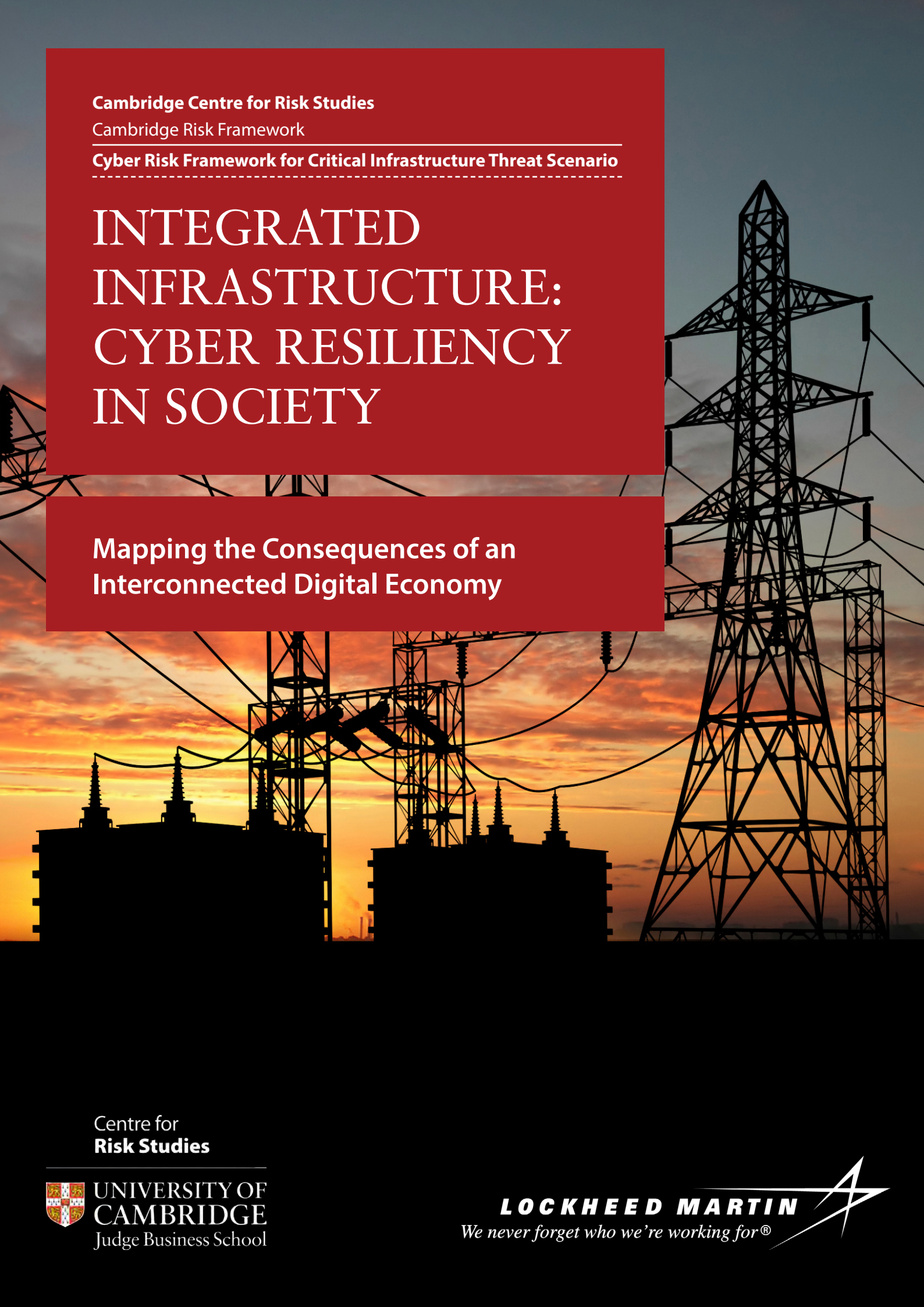

Cambridge Centre for Risk Studies

Cambridge Risk Framework

Cyber Risk Framework for Critical Infrastructure Threat Scenario

INTEGRATED INFRASTRUCTURE: CYBER RESILIENCY IN SOCIETY

Mapping the Consequences of an Interconnected Digital Economy

Centre for
Risk Studies

UNIVERSITY OF CAMBRIDGE
Judge Business School

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

January 2016

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

The Cambridge Centre for Risk Studies also acknowledges our external collaborators, the Infrastructure Transitions Research Consortium (ITRC):

Report citation:

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.

This report describes a hypothetical scenario developed as a stress test for risk management purposes. It does not constitute a prediction. The Cambridge Centre for Risk Studies develops hypothetical scenarios for use in improving business resilience to shocks. These are contingency scenarios used for 'what-if' studies and do not constitute forecasts of what is likely to happen.

Cambridge Risk Framework for Critical Infrastructure Threat Scenario

Integrated Infrastructure: Cyber Resiliency in Society

Mapping the Consequences of an Interconnected Digital Economy

Cambridge Risk Framework for Critical Infrastructure Threat Scenario

Integrated Infrastructure: Cyber Resiliency in Society

Mapping the Consequences of an Interconnected Digital Economy

1 Foreword

We are increasingly connected through, and reliant on, digital infrastructure to drive innovation, expedite efficiency and fuel better decisions. Yet the digital age has also accelerated the threat of cyber disruptions and increased the available attack surface of critical assets, networks and systems that sustain a nation's safety and prosperity.

