destructive' cyber capability within the three-year time frame of this report's outlook. However, the ambition and motivation to acquire the skills necessary to carry out such attacks may prevail, and the fluid nature of cyber knowledge and the development of powerful tools may, in time, significantly lower the user requirements to carry off an attack that is guaranteed to produce a destructive result. It is paramount that intelligence services and governments remain cognisant of the threat and monitor indicators for its development.

[2] A group calling itself 'New World Hacking' claimed responsibility for a record-breaking, intense denial of service attack on BBC website, claiming to have been testing tools to combat Daesh, *TechRadar* (2016)

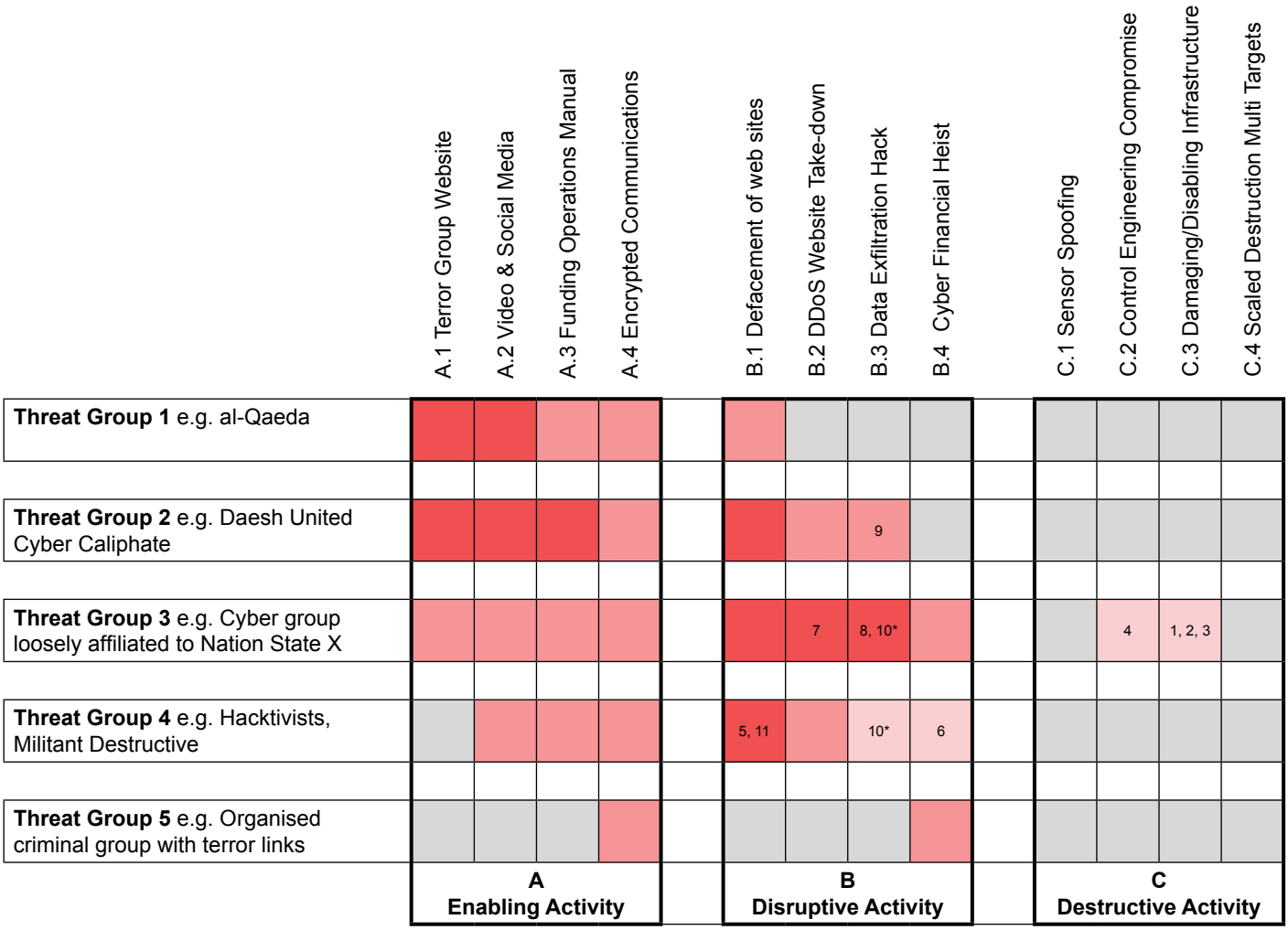


Figure 5: Cyber Threat Capability Chart, showing evidence for which threat actors have attained capabilities on a 12-point scale, left to right, towards 'Destructive' capabilities. Chart colouring indicates frequency of event and confidence in attribution at time of writing. Events and forensic updates garnered since December 2016 are marked and listed below.

1. **Ukrenegro/Ukrainian Blackout (December 2016)** – moderate confidence in state-sponsored actor
2. **WannaCry (May 2017)** – moderate confidence in state-sponsored actor
3. **NotPetya (June/July 2017)** – moderate confidence in state-sponsored actor
4. **UK and US ICS malware evidence (reported July 2017)** – moderate confidence in state-sponsored actor
5. **NHS website defacement (January 2017)** – hacktivism as claimed by Tunisia Fallaga Team
6. **Barts Health NHS Trojan malware (January 2017)** – unknown, hacktivism likely
7. **Shamoon reappearance (January 2017)** – likely state-sponsored actor
8. **Operation BugDrop (February 2017)** – moderate confidence in state-sponsored actor
9. **Kill list release by United Cyber Caliphate (April/May 2017)** – Daesh affiliated United Cyber Caliphate
10. **Brute force attack on UK MP emails (June 2017)** – likely state-sponsored (*) OR hacktivism (*)
11. **US government website defacement (June 2017)** – hacktivism, Team System Dz

A. Enabling Activity

Online activities that indicate that the group has mastered levels of information technology usage to promote and facilitate the spread of the group's ideologies, recruitment, and operational functionality.

A.1 Terror Group Website

Ability to mount an internet presence via a website with persistence against counter-terrorism removal. Skills required are simple web master and portability of site when taken down by security establishment.

A.2 Video & Social Media

Mastery of web posting of video messages, propaganda, usage of social media, professional production. Ability to sustain a following and supply a flow of communications to their wider support community.

A.3 Funding Operations Manual

Ability to distribute documents and evade counter-terrorism actions to take down documents. Documents distributed provide key know-how to the operational prosecution of terrorist activities, particularly fundraising.

A.4 Encrypted Communications

Identifiable routine or default use of encryption techniques and applications to keep messages opaque to outsiders, particularly law enforcement and intelligence services.

B. Disruptive Activity

Abilities to cause loss of function in online information technology systems operated by others, demonstrating 'hacking' capability and criminal operations.

B.1 Defacement of websites

Technical capability to hack into other peoples' websites and corrupt or change the content of sites, overcoming website security. Level of capability demonstrated within B.1 category will depend on the degree of security in place on the websites that were successfully attacked.

B.2 DoS Website Take-down

Ability to carry out denial of service (DoS) attacks on a target third-party website that causes loss of service. For a distributed DoS (DDoS) attack this requires the capability of building, purchasing, or assembling a bot-net or 'DDoS cannon'. Level of capability demonstrated within the B.2 category will depend on the type of attack, with volumetric attacks being the most common and easily achieved, and with increasing technical difficulty: application-based DoS attacks, Protocol-based (Transmission Control Protocol) connection attacks, and fragmentation attacks. Capability level is also indicated by the intensity of a distributed DoS attack (in giga-bits per second) and duration of outage achieved, relative to the capacity of the server as represented by number of visitors per month and ranking in global terms, such as the Alexa Internet website rankings.

B.3 Data Exfiltration

Ability to mount a data exfiltration attack on a network to steal data from a secure location. For example, this type of attack may be used to publicise the names and address of armed forces personnel to incite attacks on them (so-called 'kill lists'). Doxing is included in this category, although data used in such attacks may be publicly available. Level of capability demonstrated by a data exfiltration attack within B.3 depends on the techniques used for penetration, accessing stored data, and exfiltration to remove the data without detection.

B.4 Cyber Heist

Ability to mount a cyber attack that results in the theft of money, for example to fund the terrorist organisation and its operations. The capability to mount a successful cyber financial theft requires not just a level of technical expertise to overcome the high levels of security in place in financial services and monetary transaction systems, but also to launder the money to evade tracking and detection. The level of capability within B.4 is demonstrated by the scale of financial theft value, with a moderate number of fraudulent personal credit card transactions being of lower capability than a diversion of a large amount of funds from within a secure financial services payment settlement system, for example.

C. Destructive Activity

Capability to carry out digital operations that results in physical damage or interfere with real-world operations.

C.1 Sensor Spoofing

Ability to interfere remotely with a digital monitor or piece of equipment that produces data signals to cause it to send incorrect information to a third party. Sensor spoofing could be used to augment traditional terrorism operations, or to instigate damage as part of a destructive attack. The level of capability demonstrated within C.1 depends on the number and complexity of the sensors spoofed, and their protection, access controls and network configurations.

C.2 Control Engineering Compromise

Ability to remotely interfere with the correct functioning of a component of control engineering within real-world processes or machinery. The level of capability demonstrated within C.2 depends on the configuration, complexity, network access difficulty, and security protection on the control engineering component. The resulting damage that can occur may not be directly proportional to the complexity of the attack.

C.3 Damaging or Disabling Infrastructure

Ability to mount a damaging or disabling attack on critical national infrastructure requires multiple components and coordination of several elements of these capabilities. The level of capability demonstrated within C.3 depends on the type of CNI system attacked (grading from water systems, power systems, landlines to wireless telecommunications), the scale of the attack in terms of the numbers of components and units attacked, sophistication of the attack in delaying diagnosis and in preventing repair and reconnection by forensic and response team.

C.4 Scaled Destruction of Multiple Targets

Ability to mount system and widespread attacks causing physical damage to many targeted assets in the same attack operation. The range of potential types of target assets of concern to Pool Re is identified in Chapter 3. The scale of attack achieved, in terms of the number of targets attacked and the severities of damage achieved is the key level of capability of concern within the ultimate C.4 level of capability.

Non-State terrorist organisations

Non-state terrorist organisations and proscribed international terrorist cells include groups such as al-Qaeda, Daesh, and radical extremists that have demonstrated their willingness and ability to carry out acts of political violence against the West and United Kingdom. This willingness was culminated most recently in four either inspired or associated attacks on the UK mainland between March and October of 2017. The deadly and destructive acts perpetrated by these groups to date have not included sophisticated cyber techniques, although most of these organisations use the internet, social media, and IT techniques to disseminate propaganda, drive recruitment, raise funds, provide online recipes to construct homemade explosives and enable clandestine communications that support their operations.

The stated intent of terrorist groups to undertake sophisticated cyber operations currently exceeds their capabilities. Public statements regarding network size, strength or attack responsibility made on social media channels cannot be verified, due to the difficulties of cyber attribution, and, therefore, it can be difficult to accurately determine the size of such groups or properly gauge their capabilities or ambitions. Thus far, their actions have not yet caused destructive results, and they have not demonstrated the skills or coordination necessary to carry out an attack that could be classed as an act of cyber terrorism.

As of 2017, the United Kingdom Home Office lists 71 Proscribed International Terrorist Groups, not including 14 organisations present in Northern Ireland.[3] The United States State Department lists 61 organisations as Foreign Terrorist Organisations using similar criteria.[4] Cyber capability assessments for these organisations are not public, but are occasionally referenced in official documents or pronouncements and include the following cyber wings of terrorist organisations:

United Cyber Caliphate

Ghost Caliphate Section (Possible links to AnonGhost)

Sons Caliphate Army

Caliphate Cyber Army (Possible links to AnonGhost)

Kalachnikv E-security Team

The United Cyber Caliphate (UCC) is a collective of four previous disparate groups, all with an avowed allegiance to Daesh. It is thought that the groups are the successors of earlier Daesh cyber collectives, most notably, the Cyber Caliphate Army (CCA) and the Islamic State Hacking Division (ISHD), both under direction of Junaid Hussain before his death in 2015. In 2015, the CCA had published threats to attack 'internet targets' on the anniversary of September 11 and subsequently publicised plans to attack Google in January 2016. Neither attack materialised. ISHD had reportedly posted the personal information of hundreds of members of the military and government personnel in 2016, urging followers to attack them.[5] At present, the group appeared to have divided into subdivisions which are now thought to make up the United Cyber Caliphate.[6]

It should be noted that Junaid Hussain's organisations were based in Daesh territory and had direction and

[3] UK Home Office, 2017, Proscribed Terrorist Organisations; 3 May 2017

[4] US Department of State, 2017; Foreign Terrorist Organizations; Bureau of Counterterrorism.

[5] *Heavy*, 2016, 'ISIS 'Cyber Caliphate Army' Announces Plans to Hack Google'; Jan 26, 2016.

[6] L. Alkhouri, A. Kassirer and A. Nixon, 2016. "Hacking for ISIS: The Emergent Cyber Threat Landscape' , *Flashpoint,* April, 2016.

approval from Daesh officials; it is unknown whether UCC maintains a similar status. The UCC, although high profile, has had little direct relevance or impact to Daesh attacks in the West, asides from the release of several kill lists.[7] The group maintains a high level of visibility, most notably on social media platforms. In March 2017, the group claimed their leader, Osed Agha, had been killed in an airstrike in Raqqa.[8]

Team System Dz

Team System Dz is a collective with membership spread mainly across North Africa which supports pro-Daesh, anti-Israeli and other Islamic extremist causes. The group primarily participates in website defacements and shares its exploits on social media platforms. Team System Dz is thought to have a low skill level and poor operational security practices. Their targets of choice are usually outdated and consist of provincial Western websites with have minimal security. In the spring of 2017, the group embarked on a spate of US website defacements, vandalised pages associated with Ohio Governor John Kasich and Brookhaven, Long Island with messages reading: 'Anti: Govt all word [sic]. You will be held accountable Trump, you and all your people for every drop of blood in Muslim countries,' and 'I love Islamic state [sic]'.[9] The type of website affected is judged to be unimportant; the attack indiscriminately affected websites with similarly poor levels of security and associated systems.

Tunisian Fallaga Team

Tunisia Fallaga Team supports pro-Islamic causes usually seeks to bring human rights abuses in Middle East to greater attention. The group carries out website vandalism, most notably in January 2017 when it defaced 12 NHS websites.

United Islamic Cyber Force

United Islamic Cyber Force (UIFC) is a diverse and globally connected hacktivist group, supporting worldwide pro-Islamic causes. In August 2017, Group IB identified several members of their group, publicly releasing their photos, social media accounts and private email addresses.[10] Many appear to be young and inexperienced in the cyber realm. The group typically commits website defacements and crude DDoS attacks.

Syrian Electronic Army

A group of computer hackers who first surfaced online in 2011 to support the government of Syrian President Bashar al-Assad. Using spamming, website defacement, malware, phishing, and denial of service attacks, it has targeted political opposition groups, western news organisations, human rights groups and websites that are critical of the Syrian regime. They have been accused of hacking France's *Le Monde* newspaper's Twitter account in 2015. Several members have been arrested since 2016 and the group's profile has gradually receded.[11]

Hezbollah Cyber Group

Several threat actor groups operating in Lebanon and the Palestinian territories claim allegiance to Hezbollah, a Lebanon-based Shia paramilitary organisation. These organisations are thought to receive backing from Iran, Hezbollah's main benefactor. Groups linked with Hezbollah have been accused by Israel of using advanced malware against targets, an indication of state backing.[12]

Presently, the major terror groups posing a threat to the UK Mainland (Daesh and al-Qaeda) have, through their support and affiliate groups, have only developed Low Skill, Low Value Target (LS/LT) capabilities, meaning that teams are relatively unsuccessful in identifying vulnerabilities in targeted systems and have maintained this status since 2015. Attacks are low impact and mostly involve website defacement and occasional denial of service attacks. It is also clear that Daesh's targets are not strategically defined, and that the group has not yet invested sufficient time in planning and preparing its cyber attacks. For instance, the hijacking of US Central Commands (CENTCOM) Twitter and YouTube accounts by the Cyber Caliphate, remains one of the groups most high-profile achievements. Yet, the hijacking caused no operational disruptions, garnered no usable intelligence and created minimal disruption, causing no long term strategic or tactical damage. At most, it could be seen as a propaganda publicity stunt, aimed at recruiting individuals for both cyber and physical operations.

However, this does not discount the future threat of Daesh in the cyber domain. As Daesh territorial cohesion disintegrates, it is probable that they will invest renewed efforts in exploiting the cyber domain and establish a "virtual caliphate". An increased propaganda and social media presence is highly likely, with coordinated and prolonged website defacement

[7] K. Wolf, 2016. 'Evaluating the Physical Threat from UCC Kill Lists' , *Flashpoint*, 28 October, 2016.

[8] A statement from the United Cyber Caliphate was made on March 16, 2017. Screenshots of the announcement were made available by terrorist researchers on Twitter.

[9] J. McBride, 'Team System DZ Pro ISIS Hacks: Kasich, Brookhaven Targets', *Heavy*, 26 June, 2017.

[10] Group-IB, 'Hacktivists Unmasked', 2 August, 2017.

[11] E. Nakashima, 2016. 'Syrian hacker extradited to the United States from Germany,' *Washington Post,* 9 May, 2016.

[12] B. Opall-Rome, 2015. 'Israel Confirms It Was Cyber Attack Target,' *Defense* News, 24 June, 2015.

campaigns along with continued experiments with DDoS and other hacktivist tools are likely. The recruitment or radicalisation of lone wolf actors stationed in the West, however, presents the greatest strategic cyber terror threat. Lone wolves may have advanced cyber skills, as well as the means and will to act with greater freedom and opportunity in both the cyber and physical domain. The recruitment of lone wolf cyber soldiers poses a significant challenge to counterterrorism strategies, as these individuals may require little direct communication with suspect parties and can act in an impulsive fashion .[13] If Daesh can plausibly direct these individuals toward a shared destructive goal, the group will acquire the ability inflict greater physical and economic damage.

Recruiting overseas cyber specialists is not historically restricted to Daesh. Intentions to develop cyber capabilities have also been observed in Southeast Asia, especially in Indonesia, where the hacking and defacing of websites is prevalent and used to gather funds for terrorist activities or show support for arrested extremists. Immediately after the 9/11 attacks, Osama bin Laden, then first general emir of al-Qaeda, planned to co-opt cyber experts in the same way al-Qaeda enlisted the support and cooperation of some scientists. Bin Laden gave a statement to an Arab newspaper in 2002 claiming that, 'hundreds of Muslim scientists were with him who would use their knowledge… ranging from computers to electronics against infidels.'[14] Furthermore, al-Qaeda's wider leadership conceived of and planned to conduct attacks against Western critical infrastructure. This was observed when engineering software and data on computerised water systems and electronic models were discovered on al-Qaeda laptops requisitioned in Afghanistan.[15]

A handful of computer engineers worked with al-Qaeda after 2001, but there is no evidence to indicate that al-Qaeda Central engaged in preparations to mount a cyber attack. Al-Qaeda itself could not develop cyber attack capabilities but other individuals and groups did. As al-Qaeda was considered the vanguard, its associated groups also urged their supporters elsewhere to develop similar capabilities, starting in 2006. These attacks were largely conducted to generate publicity and were not otherwise strategic in nature. Attacks were advertised on Facebook, Twitter and discussion forums. Some groups intended to conduct DDoS attacks and data breaches but were not successful.

From 2012, al-Qaeda called for attacks against network-connected infrastructure and promoted plans to 'remotely hijack American unmanned aerial vehicles and drones, power stations and refineries, and communications systems.'[16] In December of that year, supporters of al-Qaeda created al-Qaeda Electronic groups with al-Qaeda Electronic in Egypt and the Tunisian Cyber Army. Associated with AQAP, al-Qaeda Electronic was formed in 15 January 2015. The group engaged in defacement of websites and occasionally conducted DDoS attacks.[17] For instance, al-Qaeda Electronic claimed to hack the website of the French sports club Fontainebleau and uploaded a page to its server with the declaration. It also defaced 22 British websites, five websites belonging to Austria-based businesses, and attempted to deface a website of the French software company Edicot. Al-Qaeda Electronic defaced Russian, Norwegian, and Vietnamese websites, displaying the statement from Osama bin Laden that America 'will not enjoy security' until legitimacy and safety is achieved for Palestinians.

The development of terrorist technologies to attack information infrastructure through cyber attack is expanding the current threat landscape as it has been understood since the 1990s. Both Daesh and al-Qaeda consider cyber attacks a valid instrument of jihad in carrying out operations against their enemies' information infrastructures. With a majority of terrorist communications with Western actors now conducted via social media, security and intelligence services have developed social media analysis as one of the sub-disciplines of SIGINT, in order to monitor the new wave of terrorist planning in this increasingly networked domain. Recent chatter on social media accounts and dark web forums indicates that Daesh affiliated groups are seeking both increased skills and capabilities. The most tangible iteration of this threat involves a terrorist group purchasing an increased cyber skill set through collaboration with or the anonymous employment of a cyber criminal actor.

Nation State cyber teams

It is thought that over 60 countries now make, use, and deploy cyber weapons, with plenty of instances of attack documented even as far back as 2003.

Many countries maintain national cyber teams, with at least six countries having capabilities that analysts consider as 'advanced'.[18] Most of the countries that

[13] D. Byman, 'How to Hunt a Lone Wolf: Countering Terrorists Who Act on Their Own', *Foreign Affairs*, Vol 96, No. 1, January 2017.
[14] D. Verton; 2002; 'Report: al-Qaeda a potential cyberthreat', CNN.com, 8 January 2002.
[15] G. Weimann; 2005. 'Cyberterrorism: The Sum of All Fears?', *Studies in Conflict & Terrorism*. 28:129-149, 2005.
[16] E. Liu, 'al-Qaeda Electronic: A Sleeping Dog', Critical Threats Project of the American Enterprise Institute, December 2015.
[17] Ibid.
[18] J. A. Lewis, 2012, 'Cybersecurity, Threats to Communications Networks, and Private-sector Responses', Testimony to House Committee on Energy and Commerce, Subcommittee on Communications and Technology, February 8, 2012.