Understanding the consequences to such critical infrastructure from a severe cyber hazard represents a shared responsibility among national and local entities, public and private owners and operators, and the IT hardware and service providers in their value chains. What's needed is an intelligence-driven defence, and this research endeavours to contribute to that knowledge-base.

The scenario and associated impacts detailed in this report suggest the network effect of two dimensions of cyber resiliency that are particularly relevant to containing disruptions to business and daily life.

The report also attempts to illustrate adverse outcomes of a severe cyber hazard in electrical distribution units not typically coordinated by security operations centres, and in ways that should prompt pioneering thinking from a broader set of stakeholders.

The scenario generated for this research focuses on infrastructure resiliency that requires a heightened level of security; a level which brings intelligence analysis of both physical and cyber assets to the forefront. With many pieces of rogue hardware in place and a faithful insider threat ring, multiple power substations can be simultaneously disabled using mobile devices and cut power to a significant number of electricity users.

The scenario illustrates why traditional security postures and protocols are insufficient to address the threat landscape we face today, characterised by advanced persistent threats (APTs), sometimes involving nation-state backing or coordination. Critical national infrastructure owners and operators will recognise the criticality of the depth of human and technical resources allocated to ICT system security, including identifying critical power distribution substations.

Next, the report affirms growing concerns over the impacts from a disruption in one infrastructure, in this instance a sizeable power outage, and the cascading effects due to interdependencies in other sectors. In this report, widespread impacts to air, rail and seaports can affect hundreds of thousands of passengers not directly affected at their own homes and offices. The shutting down of water facilities and sewage treatment plants due to power losses spikes unplanned government spending on daily water deliveries and sanitary system inspections, respectively. A system-of-systems analysis presents organisations with a clear strategy for addressing cyber threats head-on, as the risk modelling shows.

Certainly, hyper-connectivity is a powerful development tool and, in the case of energy infrastructure, presents an opportunity for governments, business, and individuals alike - a tool that enables a smarter, more efficient power grid. The challenge lies in our ability to balance and manage a complex set of cyber risks for the foreseeable future. How we measure progress, apply critical intelligence, train skilled analysts, share information and model infrastructure independencies will determine our cyber preparedness when it matters most.

- Andy Madge, *Managing Director, Security and Defence*, Lockheed Martin UK

LOCKHEED MARTIN

2 Executive Summary

Cyber attack on critical infrastructure

As digital connectivity becomes ever more integral to the global economy, companies and individuals become more exposed to vulnerabilities in the cyber system. Governments, in particular, are increasingly concerned about the threat to their economies posed by cyber attacks to individual entities and critical national infrastructure. The motivations and capabilities of cyber attackers are also changing over time with state sponsored cyber terrorism becoming more visible and threatening than the perils posed by lone hackers.

The UK economy relies heavily on digital activity. Correspondingly, around 30% of cyber attacks registered in the UK are in the financial services, with around 15% of attacks registered in each of the digital communications and energy sectors.[1] Cyber threats do not only cause chaos in the virtual realm but can affect physical systems as is analysed in the "Erebos" Business Blackout scenario stress test[2] which speculates on the effect of a cyber campaign which disables and damages a number of electricity generators in the north east of the USA.

The UK Critical Infrastructure Cyber Catastrophe Scenario

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 is a regional power supply catastrophe that affects between 9 million and 13 million electricity customers depending on the scenario variant. Its knock-on effects include disruption to transportation, digital communications, and water services for 8 to 13 million people.

The economic losses to sectors are in the range of £11.6 billion to £85.5 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.

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

On December 23, a power outage occurred in the historically significant Ivano-Frankivsk region of the Ukraine, where the blue-yellow flag was raised as a political expression of Ukrainian independence shortly before the fall of the Soviet Union. The power has since been restored but the cause of the outage is already under regional, national, and international investigation.

At the time of writing, little is known for certain about the cause of the outage but it has been verified that malware was found in a handful of substations. The Computer Emergency Response Team of the Ukraine (Cherepanov, 2015) CERT-UA confirmed the outage occurred and has identified the malware as mostly being related to threat actors associated with the BlackEnergy campaign (F-Secure, 2015). This would make the event the first known instance where a cyber attack has caused a blackout.

The investigation will continue in the coming days and weeks, and the sharing of the malware, tactics, techniques, and procedures, of the malicious actors within the OT and IT community is critical in matters of national security (Lee, 2016). There is significant political pressure to show the international community a condemnable incident and to attribute an attack to particular countries.

During the year spent formulating the following report, the Centre for Risk Studies posited the ultimate technical plausibility of a scenario which affected substation security on a regional level. The blackout in the Ukraine occured during the final stages of review and preparation for publication and may prove that an international malware attack of this type is indeed technically possible.

The likelihood of a cyber attack scenario on the scale of and with the sophistication, coordination and economic devastation as the one described in this report, however, remains improbable at the time of publication.

[1] Y. Chandiramani, "The FireEye Advanced Threat Report 2013: UK & Ireland Edition", 29 April 2014.

[2] Lloyd's and Cambridge Centre for Risk Studies. "Business Blackout: The Insurance Implications of a cyber attack on the US power grid." Emerging Risk Report 2015. May 2015

Behind the Scenario

Research

Private and public sector opinions in the UK were gathered via a set of structured interviews with representatives of the electricity industry, government and regulators.

A multi-disciplinary collaborative workshop defined key parameters of the cyber scenario, reviewed several potential narratives and developed key narrative elements for the selected scenario.