Case Study: Ukrenergo blackout, Ukraine, 17-18 December 2016

On the night of 17 December 2016, Ukrainian state power distributor Ukrenergo experienced a cyber attack that led to a short yet sustained power outage. Attribution for the cyber attack responsible was obtained on June 2017. Several distinct characteristics of the malware found – termed CRASHOVERRIDE – shared features with BlackEnergy and HAVEX malware, which have been utilised by the APT group Sandworm. APT Sandworm is thought to have connections to the Russian government and intelligence agencies. CRASHOVERRIDE is thought to be an evolutionary software effort that has demonstrated increased malware capabilities and adaptability. CRASHOVERRIDE has inherent features that allow it to map industrial control systems and adapt to operational environments, meaning that it could be launched in various settings and regions with minimal effort. The full potential of CRASHOVERRIDE's capabilities was not realised at the time of the blackout, and the malware discovered on Ukrenergo's systems likely represented a research and development effort by the APT.

maintain significant military capabilities now have cyber units. Several of these countries are potential adversaries of the United Kingdom and the West, including North Korea and Iran. Foreign state-sponsored cyber teams from several countries are suspected of conducting espionage and information gathering by penetrating systems in the United Kingdom.

Cyber attack could offer a means for hostile states to engage in 'asymmetric' warfare against the UK Mainland. The difficulty in assigning responsibility for cyber attacks affords a measure of protection for attackers seeking to avoid provoking retaliation by a stronger opponent, while the dependence of modern societies on digital networks offers the opportunity to create a meaningful impacts on the target.

State-sponsored cyber teams have the capability and resources to mount an operation such as the scenarios detailed in this report. It is possible to envision situations of either miscalculation by a potential sponsor state or a state using a proxy organisation to carry out a demonstrative attack, perhaps as a warning or deterrent to United Kingdom foreign policy. It would likely involve concealment or complex routes of attribution to avoid or complicate an international response. There are strong deterrents against nation states executing an attack on the UK, but hostile state-sponsored cyber teams are one of the few potential candidates with the resources to perpetrate significantly damaging cyber attacks on UK infrastructure.

Organised criminals

The internet is used heavily in organised crime activities, both for its traditional operations and for cyber crime. Organised cyber crime has become systemic and transformed into a service industry. The continuous release of sensitive information, such as the zero-day exploits and cyber weapons made available in the ShadowBrokers' data dumps, along with the mainstreaming of anonymous cryptocurrencies has expanded the criminal market functionality. It is now possible to buy both point-and-click and customised malware on the dark web. Several businesses offer services such as Ransomware-as-a-Service (RaaS) and Malware-as-a-Service (MaaS), meaning that those with motivation can vastly increase their capabilities without the need for further technical skill or coordination. It is thought that accrued earnings from ransomware alone has risen from $325m in 2015 to over $5 billion in 2017.[19]

Many cyber criminal organisations conduct their operations in communities overseen by kleptocratic governance, often lacking the capacity and or will to create and maintain proper enforcement or surveillance mechanisms. Certain cyber criminal groups share significant strategic overlap in motivations and aims with their native state government, sometimes resulting in clandestine collaboration or tacit sanction of damaging cyber criminal activity.

Hacktivists

Hacktivists are loosely organised cadres of activists, capable and willing to hack for political reasons. They form in groups based on a shared sense of mission. Often members do not know each other's real names and only coalesce under *nom-de-guerre* or 'handles' to achieve an aim. Groups are typically heterogeneous, geographically diverse and fractious.

Anonymous best represents this heterogeneous community, with participation spanning the spectrum of political and religious ideologies. For instance, Anonymous supporters with pro-Islamic beliefs conduct #OpIsrael annually, harassing Israeli

[19] S. Morgan, 'Ransomware Damage report 2017 Edition' , *Cyber Security Ventures,* 18 May 2017.

government and private websites with DDoS attacks and defacements. Likewise, other elements connected to Anonymous have undertaken #OpIsis to degrade Daesh cyber capabilities, member actions, and group propaganda. Disparate groups within Anonymous conduct operations including the exposure of paedophiles, support for environmental activism and anti-racist campaigns, or spreading anti-capitalist messages. Hacktivists are often mocked by security industry insiders and are considered more of a nuisance than a strategic threat. Anonymous has publicly stated that they are not interested in disrupting critical infrastructure. However, they have been known to penetrate industrial systems and explore these for the sake of embarrassing companies with poor security. Many hackers, known as 'greyhats', knowingly violate the law in order to discover security weaknesses that their services can then reconcile for profit. This semi-legal area between greyhat hackers, corporations and security services has proven highly beneficial to cyber security. Overall, the most dynamic hacktivists' skill sets have remained relatively flat over time, with no significant development seen in last five years. Their fractious and disorganised nature has limited their ability to overcome significant logistical burdens and coordinate sustained attacks on high value targets.

The commodification of hacking capabilities, with tools capable of conducting Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, and the introduction of customised malware services, has led to an expansion of hacktivist participation. A bare minimum of technical knowledge and coordination is needed to perpetrate disruptive attacks. As this market matures it is likely that the capacity of hacktivists to conduct increasingly sophisticated attacks will grow.

'Lone wolf' cyber attackers

Individuals can and do create significant damage on the internet. It is possible to hack industrial systems as an individual, and there are advantages in that operational security is better preserved and the hacker is less likely to be compromised by HUMINT operations by law enforcement. In exchange, a lone wolf attacker adopts the entire burden of attack research and development. The individual cannot depend on others for different elements of an attack or campaign, or rely on the external funding necessary to carry off an attack of great sophistication. Furthermore, lone wolves have the potential to function either individually, or as an ancillary, to every threat type, including cyber terrorists.

The most insidious type of lone wolf would be that of the insider threat, whose access and specific knowledge would significantly amplify an attack arranged by a foreign cell.

Terrorist cyber capability development

Since the emergence of the internet during the 1990s there has been a consensus that the 'cyber' domain would ultimately become a new theatre for crime, geopolitical conflict, state violence and terrorist activity.

Threat groups, like insurgents, criminals, and terrorist extremists have steadfastly developed their capabilities to exploit the virtual world. In the first of these phases, which we refer to as 'Enabling' (See Figure 5), threat groups used the Internet to disseminate propaganda and lobby constituencies, raise and move funds, procure supplies and technologies, learn how to produce multiple identities, securely communicate, provide a safe meeting place to plan and coordinate operations, mount surveillance and reconnaissance, and rehearse. The second phase – the expansion into 'Disruption' based cyber attacked – was initiated at the start of the millennium when threat groups started developing cyber capabilities to mount information infrastructure attacks. The world, however, is yet to experience the first incidence of significant cyber terrorism which is labelled as such with international consensus.

It is difficult to estimate how rapidly terrorist groups could acquire the necessary skills to implement 'Destructive' cyber attacks in the future. National security operations in many countries now devote resources to prevent terrorist groups acquiring new capabilities and aggressively disrupt their advances and leadership. In addition to national security teams, various vigilante groups are also publicising their intent to disrupt Daesh cyber capacity building.[20]

The 2015 UK National Security Assessment, which gave rise to a new National Cyber Security Programme, states that Daesh pose a threat in targeting of air traffic control systems, hospitals, and other critical infrastructure networks through cyber attack.[21] The UK NSA assessment is that Daesh do not yet have this capability but 'they are doing their best to build it.' The assessment and National Cyber Security Programme is a preparation for cyber warfare and hybrid conflicts, of which terrorist attack is one element.

[20] A group calling itself 'New World Hacking' claimed responsibility for a record-breaking Denial of Service attack on BBC website, claiming to have been testing tools to combat IS, *TechRadar* (2016)

[21] Gov.uk, 2015; 'Chancellor sets out vision to protect Britain against cyber threat in GCHQ speech'; Spending Review and Autumn Statement 2015.

Dependency on attribution

Within the Pool Re framework, the determination of whether an event is an act of terrorism is ultimately the decision of Her Majesty's Treasury and, for losses to be compensated by Pool Re, HM Treasury will need to publicly certify the cause of the loss as an act of terrorism . Therefore, it is for Her Majesty's Treasury to consider the nature of an attack to decide if its capable of certification as an 'act of terrorism'.

Under the Reinsurance (Acts of Terrorism) Act of 1993, under which the Pool Re scheme was created, terrorism is defined as 'acts of persons acting on behalf of, or in connection with, any organisation which carries out activities directed towards the overthrowing or influencing, by force or violence, of Her Majesty's government in the United Kingdom or any other government *de jure* or *de facto*.' This definition requires attribution of the act to an individual or an organisation, as well as the determination of the motivation behind the act.

Cyber attacks differ from traditional types of terrorism in terms of attribution; cyber attacks may be as destructive as a conventional act of physical violence, but can be more difficult to attribute to a specific perpetrator or trace to a reliable point of origin. We would traditionally expect acts of terrorism to be claimed by or attributed to an active group, but it may be possible for terrorist groups to carry out cyber attacks anonymously in the future and to forgo claiming responsibility for any destructive impact. Political motivation behind an attack may be similarly difficult to discern without firm proof of attribution.

5 Cyber Capabilities of Daesh

The most prominent terrorist group showing intention, persistence and determination to conduct digital attacks is Daesh. The group's early ambitions to penetrate the internet were made visible even before the self-styled Caliphate was declared in June 2014, when the group established capabilities to operate not only in the physical space of Syria and Iraq, but also in the borderless virtual space. Its fledgling online presence was restricted mostly to the dissemination of its propaganda, but this has changed in the past year with increased attacks by Daesh and its supporters on the information infrastructure of government and private businesses. Daesh's exploitation of their territorial gains and a savvy social media PR strategy allowed for the recruitment of thousands of foreign fighters and technical operators from across the globe through 2013 and 2014.

At the time, several Daesh sympathisers stationed outside of the Middle East provided the group with intellectual and material support. This support was utilised in the high number of Twitter, YouTube, Facebook and other social media posts and reposts; fighters on the ground in Syria were not responsible for most of this social media strategy. The language used in these posts and the targeting of specific grievances throughout Western communities infers localised and specialised knowledge.[22]

In response to the loss of central territory in 2016 and 2017, Daesh is expanding horizontally into a markedly more networked coalition of self-proclaimed '*wilayats'*, or provinces. Through the end of 2016 and into the first part of this year, Daesh's communications tactics began to urge Western sympathisers to either travel to affiliated *wilayats* outside of the Levantine heartland or remain at home and propagate *jihad* action locally to the best of their ability. With this strategy, Daesh seeks to conserve its manpower and influence laterally and engage localised groups whose grievances overlap with their own. While Daesh has continuously encouraged localised attacks, the disintegration of a physically coherent caliphate has accelerated the tactic and will likely continue to do so. The high number of small-scale terror attacks in the West since 2016 can be attributed to this strategic shift in Daesh thinking.

The fragmentation of Daesh's territory will very likely add to a rising convergence of interests between cyber terrorists, cyber criminals, hacktivists and enablers, as Daesh's focus transitions from military and territorial objectives to that of a traditional terrorist network. The bulk of the cyber activity thus far attributed to Daesh is heavily linked to uncoordinated lone wolves, engaged in forms of enabling and disruptive hacking. These lone wolves usually do not have insights into deep or quality intelligence, and end up targeting public profiles to little effect.

Although disrupted by military and counterterrorism efforts, Daesh's internet presence and hydra-headed communications channels are difficult to shut down completely and, while they have been significantly degraded, in practicality, remain functional. These channels often remain anonymous, and provide anything from intellectual and moral support, to ideas on how to perpetrate simple soft-target attacks, instructions for bomb making, targeting lists and network formation.[23] In the meantime, deeply indoctrinated Western fighters are returning home to Europe and the UK, posing a threat to national security that is difficult to quantify.