Scenario selection

National or regional electricity systems are typically comprised of three kinds of physical assets: generation capacity such as traditional coal or natural gas-fired generators, high voltage transmission lines for efficient transportation of power over long distances, and distribution networks which operate under lower voltage levels for general consumption. The process of stepping down power flows from higher voltages to lower voltages is achieved within a substation and with the use of a transformer. It is these substations which are the primary focus and targets of this scenario.

This scenario focusses on compromising the electricity distribution network in the south east of England. It is perpetrated as a geopolitical message by a hostile nation state with the help of a disgruntled employee acting within the distribution network service sector.

Variants of the scenario

Our 'standard' scenario, S1, is based on a three week campaign that disables up to 65 substations in the region serviced by one Distribution Network Operator (DNO). This is orchestrated as a series of rolling blackouts whereby the total lost power to all customers affected in the DNO region is equal to half the duration of the attack campaign. The S2 scenario anticipates an attack that is roughly twice as large in footprint and affects 95 substations, still in the footprint of a single DNO, resulting in a six week campaign. The most extreme X1 scenario allows for 125 substations to be compromised over 12 weeks and extends the footprint of the scenario slightly outside the DNO region to include the substations that serve Heathrow airport.

This is a stress test, not a prediction

This report is one of a series of stress test scenarios that have been developed by the Centre for Risk Studies to explore the management of situations of extreme shocks. It does not predict that a catastrophe will happen.

Impact Assessment Methodology

This research leverages a framework for classifying cyber threats and possible cyber catastrophe scenarios developed with input from subject matter experts, report collaborators, literature review and reportage from past real-life attacks on critical energy infrastructure.

The aggregate infrastructure and secondary economic impacts of the cyber attack draws upon an innovative three stage methodology developed as part of this research:

- **Disruption to UK Society**: Through risk and vulnerability modelling, using a system-of-systems model, we are able to assess how a cyber attack on electricity distribution substations could lead to failure in other critical infrastructure systems.
- **Impacts on Sectors of the UK Economy**: Through supply-side input-output modelling we are able to capture the economic interdependencies between sectors which feature the largest loss in economic output. This provides insight which can be used for supporting decision making in resilience planning, as limited resources can be targeted at those vulnerable sectors with the largest cascading effects. This can also help to bolster private and public investment into protecting interdependent critical infrastructure assets with the aim of avoiding catastrophic events.
- **Macroeconomic Impact on the UK Economy**: Through macroeconomic modelling, using our standardised GDP@Risk metric, we are able to quantify both the direct and indirect economic consequences resulting from systemic power-system failure revealing the overall long-term impact to the UK economy. Measuring different types of catastrophes using GDP@Risk enables the comparison of a wide range of natural, technological and financial catastrophes – a technique developed by the Centre for Risk Studies known as Catastronomics.

The developing scenario

Trojan Horses: Rogue hardware planted in electricity substations

A nation state plots to disrupt electricity supplies in London and surrounding areas. It spends months creating a "Trojan horse": a piece of rogue hardware that is not easily recognised as being alien to the operations of an electricity substation.

In order to implant the rogue hardware, the state seeks and finds a disgruntled employee of a subcontractor working with several DNOs. Over a six month period this malicious insider installs rogue devices in distribution substations.

A hardware attack on electricity distribution in south east UK

With many pieces of rogue hardware in place, the nation state can disable several substations at once to defeat the in-built redundancy of the distribution network and cause power cuts to large swathes of domestic and business users.

This is accomplished by using mobile phone technology to send instructions to the rogue hardware, thereby controlling a substation independently of the DNO's central control room. These rogue hardware devices are also equipped with malware that infects the substation's control systems and curtails electricity distribution even when the rogue hardware is switched off or, later, when it is discovered and removed, in order to keep it hidden.

Rolling blackouts

To maximise chaos and confusion, especially in the software and control engineering teams that will be responsible for finding and removing each piece of rogue hardware, groups of substations are identified in advance and switched off via the rogue hardware devices.

Once engineers are alerted to a problem at a substation that is not visible from the central control room, they will be able to 'reboot' the substation and power will return to the affected area within a few hours. However, these teams will not realise, until the power fails again, and then again, that they are experiencing a systematic attack.

Rolling blackouts plague the targeted region(s) for the length of the attack campaign: 3 weeks for S1, 6 weeks for S2 and 12 weeks for X1. To maximise impact the attackers execute the attack during the winter months when electricity demand is at the highest in the UK.

Cascading infrastructure failure in transportation, digital communications and public health systems

Electricity is a vital production input required to operate those transport and digital communications networks that support our economy. In addition, electricity is essential for maintaining the public health systems which we rely on.

Prolonged outages can be highly detrimental to our society, especially for the elderly and vulnerable, as homes without heating combined with a lack of fresh water supply and waste water treatment can lead to increased infectious disease and mortality.

End of the crisis

The intermittency of power failures, rolling across different sets of substations, will extend the crisis until the first Trojan horse is identified as malware.

At that point there is an energetic race by DNOs, with the help of the UK government, to find and eliminate all rogue devices and malware in substations.

UK Critical National Infrastructure impacts

9-13 million customers without power, transport, digital communications and water

In the S1 scenarios, 9 million customers are without power over a three week period. During blackout periods, transportation grinds to a halt, digital communications are intermittent, and water and waste water services are unavailable. In the X1 scenario the number of customers without electricity climbs to more than 13 million.

Over a million passenger journeys disrupted

At the peak of the attack more than 800,000 individual train journeys per day are disrupted in the S1 scenario, rising to over 1 million in S2 and X1; this has a strong negative effect on productivity as workers are physically unable to get to their place of work.

In the S1 scenario, over 150,000 airport passenger journeys are disrupted per day during the crisis. This figure doubles in X1 as Heathrow is completely shut down due to power failure, having international ramifications for air passengers around the world.

Disruption to 40%-55% of UK port freight

Felixstowe is the main container port in the UK and is severely affected by power outages. Disruption is widespread at Dover which is strategically important for supply chain distribution to and from Europe. This is felt by businesses and consumers across the UK as deliveries are unable to get to their destination. The threat, and in some cases actual, shortages of food and petrol cause further economic damage as well as social stress.

Economic losses

The UK economy suffers significantly on multiple fronts. Initially, the economic losses are caused directly by the impact of the power outage itself. Manufacturing plants are shut down, electric transport systems fail and retail outlets close unable to serve customers without light, power, or means of accepting payment.

Soon the effects of these initial impacts cause a chain of secondary consequences that cripple other parts of the economy that are not already affected and amplify the effects in areas that are already affected. These cascading impacts are propagated through disruptions in supply chains, people not able to get to work, and chaos in the financial system.

On the demand side, consumption drops and, on the supply side, distribution channels fail leaving shelves empty and people stranded.

The direct impact of the outage in the S1 scenario is estimated at £7.2 billion while the indirect impact is estimated at £4.4 billion. The sector most affected by the outage while it is occurring is Financial Services, which loses an estimated £1.3 billion during the period of the outage.

The secondary economic impacts remain for some time after the initial disaster as confidence continues to wane, perishable products are no longer fit for sale, businesses suffer, international relations are damaged and supply chains take considerable time to recover.

The longer term lingering economic impacts brought about by a collapse in consumption takes a further two years to recover to pre-disaster output levels in the S1 scenario and ultimately costs the UK economy £49 billion in lost GDP. Thus, a large proportion of the economic losses happen during the aftermath as businesses and consumers react to the catastrophe.

Risk management strategies

This scenario illustrates the threat posed by the particular security vulnerabilities of electricity substations, which tend to have a lower level of security than electricity control rooms. To mitigate the impact of this scenario this issue would need to be addressed by operators and policy makers.

Substations contain industrial control system equipment which is typically more vulnerable than mainstream IT equipment, and their network security lacks firewalls, segregation, network traffic monitoring and network access control applied specifically at the substation level. Substations tend to be remote and unsupervised and have less physical security allowing individuals unmonitored access. Some substations have CCTV facilities installed, but these can be disabled by a malicious actor.

There is a limited cyber security culture amongst vendors, supplier and contractors. Electrical engineers tend not to have cyber security awareness training and will be less likely to spot a cyber attack as a possible cause of a substation malfunction than a cyber security professional.

Substations tend not to have their individual network traffic routinely monitored making it harder to spot malicious command and data exfiltration.

The variants of this scenario explore different response capabilities exhibited by operators and authorities. The response characteristics include:

- The number of cyber security expertise of responders dealing with crisis in early stage of campaign.
- Degree of coordination with UK-CERT, GCHQ and CPNI.
- The length of time it takes for authorities to make skilled personnel available in sufficient numbers.
- The effectiveness of logistics for allowing large numbers of skilled personnel access to substations within access and safety regulations.

Conclusions

The report's findings emphasise the need for cooperation and transparent communication across various sectors, industries and practices in order to minimise losses from cyber attack and better safeguard society as a whole from a cyber threat to national security. Security planning conducted in silos cannot reconcile the systemic vulnerabilities of an interdependent national infrastructure.

It is vital that information (IT) and operational technology (OT) branches share information and threat assessments in order to diminish the number of exploitable vulnerabilities in critical infrastructures. OT systems in particular must reform traditional security procedures and build a culture of vigilance against possible cyber compromise.

Similarly, cooperation is required between government regulatory agencies and the private industry sector in recognising the true costs of an extreme cyber attack of this nature and formulating a mutually beneficial strategy to safeguard both the physical infrastructure itself and the wider economy from the threat. Recognition of existing and developing cyber threats is an important part of this process, as is acknowledging that the building of a more secure industrial network will be costly in terms of both money and time spent. The private sector must also address the issue of how return on investment is calculated for OT cyber security measures so that engagement with the threat of cyber attack may become mutually beneficial for both society and industry.

3 Cyber Risk and Critical Infrastructure Introduction

Cyber threat is a top risk for companies as businesses have increased the reliance on cyber space. The World Economic Forum's 2015 annual report on global risks ranked the threat of cyber attacks in the top ten for likelihood and "critical information infrastructure breakdown" among the top seven risks for severity of impact (WEF, 2015).[1] The WEF cites the growing number of physical systems that are connected to the internet, termed the "rise of hyperconnectivity" or interconnectivity, to be the main driver contributing to these high rankings.

In the 2010 UK National Security Strategy, cyber security was deemed a Tier 1 threat and governments are becoming increasingly concerned with those cyber attacks in particular which target critical national infrastructure. They have the potential to cause massive damage to essential systems leading to national chaos. Protecting against attacks on critical infrastructure systems has become "a key component of national security and cyber security strategies" (EPRS, 2015).[2] If a cyber attack caused a loss of power to key UK sectors, disrupted communication networks or caused a significant transportation delay, the impact on the economy could be tremendous. To help mitigate this threat and others, the UK government has set aside £860 million to fund a National Cyber Security Programme (UK Government, 2014) in order to tackle cyber crime, increase national resilience against attacks, and ensure the security of UK cyberspace.[3]

The risk profile of cyber attacks is unique due to the evolving threat landscape. As a greater numbers of companies adapt technologies and develop new systems that engage with the "hyperconnected" web, so too does the number of system vulnerabilities and potential attack vectors grow. In addition to the expanding landscape of vulnerabilities, the level of skill required of a potential cyber attacker to compromise these vulnerabilities has decreased over time as the availability and sophistication of tools has increased, see Figure 1. This has led to a rise in the risk of large scale attacks.