Daesh threat

The threat posed by Daesh in the immediate (one to two years), mid (five years) and long term (10 years) can be forecast by considering their intent, capability and opportunity to attack. The growth of the market for hacking tools since 2016 has benefited Daesh; the group has stated its interest in keyloggers, RaaS, MaaS, and the development of experimental DDoS tools, which are available from dark web marketplaces.[24]

To date, Daesh's most effective cyber achievements do not suggest they have advanced their available skill set significantly. The active groups can, however, give the impression to their followers and an interested, though under-informed, audience that they have hacked and accessed the encrypted sensitive information themselves. Currently, Daesh's affiliate cyber groups do not possess the capability to penetrate secured systems. However, their experiments with DDoS attacks, such as with the so-called Caliphate Cannon, show a degree of initiative. While these groups are not currently capable of penetrating and manipulating secured systems, there is communications evidence to suggest that they have sought out tools to do so, and that the risk of

[22] D. Byman, J. Shapiro, 2014. 'Be Afraid. Be A Little Afraid: The Threat of Terrorism from Western Foreign Fighters in Syria and Iraq.' *Foreign Policy at Brookings,* November.

[23] B. Hoffman, 2017. 'ISIS Intent on an Even Deadlier Ramadan This Year.' *The Cipher Brief,* June 6.

[24] K. Wolf, 'Cyber Jihadists Dabble in DDoS: Assessing the Threat', *Flashpoint*, 13 July, 2017.

cyber terrorist action against the West will intensify in the mid to long-term.

Both Daesh Central and its supporters, including lone wolf actors, may move to build up their capabilities using the dark web to download hacking tools and trade information and knowledge with their fellow members. The dark web hosts black markets that sell malware and tool kits, (e.g. key loggers), to carry out cyber attacks. Although Daesh has retained some resident IT experts throughout its *wilayat* network, these individuals are not highly skilled, and are reliant upon on outside capabilities.

The transition to a 'United Cyber Caliphate'

Since 2014, the internet savvy media units of Daesh, such as al-Hayat and al-Furat Media, exhibited great success in disseminating propaganda via the internet. A British foreign fighter in Syria with expertise in hacking, Junaid Hussain, going by the alias Abu Hussain al-Britani, coordinated the gathering of pro-Daesh individuals with cyber expertise, and directed them to conduct Daesh-inspired attacks in the name of the group. It became known as the Cyber Caliphate after claiming to have carried out a cyber attack against the *Albuquerque Journal* and on unnamed 'US official network communications ' in December 2014.[25] While living in Birmingham, Junaid Hussain was a member of hacktivist group Team Poison, and claimed to have 'hacked Mark Zuckerberg's Facebook page, named and shamed members of the far-right English Defence League, and leaked the address book of Tony Blair's personal assistant.'[26] After relocating to Syria in 2013, he reportedly compromised French websites during the 2015 Île-de-France attacks, and the Twitter feeds of the U.S. Central Command, *Newsweek* and the *International Business Times*.

After a joint US-UK drone strike killed Junaid Hussain on 24 August 2015, Daesh rebranded Cyber Caliphate as the Cyber Caliphate Army (CCA).[27] The group's presence was detected in January 2015 when they carried out several disabling cyber attacks against the US Military's Centre Command (CENTCOM) Twitter and YouTube social media, which were taken offline. CENTCOM stated that military networks were not compromised and that the incident was regarded 'as a case of cyber-vandalism.'[28] Since then, CCA had appeared to be expanding with its partnership with pro-Palestine hacking group AnonGhost. The partnership was dubbed the Ghost Caliphate and was announced by the group using a YouTube video titled, 'The Rise of the Caliphate Ghosts'. In the video, CCA and AnonGhost used the online moniker 'Ghost Caliphate', and pledged allegiance to Daesh.[29]

On 4 April 2016, an Daesh supporter known as Husam al-Tunisi announced on his Twitter page that three pro-Daesh cyber groups – the Caliphate Cyber-Army, Sons Caliphate Army and Kalashnikov Team – had merged to form a new hacking group called the United Cyber Caliphate. Such a merger can be seen as an effort to improve the groups' capabilities at the disposal of Daesh command through greater coordination and collaboration. In many respects, the formation of the United Cyber Caliphate (UCC) could be thought of as the successor of the CCA along with the Islamic State Hacking Division. Like the CCA, UCC, and other Daesh-linked cyber groups are involved in the release of Westerners personal information, especially the details of government and military personnel, with the intent to inspire lone wolf attacks on these individuals. The use of social media to encourage and facilitate random lone wolves has been extremely effective: 2015 and 2016 saw the rate of lone wolf attacks in the United States and Europe double compared to 2011 through 2014.[30] Although high profile, due to its mission statement and stage of 'evolution', the UCC has thus far shown little direct impact in the size or importance of its attack against the west, outside of the release of kill lists, propaganda, and terrorist snuff videos. The UCC's most recent major action was the April 2017 release of 8,786 US targets including churchgoers and synagogue members for lone wolf attacks following the death of their leader Osed Agha.

Determining cyber ambitions

The formation of the UCC demonstrates a willingness to coordinate resources and attacks, which could be considered a stepping stone to enhancing cyber capabilities to a HS/HT nature. For instance, it has been rumoured that al-Qaeda and Daesh have experimented with developing their own secure chat platforms around existing architecture, though Daeh's' prolific use of Twitter, Telegram, WhatsApp and other known encrypted communications apps suggests limited success.[31]

[25] 'Anonymous Declares War on "Cyber Caliphate" as Part of "Operation Ice ISIS Phase II", *SITE Intelligence Group*, 12 January, 2015.

[26] L. Murphy, 'The Curious Case of the Jihadist Who Started Out as a Hacktivist', *Vanity Fair*, 15 December, 2015.

[27] Ibid.

[28] D. Lomothe, 'US military social media accounts apparently hacked by Islamic State sympathisers', *The Washington Post*, 22 January 2015.

[29] 'Caliphate Cyber Army Releases Video, Joins with AnonGhost to Form 'Ghost Caliphate', *SITE Intelligence Group*, 8 January 2016.

[30] D. Byman, 2017. 'Can Lone Wolves be stopped?' *Brookings,* March 15, 2017. Accessed August 28, 2017.

[31] L. Alkhouri and A. Kassirer, 2016. 'Tech for Jihad: Dissecting Jihadists' Digital Toolbox' , *Flashpoint,* July, 2016.

Flashpoint has noted that the UUC and several other cyber terrorist groups linked with Daesh have been experimenting with DDoS attacks, believing that these instances demonstrate that DDoS-for-hire services have been used. The intended development of the so-called Caliphate Cannon, a DDoS tool modelled on the Low Orbit Ion Cannon (LOIC) used by Anonymous, shows initiative, willingness to experiment and a desire to increase their capabilities or, at least, apply Daesh branding to a generic cyber tool. *Flashpoint* also notes that cyber attacks attributed to Daesh affiliate groups have had a limited and unconfirmed success rate and have slowed significantly since the beginning of the year. If DDoS-for-hire has been utilised then these groups will likely purchase and experiment with other capabilities in the future, and chatter on dark web forums continues to indicate an increased willingness to both develop and purchase capabilities. The UCC and several other collectives aligned with Daesh have carried on with their traditional activities for propaganda and radicalisation online, in addition to these exploratory ventures.

The loss of territorial cohesion may well see Daesh realigning their strategic goals towards the cyber realm. The absence of a physical base of operations limits physical attacks to insurgent groups who have claimed allegiance to Daesh, along with low-level physical attacks from lone wolfs and small groups scattered throughout the West. Accordingly, an established presence on the Internet to disseminate propaganda, strategic advice and individual encouragement will be needed in order to inspire such attacks and function as a device for Daesh's continued relevance. Likewise, the burdens of maintaining a physical presence are high. It is thought that Daesh's revenue for the year 2016 was a maximum of $870m.[32] Although the territory in it of itself was Daesh main revenue stream, hundreds of millions of dollars are now free to be used elsewhere. The acquisition of high end exploits such as zero-days, the hiring of mercenary information security specialists in the short term and the recruitment and further education of Daesh cyber operatives in the long term are now distinct possibilities.

Over the past twelve months, Ransomware-as-a-Service (RaaS) has proliferated throughout the dark web and it could function as an additional stream of financing available to would-be cyber terrorists. In the hands of an Daesh-affiliated cyber group, even faulty ransomware (in the mould of WannaCry) could be used to maximise publicity, business interruption and frustration amongst security agencies and the general public.[33] In time, Malware-as-a-Service (MaaS), although costlier, could provide Daesh-related groups with potential HS/HT capabilities, allowing for true penetration of industrial or other vital systems. It should be noted, however, that the provision of a bespoke and/or truly corrosive piece of point-and-click malware would require a high level of customisation on the part of the provider, and some degree of sophistication and coordination on the part of the user in order to be implemented effectively. Daesh and its cyber affiliates are currently limited in the damage they can cause by the quality of their received intelligence, and may seek to collaborate with an insider in order to plan a significant attack against some aspect of national infrastructure. If an insider can be radicalised, recruited and is successful in leaking sensitive information, both Daesh Central and lone wolves and wolf packs will receive crucial intelligence and will be better equipped to mount a successful cyber attack against UK cyber domains. Although it is not always possible to prevent attacks by maintaining basic cyber security, both governments and businesses must collaborate to prevent a high impact cyber attack, or, at least diminish its effectiveness. At all times, it is essential to review the cyber security to identify the gaps and loop holes to prevent a highly skilled hacker from penetrating the system.

At present, Daesh has limited skill and limited intelligence to act outside public domain. This can be attributed to the lack of intelligence to mount attacks against command and control systems of military and economic and financial centres and other highly secured targets. To carry out HS/HT cyber attacks, Daesh central would need to acquire the cooperation highly skilled, PhD-level computer scientists and engineers to plan, prepare and execute attacks. The number of individuals with this skill level is increasing worldwide, and there are educated and experienced students from Indonesia to India, Malaysia to Tunisia, potentially liable – however unlikely – to radicalisation and remote-recruitment.

Targets and activities: inspiration for others to follow

Like al-Qaeda, Daesh cyber affiliate-groups and their peripheral agents initially targeted US and its Western allies. The range of targets has since expanded to include Middle Eastern and Asian governments and their major private firms since coalition successes against Daesh. International military and municipal police websites, as well as pan-national technology headquarters including Facebook, Twitter and Google,

[32] S.Heißner, P. Neumann, J. Holland-McCowan and R. Basra, 2017. 'Caliphate in Decline: An Estimate of Islamic State's Financial Fortunes' , *ICSR,* 2017.

[33] 'Ransomware-as-a-Service is Booming: Here's What You Need to Know' , *Barkly,* March, 2017.

have been targeted by Daesh affiliated cyber groups in the past year. Reported targets include states that oppose Daesh, namely the U.S., UK, Saudi Arabia, Israel, France, Turkey, Iran and Russia, which were all named as part of the CCA's #WorldUnderHacks campaign, in which CCA members posted lists of names and details apparently obtained from institutions and government departments in the last quarter of 2015. *Site Intelligence Group* recorded that the campaign #FranceUnderHacks was the 'longest-lasting hacking campaign' and was conducted in October 2015. CCA made false claims of releasing sensitive information of French personnel including that of eight French soldiers and French Ambassador to South Africa. None of the information released is believed to be authentic.[34] CCA also released a video on 22 October 2015, in which it declared the start of the hacking campaign against France. The video suggested that these cyber attacks would take place on 24 October 2015, but these did not materialise.