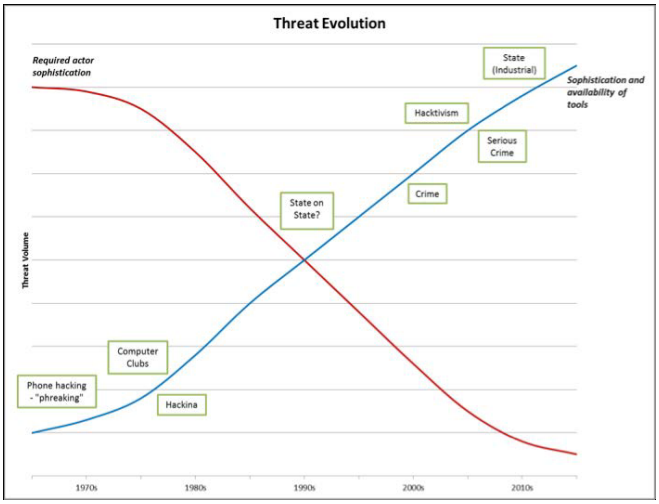

Figure 1: The cyber threat evolution (Source: CRO Forum)[4]

Cyber attacks on critical infrastructure

Numerous cyber attacks on critical infrastructure and, more specifically, on industrial control systems (ICS), have occurred around the world, as summarised in the event catalogue (see Appendix A: Recent ICS cyber incidents).[5]

ICS is a term that encompasses supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and programmable logic controllers (PLC). These systems are found in many industrial applications from industrial production to electricity distribution operators. Electricity distribution operators use some form of ICS to control, automate and maintain operation of their equipment and transmission of electricity to the grid.

A 2014 Ponemon survey of global IT security professionals showed that 57% of respondents believe that the threat to ICS and SCADA systems is increasing.[6] Before Stuxnet, the threat of ICS compromise was deemed extreme, unlikely, or only theoretical. Only in the past five years has the industry taken real steps to recognise and mitigate their cyber risks and begun to adapt the organisational structure of its technology teams though this process can take several years from start to finish.

Many in the industry believe falsely that ICS are "air-gapped" and thus immune to outside infection.

[1] World Economic Forum (WEF). "Global Risks 2015" 10th Edition.

[2] European Parliamentary Research Services (EPRS). "Cyber Diplomacy EU dialogue with third countries" June 2015.

[3] UK Government. "The UK Cyber Security Strategy – Statement on Progress." 11 December 2014. https://www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-progress-3-years-on [Accessed: Dec 2015]

[4] CRO Forum, Cyber resilience: The cyber risk challenge and the role of insurance; December 2014, p.3

[5] E. Leverett, Burning Rivers, Sewage in the Lobby and Giant Train Sets, Presentation at National Cyber Security Centre, January 23, 2013

Historical Case Study: Dragonfly

Perhaps the most alarming historical incidence of industrial systems attack is the compromise of ICS software vendors update mechanisms, causing them to become the infection mechanism for their customers. One important ongoing campaign used as a basis of this scenario is called Dragonfly, but also referred to as Energetic Bear and Havex.

This campaign was first detected in 2011 and may have been underway for a few years beforehand. Known infections have occurred in United States, Spain, France, Italy, Germany, Turkey, and Poland. With more than 300 known victims, it is very likely that attacks have occurred in other countries as well and that some infections have not yet been detected. The attackers had three different phases of infection tactics, beginning with spamming, progressing to watering hole attacks on legitimate websites, and finally using the HELLO exploit kit. While no known physical attacks have been perpetrated with this methodology, a significant amount of control system data was exfiltrated at many sites, probably for use in a future campaign.

This assumption ignores the fact that USB drives, CDs and file transfer methods used to directly access systems are a proven and effective vector of attack and that many industrial control systems are in fact connected to the internet. Although historically ICS for the operation of the UK electrical grid have been networked locally, many of these systems are now connected to the internet in order to save on costs and improve system reliability. For example, a distribution system comprising of transformers at substations is connected to a control room via a corporate IT network which, in turn, maintains a data connection to the internet. This is a major concern as ICS were not originally developed with network security in mind, potentially giving a hacker a back door into the control rooms and distribution systems.

Despite this and although cyber attacks on ICS and SCADA have been documented, only 55% of industry respondents to the 2014 Ponemon Critical Infrastructure Security survey have a dedicated employee responsible for the security of ICS systems; of these only 10% have more than one person on the security team responsible for ICS (Ponemon Institute, 2014).[6]

[6] Ponemon Institute. "Critical Infrastructure: Security Preparedness and Maturity." July 2014.

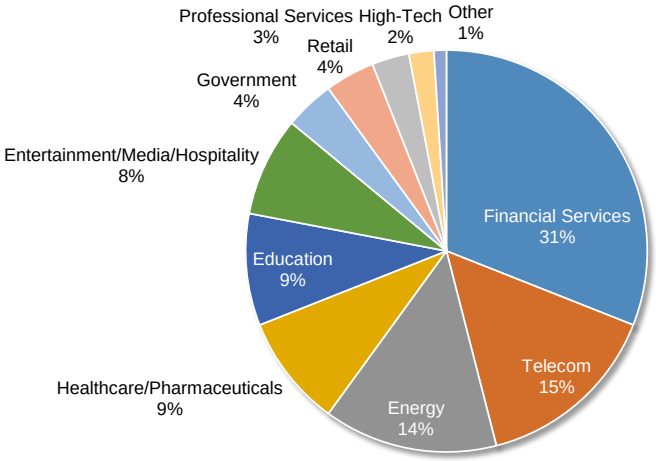

Figure 2: Registered UK cyber attacks by UK sector (Source: Chandiramani, 2014)

Infrastructure	Sub Sector
Energy	Electricity, Gas, Fuel
Communications	Telecommunications (including Digital communications), Postal Services, Broadcast
Transport	Aviation, Maritime, Land
Emergency Services	Ambulance, Fire & Rescue, Marine, Police
Financial Services	Payment, Clearing & Settlement Systems, Markets & Exchange, Public Finances
Food	Production, Processing, Import, Distribution, Retail
Government	Central government, Devolved administration/ functions, Regional and local government, Parliament
Health	Health & Social Care
Water Supply	Portable water supply, Waste water services, Dams

Table 1: Summary of the UK critical national infrastructure at the sector and subsector level (Cabinet Office 2010).*

* Cabinet Office. Strategic Framework and Policy Statement - on Improving the Resilience on Critical Infrastructure to Disruption from Natural Hazards. March 2010. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf [Accessed: March 2015]

UK Critical Infrastructure

The UK government defines critical national infrastructure (CNI) as: "those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends."[7] The definition of critical national infrastructure has evolved beyond a catchment of simply physical systems to include the digital systems as well.

There is growing concern over the impacts from an outage or disruption in one infrastructure and the cascading effects due to interdependencies in other sectors.

Energy and Communications are chief among these sectors as they have an "enabling function", meaning that their continuing function is necessary for the other sectors to operate.

In the 2015 National Risk Register of Civil Emergencies, the UK Cabinet Office classified a potential widespread electricity failure as having an impact of 4 (out of possible 5) despite having a likelihood between a 1-in-200 and 1-in-20 year event. If the UK did experience a significant power outage, it would take up to five days to recover, using the "Black Start" process which involves "starting generators from first principles".[8]

[7] CPNI website. "The national infrastructure." [Accessed: March 2015]

[8] Cabinet Office. "National Risk Register of Civil Emergencies." 2015 edition. March 2015.

4 The UK Electricity Grid

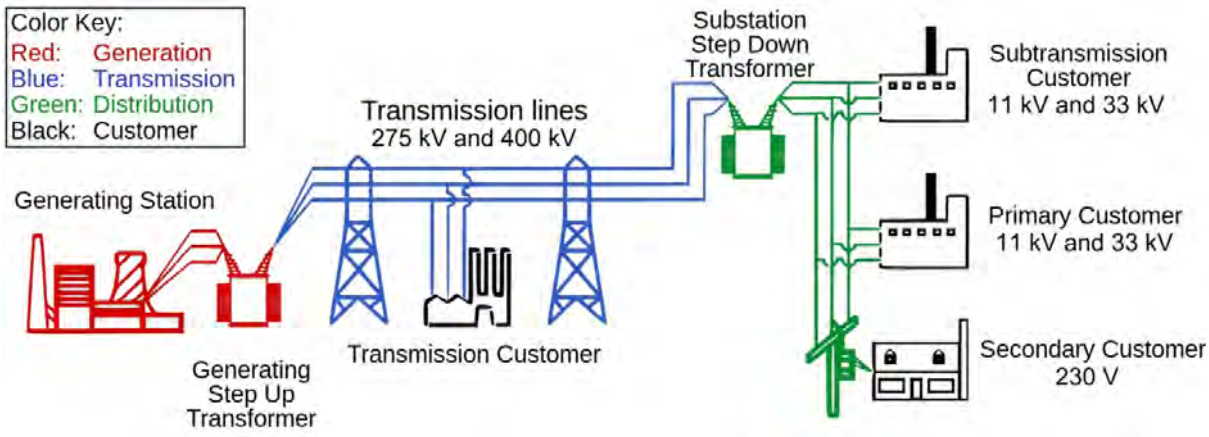

Figure 3: Overview of the UK generation, transmission, and distribution electricity grid

Generation, transmission and distribution

There are three components to the electricity grid in the UK: generation, transmission and distribution. Power plants generate electricity using different fuel sources such as coal, natural gas, nuclear, etc. as shown in Figure 4 while the transmission system delivers energy at high voltage up and down the country. The consumption of electricity varies by sector as shown in Figure 5. The efficiency of the system is managed by National Grid.

This report focuses on vulnerabilities within the UK distribution network, which represents a lower voltage synchronised system that delivers electricity to households, business places, and industrial plants.