Throughout 2016 and 2017, the United Cyber Caliphate (UCC) and other Daesh affiliates have continued the trend for setting ambitious goals but achieving little. For instance, the UCC released several kill lists containing the personal information of thousands of Western civilians, the largest being an April 2017 kill list containing 8,786 Western names.[35] Terrorist-associated cyber groups often assert that they have the capabilities to penetrate sensitive systems and gain confidential information against people of interest. However, in most cases, and in this, this information has been derived from publicly available open-source information.[36]

Several groups such as the Tunisia Fallaga Team and Team System Dz have conducted thousands of unspecific website defacements.[37] Although more of nuisance, hacking collectives that support Daesh are most inclined to participate in website defacements because of the relative ease of the vandalism. Defacements can be carried out individually and do not require high levels of coordination or resources; often a hacktivist can conduct these attacks in the relative safety of their own home or neighborhoods. Furthermore, the collapse of Daesh's territorial integrity will likely encourage an increase in defacements as their physical presence deteriorates.

In the winter of 2016 and January 2017, the UCC and other Daesh affiliates claimed credit for several DDoS attacks against government, military and non-governmental organisations. The veracity of these claims cannot be determined. If actual, these types of attacks represent a new phase for Daesh-linked cyber terrorist organisations. MaaS and DDoS-for-hire services, as well as other point and click tools on the dark web, allow Daesh-linked groups to expand their capabilities in a cheap and easy way.[38] Likewise, as with website defacements, the ability for several disparate groups or individuals to coordinate their actions while acting in the relative security of their homes means that such attacks are far more attractive to Daesh's current cadre of computer-literate affiliates, raising the frequency and intensity of this disruptive behaviour. However, these capabilities do not amount to real cyber terrorism; hacktivist networks have used similar tools before, to far greater effect. However, the recruitment of more capable individuals, possessing skill sets that would allow for technically advanced research, could see the eventual customisation of DDoS and malware tools for specific Deash attacks, amplifying the scope and damage that would occur as a result.

34 Ibid.

35 P. Paganini, 2017. 'United Cyber Caliphate published a kill list of 8, 786 individuals in the US, UK.' *Security Affairs,* April 6, 2017.

36 K. Wolf. 2016. 'Evaluating the Physical Threat from UCC 'Kill Lists'.' *Flashpoint,* October 28, 2016.

37 K. Sengupta. 2017. 'Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images.' *Independent,* February 7, 2017.

38 K. Wolf. 2017. 'Cyber Jihadists Dabble in DDoS: Assessing the Threat.' *Flashpoint,* July 13, 2017.

6 Defence Against Cyber Terrorism

A significant growth in the number of capable and motivated terrorist opponents may lead to an increase in the number and severity of cyber incidents in the UK. However, provide an accurate outlook on the future of cyber terrorism in the UK, it is crucial to not only monitor the threat actors but to understand the threat landscape and its mode of evolution.

The following chapter profiles the range of vulnerabilities present in UK digital systems and highlights the issues facing the gathering of accurate information and effective defence of national networks and technologies. All systems are inherently vulnerable but our understanding of these vulnerabilities and how to resolve or counteract them is significantly limited by the changeable nature of the cyber domain. The rapid development of the UK digital economy provides a growing platform for cyber attack from all types of malicious actors.

Estimating vulnerabilities

The number of vulnerabilities present in the global supply of digital products in aggregate is not known and new products or updates, when released, are rarely thoroughly interrogated for an accurate count of new avenues of compromise or susceptibility. Exploitable vulnerabilities can exist in hardware, software, network protocols and programming languages, and be present on both local and remote, or isolated or connected systems. Vulnerabilities found in hardware and network protocols are difficult to reconcile or patch, due to issues surrounding backwards compatibility, and may therefore be broadly scalable. If a programming language contains a vulnerability, that vulnerability can be replicated in any software or system written using the language.

There is substantial debate in the technology community over whether the proliferation of vulnerabilities in the digital trade is limited or infinite with regard to all software, hardware, networks, and procedures, present on both local and remote, and isolated or connected systems. What can be said with confidence is that digital systems are vulnerable, and the growth of the cyber economy and the development of new and updated technologies will create new imbedded system flaws which can conceivably be compromised, as new protocols are added and old vulnerabilities are grandfathered in.

There are vulnerabilities that are recognised and acknowledged, latent vulnerabilities that are known to exist but have not been isolated, and a further unknown quantity of vulnerabilities which are yet to be discovered. It is difficult to estimate the number of known and recorded vulnerabilities due to issues of international standardisation. Different countries record digital vulnerabilities differently, and there is no one definitive data base of vulnerabilities that the world uses. Efforts to establish such a resource are ongoing.

To complicate matters further, the naming schemes for vulnerabilities differ, and what lists do exist likely feature duplicates. Vulnerabilities that are identified are subject to a selection bias and preferential attachment. Companies and brands which are more popular can fund more vulnerability research or offer larger rewards and incentives for independent security testing than smaller firms and, as such, indirectly contribute more to known exploits databases.

Leaving the complexities of standardisation aside, the data that exists can still provide some rough metrics for estimating the breadth of vulnerabilities in the cyber domain. The number of vulnerabilities published per year numbers between 5,000 and 15,000. However, this number can vary significantly quickly, and should be expected to grow as vigilant cyber security becomes a greater social responsibility and more experts flood the field. For example, in 2014, the CERT Coordination Centre performed some testing of mobile phone apps and how they used SSL encryption methods. By automating the testing of 1 million apps, they found more than 23,000 vulnerabilities in a single year. This significantly affected the reported statistics for 2014, and illustrates how quickly these numbers can fluctuate. It also suggests that greater numbers of system exploits are identified when subject to dedicated analysis; as the cyber security field grows, the scale of vulnerabilities recognised in existing technologies is likely to increase significantly.

The number of vulnerabilities corresponds approximately to the amount of money and effort a society (or, very likely, its adversaries) puts into finding such flaws and increased funding in this area would illuminate further exploits which may be straightforwardly resolved. In the meantime, malicious blackhat hackers – individuals who purposefully breach computer security systems solely for personal gain or malice – and programmers will be looking for and selling other vulnerabilities on the dark web, without reporting their existence to databases. Their capabilities will remain hidden from our metrics, unless significant effort and intelligence gathering gives us a view into their capabilities, individually, and collectively.

The Cyber Green project

The world's computer emergency response teams report into a metrics portal at the Cyber Green Website.[39] This shared resources allows for a general metric of the performance of computer emergency response teams (CERT) globally. This useful risk metric is derived from reports submitted by global CERTs, and these teams agree to report the submitted incidents they receive in two categories: vulnerable nodes and compromised nodes.

- **Vulnerable nodes** are reports from individuals or companies regarding systems, devices, websites, or computers that are susceptible to a known vulnerability.
- **Compromised nodes** on the other hand, are those systems that have had an actualised risk, and are actively reporting bad behaviour. These can be computers that have been generally infected or incorporated into botnets and can be used for further malicious behaviour.

Loosely speaking, responding to vulnerable nodes is a 'proactive' exercise, whereas responding to compromised nodes is a 'reactive' effort.

The data is also used to provide a country-by-country risk index by ranking each country between 1 (very low risk) and 100 (very high risk). As of 2016, the UK appears in the middle of this table, with a risk index of 50.0. This represents a slight improvement from where the country was ranked in the last quarter of 2015, at 62.5.

Growth of vulnerable nodes

The list of vulnerable nodes across the UK illustrates the continually changing and shifting landscape of cyber security in the country. Indeed, at no time do we possess a complete view of our susceptibility to cyber compromise. This uncertainty is managed as well as possible, but is of significant enough size to procure sizeable risk to our digital systems.

If an ethical security researcher finds a new vulnerability, for example, in a particular brand of industrial Ethernet switch, they report it to the vendor and often a neutral third-party, such as a CERT. When such report is made public (usually after a patch has been created), then there will be a suddenly jump in the number of registered vulnerable nodes. Essentially, that number is the market share of the device or product with respect to that vulnerability. If the affected device is rare, then only a few new vulnerable nodes are added to the lists. However, if the product is widespread, such as in Apache webservers, or Linux machines, then the number of recognised vulnerable nodes increases significantly. An unethical hacker, in comparison, who perhaps has a greater budget and no morals about penetrating sensitive systems to search for exploits, will not publish a vulnerability and this contributes to our uncertainty of how many vulnerable nodes ultimately exist.

It should be noted, however, that even vulnerabilities with a low market footprint can be compromised, and these may affect particularly critical locations, companies, or systems. The concept of vulnerable nodes and market share concerns proportionality and effort for proactive remediation. It should not be confused with criticality which is determined by impact and effect. Products with a small share of the market can still have significant impact if compromised or hacked. For example, a product sold to Wembley Stadium has a small market share, but compromising Wembley in a significant way still has a heavy cost.

Growth of compromised nodes

Creating a complete list of compromised nodes at any one time is subject to the same obstacles as those for vulnerable nodes.

The main driver of volatility in compromised node registers is the publication of new research on types of botnet or infection. These publications suddenly add methods of identifying compromised nodes to the community, thus numbers can increase suddenly by millions of machines. As an example, the Conficker infection once controlled between 3-4 million machines. Actions were taken over a number of years by private security companies and law enforcement collaborations and it was eventually crippled and shut down by a variety of technical and legal methods, indicating how the numbers of known compromised nodes can rise and fall by several million in a single turn of events.

Criticality

One of the main challenges for both a cyber attacker and defender is judging which assets are the most critical. This section aims to define what we mean by criticality in national infrastructures. In particular, we identify several types of criticality, and apply these types to identify potential targets and unexpected effects within insured facilities.

[39] CyberGreen, 'Green Index'; https://stats.cybergreen.net/global; (accessed 21 April, 2016).

Critical dependencies often exist outside a region of influence

There is a tendency to imagine vulnerabilities in any organisation or system as being limited to the geographical location of that system. When considering vulnerabilities in infrastructure systems, however, there are many counter examples to this assumption. For example, Ireland depends heavily on natural gas from the UK. The gas pipes that cross the Irish Sea have are controlled by pumps in the UK, which Ireland is then dependent on. In the event of a black start scenario where the National Grid is compromised and a cascading blackout occurs, the UK will depend on French infrastructural support to help restart the Grid. Luxembourg has no electrical generation capacity of its own at all, importing all electricity from other countries.

The same is true of highly interconnected digital systems, therefore, the range of exposure for a particular network cannot be adequately measured in topographical terms.

Criticality varies by time

Some critical dependencies are temporal, and do not remain constant over time. For example, a stadium is hypothetically a high value target for cyber terrorism during an event, but not when it is empty. That said, an attack can be prepared before an event and automated to occur at a particular time. Temporality, therefore, works for attackers and defenders both.

On a distributed system such as the internet, it is important to recognise that many protocols depend on machines in other places. Plane tickets are emailed from a machine that isn't at Heathrow; a credit card is verified in cities far away from any purchases made using it; a petrol pump may depend on security updates from servers in China.

In a world where the appearance of destructive cyber terrorism is of major concern, the role of temporality needs to be considered at a much finer timescale. On the internet, microseconds can matter. Do we have a sense of embedded devices that are temporarily critical to our safety, security, and wellbeing?

Should it expand its coverage to include losses from cyber terrorist activity, Pool Re may be compelled to examine its portfolio to see if there are facilities whose insurance may be more or less time-sensitive, as this may provide ways of reducing cyber risk in its exposed categories. Innovative methods of policy writing might allow risk to be time-segmented instead of geographically defined.