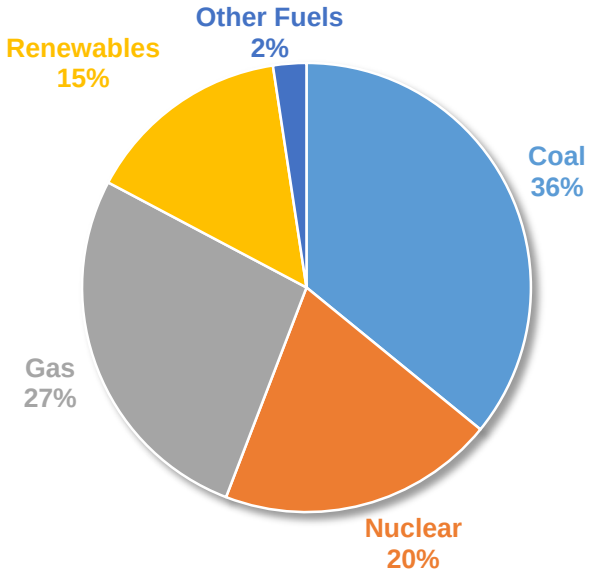

Figure 4: Breakdown of fuel sources used in the generation of UK electric power as of 2013 (Data source: DECC, 2014)

The synchronised operating frequency of the distribution system is 50 Hertz (Hz). National Grid is obliged to maintain the system frequency between 49.5Hz and 50.5Hz, although normal operating limits ranging from 49.8Hz to 50.2Hz also apply.[9]

Distribution Network Operators

The UK is divided into nine electricity regions where the distribution process is managed by distribution network operators (DNOs). There are only seven DNOs in the UK, see Figure 6. Each of these DNOs manages the cables, transformers, substations, communications networks, and control rooms for their respective regions. While each region has its own different assets, networks, and challenges, all perform their work focussing on reducing customer minutes lost, a metric OFGEM uses to measure quality of service to the UK population. This is discussed further later in this section. To perform these tasks, each DNO uses a control room to control the flow of electricity from National Grid substations to their own substations, and on to their individual customers.

A DNO can be responsible for several hundred substations, each of which has to be protected in both a physical and systemic sense. In fact, the two protection tasks are highly coupled and inter-related. If there is no lock on a substation or CCTV monitoring, it can be trivial to break in and interact with ICS components to create a malicious effect. Equally, if it is possible to remotely disable CCTV cameras with hacking, this can make it possible for someone to break into a substation to steal copper or perform acts of physical sabotage.

[9] "Electricity Transmission System Operations | National Grid." Accessed January 15, 2015.

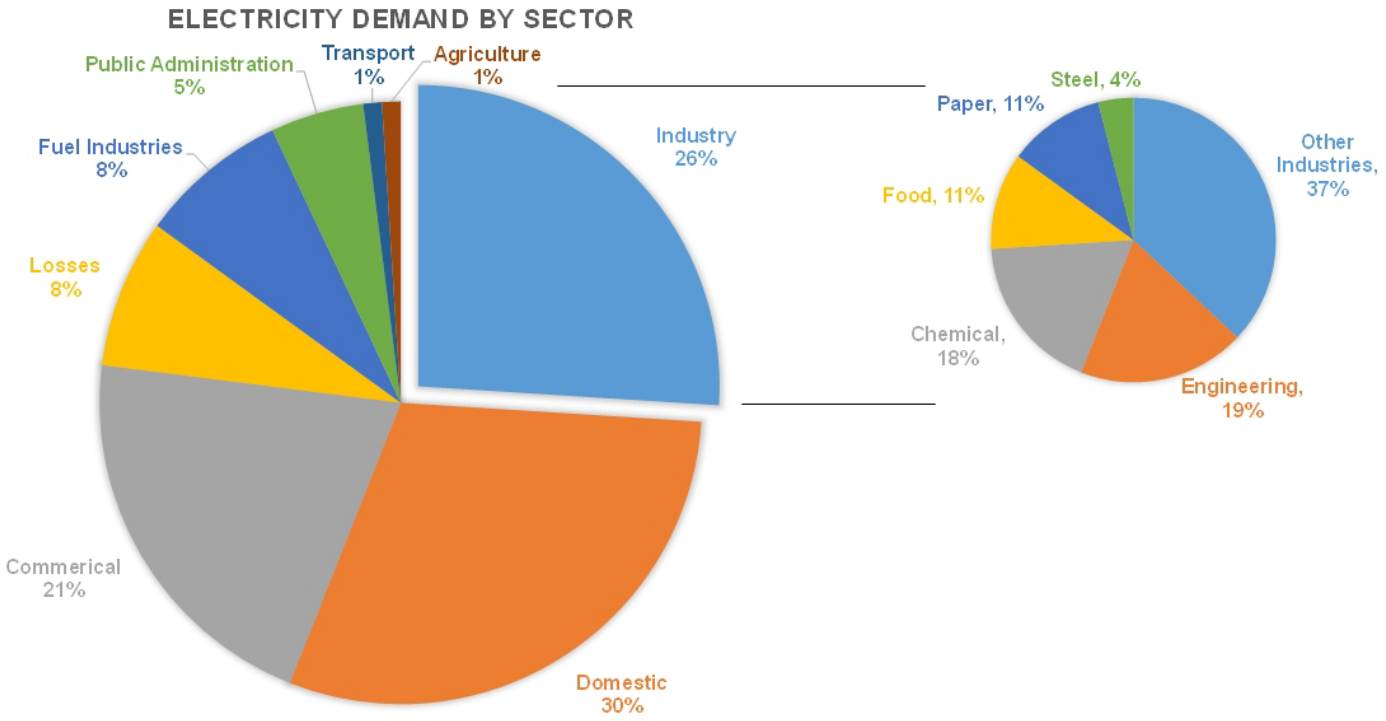

Figure 5: Breakdown of electricity usage by sector as of 2013 (Data Source: DECC, 2014)

This scenario is focussed on substation attacks. Compromising a large number of geographically distributed substations, each of which needs protecting in both a physical and a cyber capacity, and that have varying degrees of criticality to the distribution of electricity to consumers, is the focus of this scenario. The attacks described below offer lessons to both attackers and defenders but, more importantly, demonstrate many opportunities for innovative and well informed mitigation strategies. The unique element of this report is the loss estimation of both direct and indirect costs to the UK economy should such a fictional scenario occur.