Criticality by numbers (non-linear effects)

Criticality of individual nodes of a graph is often defined by centrality. However, when it comes to cyber, one of the key features is the ability to compromise or disrupt systems in large numbers. As previously seen, the ability to infect millions of machines is commonplace within cyber crime cases. Consequently, we have to consider another element of critical failures, which is the non-linearity of effects when multiple nodes are compromised and manipulated or disrupted together. For example: a single petrol station in the UK could never be considered critical national infrastructure. However, if an attacker could develop the ability to disrupt 10-25% of the petrol stations around a certain container port, this could have a significant impact on shipping.

When insuring against cyber terrorism, firms ought to bear smaller systems -- which may not be individually critical but might be critical collectively -- in mind. Also consider that such smaller systems are often extremely vulnerable; because one system is rarely seem as critical, there is little justification for rigorous security testing. Indeed, per the example mentioned above, petrol stations have vulnerable systems that can be found in large numbers on the internet.[40]

It may be prudent to write exclusions protecting against such interpretations of multiple parallel hacks as one event or 'occurrence', particularly because cleaning up a large cyber incident affecting so many might be costly. However, it is also a complicated exclusion that would have to explain some threshold of 'number of systems' exploited in a cyber terrorism policy.

The 'dark economy' of cyber

A final key consideration in understanding the UK's breadth of vulnerability to cyber terrorism is that there is a thriving underground economy for malicious hacking. This is a key driver for the development of cyber terrorist capabilities. Terrorists already acquire explosives or physical weapons through similar black-market means. The relative scarcity of explosives or military weaponry on the UK Mainland means that such products can be tracked or monitored to thwart terrorist plots.

In comparison, the cyber economy is far more difficult to monitor. The items needed to pull off potentially catastrophic cyber attacks are literally copied from other hackers or research. There is very little scarcity of resource, intelligence may be transferred

[40] K. Wilhoit, S. Hilt. 'The GasPot Experiment: Unexamined Perils in Using Gas-Tank-Monitoring Systems,' *Trend Micro*, 6 August 2015.

via encrypted communications, and the individuals involved in the trade of dangerous vulnerabilities or zero-days are unlikely to be flagged by current counterterrorism profilers, checking for traditional signs of terrorist activity.

The tools of cyber crime are also the tools of cyber terrorism. Consequently, a would-be-cyber terrorist might purchase diverse services and capabilities from the underground and dark web, without participants in transfers being alerted that they are about to be involved in the supply chain of a terrorist act.

Terrorist groups, however, may fear using such underground markets due to a risk of exposure to intelligence-gathering activities and informants who monitor the dark web and can disrupt nefarious operations. There are therefore some aspects of cyberspace that work in favour of counterterrorist efforts, and embracing and exploiting these is an important part of the combat against the growing threat.

Summary

The landscape of cyber space is diverse and complicated. Even measuring the field in broad strokes leads to considerable volatility in the numbers. The internet as it exists today is significantly different that the one that may exist tomorrow, in terms of number of systems deployed, ‘safe’, vulnerable, or compromised. The number of threat actors and their growth or decline is not known, and the number of tools (vulnerabilities, exploits, and black markets) at their disposal are difficult and time consuming to track and research. We have provided a snapshot, and some sources for metrics to reduce the uncertainty, but the risk landscape is still being mapped. This analysis should serve to inform discussion of what risks are associated with providing insurance against cyber terrorism activity, but also demonstrates that there are paths to reducing uncertainty, measuring, mapping, and providing future cover against cyber terrorism.

7 Insuring Cyber Terrorism

There is an inherent risk for insurers in introducing cyber terrorism coverage, even given the unlikelihood of terrorist groups developing sufficient, sophisticated attack means in the next three years . New methods for measuring cyber risk are continually adjusted, applied, and evaluated for usefulness. As this process matures over time, the field of cyber terrorism insurance will become more manageable.

There are a variety of computer security services that can determine how vulnerable a company or system may be to cyber compromise. They range from full red-team services, to penetration tests, vulnerability assessments and beyond. Services are typically more intensive in terms of manpower and financing needed and time taken than other risk testing and analysis practices. These may, however, be an appropriate way to approach cyber terrorism insurance to judge susceptibility and devise system profiles which will flag insecure or risk-enhancing elements.

For example, a small team of consultants working directly with an insurer could continually assess the security of its clients. That can be done either internally, through penetration tests or audits, or non-intrusively, using external means such as Shodan searches - which provide details on internet connected devices - and external network metrics evaluations. Insurers could require potential clients seeking coverage for cyber loss to carry out penetration testing and share the results annually. Care must be taken in the latter case that insureds maintain high assessment standards.

The insurance industry could also drive vulnerability reductions in other ways, for example by evaluating products routinely found in their insureds. A handful of systems each year, found and used by many of the insureds, could be subjected to close evaluation. The discovery and identification of vulnerabilities could ultimately lead to a reduction in exploits in insureds' systems.

These suggestions are primarily technical but there may be procedural or policy based alternatives to explore as well. For example, offering time-limited products for large sporting events, conventions, concerts, or gatherings may lead to better knowledge about how to time segregate cyber risk, which could be more useful than geographic segregation. It is also a non-trivial market; years of effort were put into safeguarding the 2012 Olympic Games from serious cyber attack.

Understanding the peril

For any underwriter, understanding the risk to be written is a crucial aspect of the process of accepting and pricing the risk. Clearly this is difficult when the risk is of an emerging nature and there is little or no historical data to form the basis of evaluating the risk. For cyber risks, terrorism included, the process of understanding the risk is further complicated by the dynamic nature of the connected world in which we live and the significant changes in vulnerability this may bring. Risk modelling toolkits can only be calibrated once the risk landscape is fully understood and this is something CCRS and Pool Re will be working upon in 2018 and beyond.

Peril manifestation

For natural perils, the question of what does an event look like is more easily understood. Storms produce wind and rain, floods involve inundation of land and earthquakes see the ground shaking. Hitherto there has been no real evidence of catastrophic cyber events perpetrated by terrorists and so it is more difficult to assess what an event might involve. Furthermore there are a number of potentially complicating factors that complicate any assessment of what a cyber event may look like.

Firstly, the lack of sufficient historical data or loss experience. Secondly, terrorism is a threat designed by humans to cause damage or harm, so unlike natural perils it is more likely the manifestation of the perils will change and adapt over time. This makes predicting future frequency and severity very difficult. Next, 'weapons of mass destruction' designed by nation states for use against their enemies are kept secure and are almost impossible for terrorists to procure. This may not be the case with equivalent cyber weapons or techniques, some of which seem to find their way onto the dark web. Given underwriters do not routinely offer cover for war, this adds significant complications to an assessment of disaster scenarios, as indeed does the involvement of state actors in cyber warfare and the connections with organisations purporting to be terrorists. Finally, there are questions around the ability of traditional risk prevention methods to deter and prevent cyber attacks, which are magnified by the gap between physical security and cyber security where, too many businesses are effectively leaving their factory door open for cyber criminals or terrorists to walk through.

This study will form the foundation stone of Pool Re's risk understanding and our modelling toolkit.

'Occurrence' issues

One important area for clarification with regard to cyber is the idea of occurrence. The occurrence of terrorism is reasonably clear, although cases do exist where simultaneous incidences may or may not be considered as single attacks. However, cyber incidents at the machine or user level can easily number in the thousands and millions. It is not uncommon for 50-100 different organisations to be involved in a single DDoS attack, or millions of machines to be impacted by a botnet. Even in the extreme scenarios proposed in this report, it would be reasonable to expect such an event involves 50-200 machines in various state of compromise. In order for an attack to successful, those compromised machines might exist in multiple organisations.

If expanding to provide cover for cyber terrorism losses, the insurance industry ought to be exacting with terminology to clarify the meaning of the word 'occurrence' in order to protect themselves from having each machine compromised – or each business impacted – in a single act of cyber terrorism being considered its own separate occurrence. A single cyber terrorist attack may also have multiple phases, and some thought and clarification around the meaning of 'occurrences' in the phase of a multi-staged attack will be prudent for maintaining future market confidence.

An incentive to maintaining good security measures

Patching systems and keeping software up-to-date is a key part of maintaining good levels of basic cyber security and diminishing the overall number of known vulnerabilities in a system. The process is time consuming, however, and there may be legitimate reasons for not using a patch or delaying its application (for instance, a patch may break a piece of key functionality). Patched systems are also not invulnerable, only better and proactively protected.

It is imperative that re/insurers do not expand cyber terrorism coverage as a perverse incentive to abandoning basic cyber security measures. Indeed, cyber terrorism insurance should be carefully crafted to reward those companies which maintain rigorous and regular cyber security practices.

Non-physical cyber terrorist targets

It is possible that cyber terrorism insurance policies could be expanded to include non-physical damage, but verifying such claims would require evidence that a zero-day was used and reasonable security standards were met in other respects, such as well-patched systems. Applying such policies to systems or organisations declared part of the critical national infrastructure by CPNI would narrow the field of potential buyers, but limit the cover to those truly in need.

Security exclusions

There are several unifying themes among the proposed cyber terrorism scenarios featured in this report which can be studied. The most damaging scenarios target facilities (airports, chemical factories, refineries, etc.) where active safety measures are already employed. Aviation facilities require fuel, navigational information, and working controls, and factories require energy, sensors and actuators, also in working order. When it comes to describing exclusions in cyber terrorism coverage policies, it might be prudent for insurers to exclude or extend based on less tightly-defined technical elements, but still have a technical impact. For example, excluding companies that do not have a dedicated person or team applied to patching vulnerabilities rather than on some basis which concerns the state of the system itself.

This would also allow any selection process to be focussed on auditing personnel and processes instead of a narrow field of technical details. Excluding non-physical damage is also practical, as many other coverages exist for such events. Some companies currently offer coverage for physical damage to industrial processes resulting from cyber.

The core challenge facing insurers choosing to develop cyber terrorism cover, involves the clarifying of occurrence issues and the setting of exclusions. This should involve studying prior computer security incidents (even those which would not be considered economically devastating), so that a deeper understanding of the diversity of cyber damage and attack vectors is achieved. Policy design can then account for some of the scale and complexity that cyber incidents incorporate.

8 Key Findings

Scenarios of cyber terrorism

The likelihood of a cyber terrorism attack is determined partly by the attraction of a successful attack to the terrorist actor, measured by body count and associated social shock compared with the practicality of mounting such an attack. The ease by which method of attack can be scaled, i.e., repeated without needing bespoke attention is an attractive feature of cyber techniques for a putative terrorist group. Together, these considerations lead to identification of Chemical Reactor Target, Rail Infrastructure Target, Airplane Target and Ordnance Target as four of the more extreme scenarios with respect to both scale of physical damage and mortality rate. This report, however, highlights a broad range of potential scenarios that may be feasible, and which may contribute to small scale losses and deliberate public disruption in the near future.

Capability of terrorist threat groups

The ability to inflict severe physical damage by a cyber attack requires deep, domain-specific knowledge. Categorising that capability into the stages of Enabling, Disruptive and Destructive gives a lens through which to examine threat actors. Currently and in the foreseeable future, non-state terrorist organisations and nation state cyber teams are the most relevant to causing physical damage by a cyber attack. These organisations have the potential depth and longevity to learn in the Enabling space, graduate to Disruptive capability and aspire to Destructive impacts.

To date the last category requires a sophistication in information technology and associated computer science techniques that needs to be combined with engineering expertise in digital control of physical plant. Whether by altering the control algorithms of that plant or in spoofing sensor data streams to fool automated controllers into certain responses, a destructive outcome can be engineered. This suggests a bottleneck in that engineering domain expertise needs to be developed, potentially *in situ*, and connected over time to a cyber intrusion.

Our main conclusion is that the most relevant cyber terrorist actors currently appear to pose a low likelihood of inflicting severe physical damage at the level of the scenarios identified above at present. However, given the fluidity of the cyber domain and potential power of cyber weapons in the right hands, any changes to or advancements in the state of the threat are likely to occur quickly, and monitoring of the threat is highly recommended.

Cyber terrorism as an emergent threat

This conclusion must be mitigated in recognising that cyber terrorism is an emergent threat. The population of digital devices, which form the first line of vulnerability to a cyber attack, is growing rapidly. The complexity of the interaction of those devices with each other and with existing physical systems, from manufacturing and other industrial facilities to biological systems, the latter including human healthcare, likewise increases the potential means or vectors of destructive attacks. The same complexity also masks criticality of digital processes or devices, i.e., the extent to which compromising a relatively rare process or device leads to an exponentially larger effect on the whole system. In this context, issues such as the cost of business interruption insurance payouts, currently found to be a relatively low priority concern, and the ongoing progress in industry and commerce of cyber education, data and process standards, and IT capability in monitoring and responding to digital anomalies, are expected to become more visible and significant over time.

Therefore a qualifying conclusion is that the emergent nature of the digital economy, cyber tools, and the capabilities of our own adversaries require a repeated reassessment of cyber attack over time. A greater depth of understanding and threat assessment will be gained through continued collaboration between Pool Re and the Cambridge Centre for Risk Studies in the coming years.

9 References

Further reading

Hoffman, B. (2006), *Inside Terrorism*, Columbia University Press.

Nance, M., Sampson, C., (2017), *Hacking ISIS: How to Destroy the Cyber Jihad*, Skyhorse Publishing.

Weimann, G. (2015), *Terrorism in Cyberspace: The Next Generation*, Columbia University Press.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown Publishing Group.

Bibliography

Alkhouri, Laith and Alex Kassirer. 2016, 'Tech for Jihad: Dissecting Jihadists' Digital Toolbox.' *Flashpoint,* July 2016.

Alkhouri, Leith; Alex Kassirer and Allison Nixon, 2016. 'Hacking for ISIS: The Emergent Cyber Threat Landscape.' *Flashpoint,* April 2016.

Allan, Darren; 2016; 'Was attack on BBC website the biggest volley of DDoS fire ever seen?' *TechRadar*; 11 January 2016.

16 March 2017 declaration from United Cyber Caliphate as reported on the Twitter account of Amarnath Amarasingam, 16 March, 2017.

APF, 'Top Chinese university hacked by IS infiltrator: Reports.' *Channel NewsAsia,* 18 January 2016.

Barkly, 'Ransomware-as-a-Service is Booming: Here's What You Need to Know.' *Barkly,* March, 2017.

Belikovetsky, Sofia, Mark Yampolskiy, Jinghui Toh, Yuval Elovici; 2016; 'dr0wned – Cyber-Physical Attack with Additive Manufacturing.' Cornell University Library.

Bhutia, Jigmey, 'ISIS 'Cyber Caliphate hacks more than 54,000 Twitter accounts.' *International Business Times*; 9 November 2015.

Bronk, C. a.-R. (2013). 'Hack or attack? Shamoon and the evolution of cyber conflict,' *Shamoon and the Evolution of Cyber Conflict.*

Byman, Daniel; 2017. 'Can Lone Wolves be stopped?' *Brookings,* March 15, 2017.

Byres, Eric; 2013. 'Patching for SCADA and ICS Security: The Good, the Bad and the Ugly.' *Tofino Security*; 26 March, 2013.

Costin, A., Fancillon, A. 2012. 'Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices.' EURECOM; *Black Hat USA*.

CyberGreen, 'Green Index'; https://stats.cybergreen.net/global

GAO Report. (2007). GAO-07-1036 . Washington DC: Government Accountability Office.

Gov.uk, 2015, 'Chancellor sets out vision to protect Britain against cyber threat in GCHQ speech.' *Spending Review and Autumn Statement 2015.*

Gov.uk, 2015; National Risk Register of Civil Emergencies, 27 March 2015.

Group IB; 2017; 'Hacktivists unmasked.' *Group IB Blog*, 2 August, 2017.

Gunaratna, Rohan; 2002; *Inside Al Qaeda: Global Network of Terror*; Columbia University Press, New York.

Harris, Shane, 2014; *@War: The Rise of Cyber Warfare*; Headline Publishing Group.

Heavy, 2016, 'ISIS 'Cyber Caliphate Army' Announces Plans to Hack Google.' 26 January 2016.

Heißner, Stephan; Peter R. Neumann; John Holland-McCowan and Rajan Basra, 2017. 'Caliphate in Decline: An Estimate of Islamic State's Financial Fortunes' , *The International Centre for the Study of Radicalisation and Political Violence,* 2017.

Hoffmann, Bruce; 2006; *Inside Terrorism*; Columbia University Press.

Kaspersky Lab Global Research and Analysis Team, 'Energetic Bear – Crouching Yeti.'

Knapton, S.; 2008; 'Power station break-in sparks security review.' *The Telegraph*, 11 December 2008.

Kravets, D.; 2009, 'USA v Mario Azar.' *Wired*, March 18 2009.

Laquer, Walter; 1998; *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*; Johns Hopkins University Press; edited by Walter Reich.

Lee, Robert, Assante, Michael, and Conway, Tim. 2016. 'Analysis of the Cyber Attack on the Ukrainian Power Grid.' Electricity Information Sharing and Analysis Center, 18 March 2016.

Lewis, James A., 2012, 'Cybersecurity, Threats to Communications Networks, and Private-sector Responses.' Testimony to House Committee on Energy and Commerce, Subcommittee on Communications and Technology, February 8, 2012.

Lewis, James; 2012, 'Testimony to House Committee from Center for Strategic and International Studies.' 16 February 2012.

Liu, Eric, 'Al Qaeda Electronic: A Sleeping Dog.' Critical Threats Project of the American Enterprise Institute, December 2015.

Lloyd's, 2015; ***Business Blackout***; Report prepared by Cambridge Centre for Risk Studies.

Lomothe, Dan, 'US military social media accounts apparently hacked by Islamic State sympathisers.' *The Washington Post*, 22 January 2015.

Maras, M.-H; 2012; *Computer forensics: Cybercriminals, laws, and evidence*. Jones & Bartlett Learning.

McBride, Jessica, 'Team System DZ Pro ISIS Hacks: Kasich, Brookhaven Targets.' *Heavy*, 26 June, 2017.

Milhorn, H. T.; 2007; *Cybercrime: How to avoid becoming a victim*. Universal-Publishers.

Morgan, Steve. 2017, 'Ransomware Damage report 2017 Edition.' *Cyber Security Ventures,* 18 May, 2017.

Murphy, Lorraine, 'The Curious Case of the Jihadist Who Started Out as a Hacktivist.' *Vanity Fair*, December 15, 2015.

Naim, Bahrun, 'Hijrah: Jujur Dalam Niat (Migration: Sincerity in your Intentions).' *bahrunnaim.co*. 2015.

Nakashima, Ellen. 2016. 'Syrian hacker extradited to the United States from Germany.' *Washington Post,* 9 May, 2016.

National Safety Transport Board. (2002). NTSB/PAR-02/02 PB2002-916502. Washington DC: National Safety Transport Board.

Nazeer, Zubaidah, 'Terror financing cell busted in Medan.' *The Jakarta Post*. 23 June 2012.

Opall-Rome, Barbara. 2015. 'Israel Confirms It Was Cyber Attack Target.' *Defense News*, 24 June, 2015.

Paganini, Pierluigi. 2017. 'United Cyber Caliphate published a kill list of 8, 786 individuals in the US, UK.' *Security Affairs,* April 6, 2017.

Risk Management Solutions, Inc, and Cambridge Centre for Risk Studies, Managing Cyber Insurance Accumulation Risk, Cyber Accumulation Risk Management; 2015.

Scannell, Kara, 'CEO email scams cost business $2b as staff fall for trick to send cash overseas.' *The Financial Times*, 25 February 2016.

Sengupta, Kim. 2017. 'Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images.' *Independent,* February 7, 2017.

SITE, 2015. '#FranceUnderHacks': Islamic Cyber Army Announces France as Next Target of Hacking Campaign.' *SITE Intelligence Group,* 22 October 2015.

SITE, 2016. 'Caliphate Cyber Army Releases Video, Joins with AnonGhost to Form 'Ghost Caliphate.' *SITE Intelligence Group*, 8 January 2016.

SITE, 2016. 'IS Supporters Redistribute OPSEC Manuals following Government -Tech Firm Meeting.' *SITE*

Intelligence Group, 11 January 2016.

Slay, Jill and M. Miller. (2008). 'Lessons Learned from the Maroochy Water Breach'. In E. a. E Goetz, *Critical Infrastructure Protection* (pp. 73-82). Springer: IFIP.

Symantec, 'Dragonfly: Cyberespionage Attacks Against Energy Suppliers.' 7 July 2014. Symantec Security Response.

UK Home Office, 2017, Proscribed Terrorist Organisations; 3 May 2017.

US Department of State, 2017; Foreign Terrorist Organizations; Bureau of Counterterrorism.

Verton, Dan; 2002; 'Report: Al Qaeda a potential cyberthreat.' *CNN*, 8 January 2002.

Weimann, Gabriel; 2004; 'Cyberterrorism: How Real Is the Threat?' United States Institute of Peace Special Report.

Weimann, Gabriel; 2005. 'Cyberterrorism: The Sum of All Fears?', *Studies in Conflict & Terrorism*. 28:129-149, 2005.

Weimann, Gabriel; 2006; *Terror in the Internet: The New Arena, the New Challenges*; United States Institute of Peace Press, Washington D.C.

Wilhoit, Kyle, and Stephen Hilt. 'The GasPot Experiment: Unexamined Perils in Using Gas-Tank-Monitoring Systems.' *Trend Micro*, 6 August 2015.

Wilshusen, G. C. (2007). Testimony GAO-08-119T. Washington DC: Government Accountability Office.

Wolf, Ken. 2016. 'Evaluating the Physical Threat from UCC 'Kill Lists.' *Flashpoint,* October 28, 2016.

Wolf, Ken. 2017. 'Cyber Jihadists Dabble in DDoS: Assessing the Threat.' *Flashpoint,* July 13, 2017.

Zetter, K. (2015), 'A cyberattack has caused confirmed physical damage for the second time ever.' *Wired*, 8 January 2015.

Appendix 1 UK Cyber Blackout Scenario

During 2015, the Cambridge Centre for Risk Studies designed and modelled a potential cyber blackout affecting industrial centres on the UK Mainland in the near future. The UK Critical Infrastructure Cyber Catastrophe Scenario describes a well-resourced and carefully developed attack on the electricity distribution network in the south and east of the UK and its impacts on UK Critical National Infrastructure (CNI). This analysis was published in April 2016 as the *Integrated Infrastructure: Cyber Resiliency in Society* report in collaboration with Lockheed Martin UK.

This is a regional power supply catastrophe that affects between 9 million and 13 million electricity customers across three variants of the scenario. The knock-on effects of the outage include disruption to transportation, digital communications, and water services for a further 8 to 13 million people.

In the hypothetical scenario, a rogue nation-state operating in partnership with a disgruntled insider are able to plant a number of rogue hardware devices undetected throughout the South East electricity substation network. Using mobile phone technology, the attackers are able to send instructions to the installed hardware and seize control of the power distribution system supplying the region. A series of rolling blackouts begins, causing chaos in the impacted region and along vital supply lines. The scenario envisions attackers focusing their efforts on achieving a series of blackouts across one distribution region, with small extension of the region to include the substations that serve Heathrow airport in the most extreme (X1) scenario variant. This includes the high profile economic regions of London and the South East of England, and the key critical infrastructure components of the City of London financial district, Heathrow (X1 only), Gatwick, Stansted and City airports, and Dover, Felixstowe and London seaports.

Scenario variants and rectification timescales range from rapid response (3 weeks until full power restoration), average response (6 week restoration) and slow response in the most extreme scenario (12 week restoration).

While the UK cyber blackout scenario is described as an act of cyber war from an unknown enemy, it could be viewed as an act of cyber terrorism. It is summarised here in order to provide a closer examination of the impacts of a cyber terrorism catastrophe.

Economic impact

The direct economic losses to sectors modelled in the scenario were estimated in the range of £7.2 billion to £53.6 billion in the different variants of the scenario. The overall GDP impact of the attack (GDP@Risk) amounts to a loss of between £49 billion to £442 billion across the entire UK economy in the five years following the outage, when compared against baseline estimates for economic growth. Both direct and indirect individual sectorial losses are described in Table 3 on the following page.

Table 2: Summary of UK cyber blackout scenario variants

Scenario Variant	*Description of Scenario*	*Number of Substations compromised with rogue hardware*	*Length of Cyber Attack Campaign (weeks)*	*Effective total Length of power outage (weeks)*	*Time to identify first rogue device in one substation (weeks)*	*Period for reverse engineering and planning the clean up (weeks)*	*Clean up and power recovery period (weeks)*	*DNO Region(s)*	*Physical Damage*
S1	Optimistic / Rapid response	65	3	1.5	1	1	1	1 region	No
S2	Conservative / Average response	95	6	3	1	2	3	1 region	No
X1	Extreme / Average response + physical transformer damage + 2 rogue devices + 2 regions	125	12	6	2	4	6	2 regions	Yes

Table 3: Direct and indirect sector losses (£millions) from UK cyber blackout scenario

	S1		S2		X1	
	Direct	Indirect	Direct	Indirect	Direct	Indirect
Mining	2	9	6	23	21	68
Agriculture, Forestry and Fishing	28	37	75	94	318	294
Defence Manufacturing	22	55	57	139	186	412
Electricity	17	64	44	160	133	467
Energy (Oil and Gas)	12	74	30	184	80	529
Water Supply and Waste Management	62	54	160	135	529	402
Arts, Entertainment and Recreation	120	64	300	159	901	457
Food	63	135	162	341	589	1,079
Communications	82	139	205	345	578	983
Accommodation and Food Service Activities	205	135	511	338	1,473	1,006
Other Services Activities	361	42	900	104	2,550	296
Government And Emergency Services	318	206	797	515	2,407	1,511
Information Technologies	440	96	1,085	239	2,776	672
Education	441	114	1,113	286	3,451	859
Transportation	304	252	762	628	2,317	1,822
Administrative Services	362	211	902	524	2,613	1,489
Health	402	255	1,013	638	3,101	1,900
Manufacturing	354	379	922	953	3,442	2,922
Construction	428	406	1,088	1,020	3,574	3,123
Professional Services	700	335	1,736	834	4,857	2,369
Real Estate Activities	820	388	2,063	956	6,295	2,601
Wholesale and Retail trade	770	505	1,950	1,263	6,126	3,710
Financial Services	897	419	2,175	1,039	5,325	2,870

Black Start procedures in the UK

In the remote possibility of a significant loss of power resulting from an act of cyber terrorism or cyber war, the National Grid may be forced to pursue a Black Start operation in order to recover the national transmission system. The process involves particular facilities installed with auxiliary generators which are able to provide energisation for up to three to seven days for sections of the transmission system.

The number of Black Start facilities and their capabilities must be carefully maintained. This process is costly and must be continuously justified in a world where electricity infrastructure seems resilient – a significant UK blackout has not occurred in the last decade. Such demands for justification pressure reliability organisations to reduce the number of Black Start facility commercial contracts, which diminishes the resources available in the event of a catastrophe.

It is unknown exactly how long a Black Start process in the UK would take. Though the National Grid conducts its own tests on facility capability, the results of these are not published and individual facility resources are not public knowledge. The 2015 National Risk Register for Civil Emergencies considered Black Start capabilities critical to the maintenance of a robust national infrastructure, and acknowledged that a recovery procedure could take up to five days.[41]

It should be noted that Black Start capabilities could be badly impacted by cyber terrorist activity and that the process could be sabotaged in the roll-out of a wider attack on UK critical infrastructure. Due to the confidential nature of Black Start contracts and internal reporting means, it is difficult to estimate vulnerabilities in the system and gauge their level of cyber security.

With respect to the provision of cyber terrorism insurance, Black Start capabilities are critical enough to the maintenance of national infrastructures and economic continuity that they will require coverage from cyber threats as the peril develops, assuming the risk can be quantified and limited to restoration costs, and would not incur liability for failure to supply.

[41] Gov.uk, 2015; National Risk Register of Civil Emergencies, 27 March 2015.

Appendix 2 Major ICS cyber events to 2017

Table 4: Catalogue of major ICS cyber events from 1999 through 2017 with primary consequence or harm (Rid, 2013)

Date	Event Name	Detailed Description	Actors	Motivation	Methodology	Outcome
April 1999 (Milhorn, 2007)	**Gazprom – Russian gas supplier**	A Trojan was delivered to a company insider who opened it deliberately. The control system was under direct control of the attackers for a number of hours.	Targeted Attack & Insider	Sabotage & Ransom	Trojan & Insider	Unauthorised Access
July 1999 (National Safety Transport Board, 2002) (Wilshusen, 2007)	**Bellingham**	Over 250,000 gallons of gasoline leaked into nearby creeks and caught fire. Large amount of property damage, three deaths and eight others injured. During the incident the control system was unresponsive and records/logs were missing from devices.	Accident	Unknown	Accidental	Physical Damage and Bodily Injury
Feb and April 2000 (Jill Slay, 2008) (Wilshusen, 2007)	**Maroochyshire**	A recently fired civic employee sabotaged radio communications and released 800,000 gallons of raw sewage into parks, rivers and the grounds of a hotel.	Insider Attack	Sabotage	Radio man-in-the-middle	Physical Damage
May 2001, (HEARING, JOINT, COMMITTEE ON ECONOMIC, and COMMITTEE ON EMERGENCY, 2005)	**California**	A hacking incident at CASO lasted two weeks, but did not cause any damage	External Attack	Unknown and contained	Deliberate	Thwarted
August 2005 (GAO Report, 2007)	**Daimler-Chrysler**	Thirteen Daimler-Chrysler US auto manufacturing plants were taken offline for about an hour by an internet worm. This resulted in an estimated $14 million in downtime costs.	Unknown	Spyware Installation	Zotob Worm and MS05-039 Plug-n-Play	Infection

Date	Event Name	Detailed Description	Actors	Motivation	Methodology	Outcome
Jan 2008 (Knapton, 2008)	**Kingsnorth**	Attacker broke into the EON Kingsnorth power station which caused a 500MW turbine to make an emergency shutdown.	Targeted Threat Actor	Sabotage	Physical Penetration	Environmental Protest
Nov 2008 (KRAVETS, 2009)	**Pacific Energy**	A recently fired employee disarmed safety alarms on three offshore oil platforms.	Insider Attack	Disgruntled Employee	Disabling alarm systems	Revenge & Sabotage
June 2009 to 2010 (Zetter, 2014)	**Stuxnet**	Malicious code targeted ICS at an Iranian nuclear plant.	Virus, Unknown Presumed Nation State	Sabotage	Destroying centrifuges and thwarting uranium enrichment	Revenge & Sabotage
2010 to Aug 2014 (Symantec, 2014) (Kaspersky, 2014)	**Dragonfly/ Havex/ Energetic Bear campaign**	A campaign against defence, aviation, and energy companies	RAT, Espionage	Unknown	Malware infection and remote access	Malware clean-up
August 2012 (Bronk, 2013)	**Shamoon/Wiper**	A Saudi Arabian oil company, Saudi Aramco, has over 30,000 workstations knocked out	Unknown, presumed Hacking group, RAT	Mischief	Wiping 30000 machines of their data	Unknown
2013	**Bowman Avenue Dam**	Iranian hackers breached the control system of a small dam outside New York City but were not able to remotely control the sluice gate	Targeted Attack	Revenge/ Sabotage	Penetration of computer systems via cellular modem	Thwarted, significant political attention paid to advancing cyber teams by foreign nations
April 2013	**California Power Station**	Snipers fired at a California substation, knocking out 17 transformers.	Unknown	Unknown	Destruction of substation oil tanks	Unknown
December 2014 (Lee et al, 2014)	**German steel mill**	Experienced hackers used a spear-phishing campaign to gain access firstly to the corporate and then to the wider plant control network.	Unknown, presumed hacking group	Unknown	Compromised plant control network, causing system components to fail	Physical Damage
December 2015	**Ukrainian Blackout**	Three energy companies in the Ukraine were taken offline, causing an eight-hour blackout which affected 225,000. Malware was later found in the substations.	Presumed Nation State	Unknown	Infection of vulnerable power substations	Unknown

Date	Event Name	Detailed Description	Actors	Motivation	Methodology	Outcome
November 2016	**Fidelix BMS Attack**	A sustained DDoS attack against a vulnerable building management system (BMS) caused internal heating to shut down for 24 hours in two apartment buildings in eastern Finland during sub-zero temperatures	Unknown	Unknown	Sustained denial of service attacks caused system to restart every few minutes	Firewall installed
December 2016	**Ukrenergo Ukranian power outage**	A second attack on Ukraine's power distributor left Kiev and the surrounding area without power for several hours during the night of 17-18 December	Suspected APT	Unknown	Targeted CRASHOVERIDE malware attack	Unknown
May 2017	**WannaCry**	A virulent strain of ransomware affected 300,000 computers in 150 countries, demanding $300 to release files per affected computer. An activated kill-switch stopped the malware from spreading further.	Suspected North Korean APT, Lazarus Group	Unknown; the malware did not accrue sufficient funds to suggest financial gain.	ETERNALBLUE and DOUBLEPULSAR exploits as released by ShadowBrokers in April 2017	Killswitch activated
June-July 2017	**NotPetya**	A second attack utilising ShadowBrokers exploits affected 12,500 machines in 64 countries. The attack presented as a ransomware but functioned as a diskwiper Trojan.	Presumed Nation State	Unknown	ETERNALBLUE ShadowBrokers' exploit	Malware clean up and patch roll out

Cambridge Centre for Risk Studies
Cambridge Judge Business School
University of Cambridge
Trumpington Street
Cambridge
CB2 1AG

T: +44 (0) 1223 768386
F: +44 (0) 1223 339701
enquiries.risk@jbs.cam.ac.uk
www.jbs.cam.ac.uk/risk

Join our LinkedIn group at Cambridge Centre for Risk Studies

Follow us @Risk_Cambridge