Historical Outage Catalogue

The Office of Gas and Electricity Markets (Ofgem) is the economic regulator for the electricity and downstream natural gas markets in Great Britain. It has the key objective of protecting the interests of all current and future consumers. The long-term safety and reliability of the electricity distribution networks and their impact on customers are key priorities for Ofgem.

The average customer interruption in the UK is 7 events per 10 years, with an average of 1 hour and 10 minutes of lost supply per customer per year (Ofgem, 2012).[10] There were a total of 18.3 million customers interrupted and 102 customers per fault in 2010-11.[4]

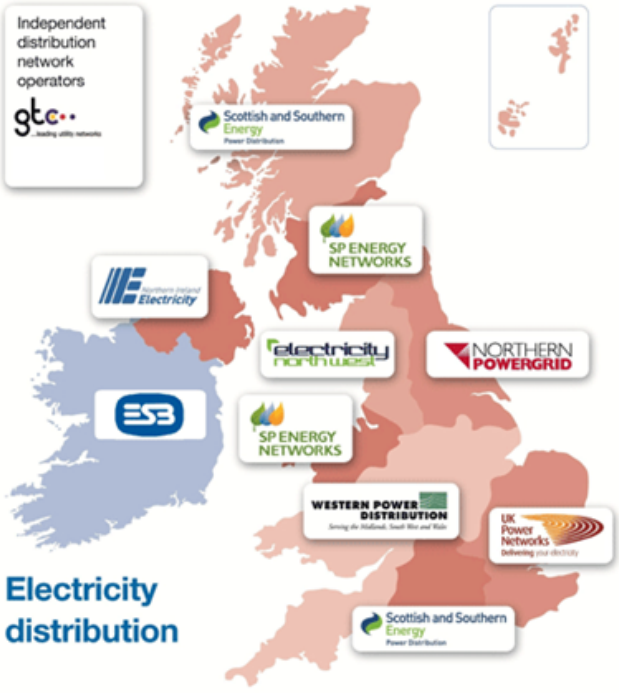

Figure 6: Overview of the DNOs in the UK (Source: National Grid. "Distribution Network Operator (DNO) Companies").

[10] Ofgem. "Electricity Distribution Annual Report for 2010-11". 20 march 2012

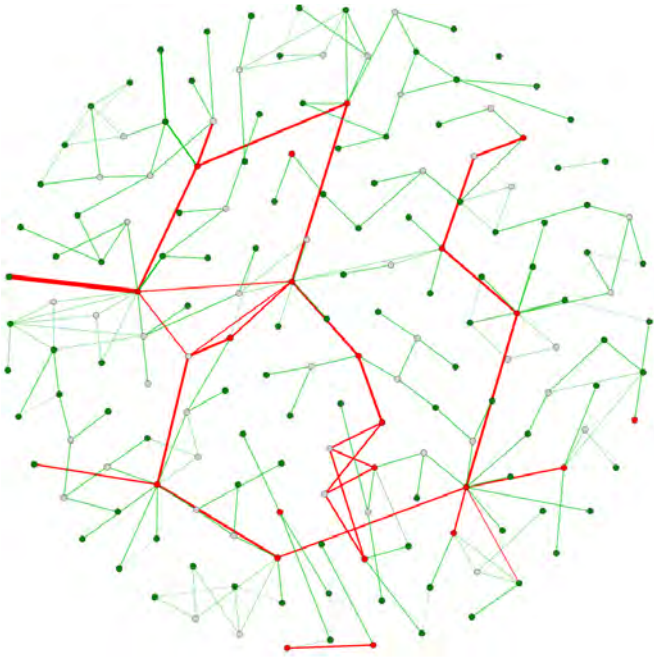

Figure 7: Simplified part of one typical UK DNO substation network showing how National Grid 400 kV and 275 kV transmission lines (red) connect to the DNO's 132 kV and 33 kV distribution lines (green). Nodes represent substations and line junctions. Network topology is 173 nodes, 219 edges, diameter of 15 and average degree of 2.5.

The Department of Energy and Climate Change (DECC) hosted a workshop in July 2014 to review the emergency response plan for a widespread and long-term electricity outage (DECC, 2014).[11]

"The event brought together a wide range of stakeholders from across Government and Industry, to explore the impacts and responses to a widespread and long-term electricity outage, based upon a scenario of the loss of power to South West England. Members from the Electricity Task Group worked extensively with the Exercise team to develop a credible and challenging incident scenario and were also present during the workshop itself both to provide expertise to the workshop and ensure that a realistic and robust discussion on interdependency issues took place."[12]

Since 2011, the UK has steadily been losing spare capacity in the winter months due to increased demand and decreased generation capacity (BBC, 2014).[13] During the 2015/16 winter season it is predicted that on the highest demand day (i.e., the coldest day) there will only be a 5.1% capacity margin,

[11] DECC. "Energy Emergencies Executive Committee Annual Report 2014", 15 December 2014.

[12] Ibid., 8

[13] *BBC*. "National Grid warns of lower winter power capacity". 28 October 2014.

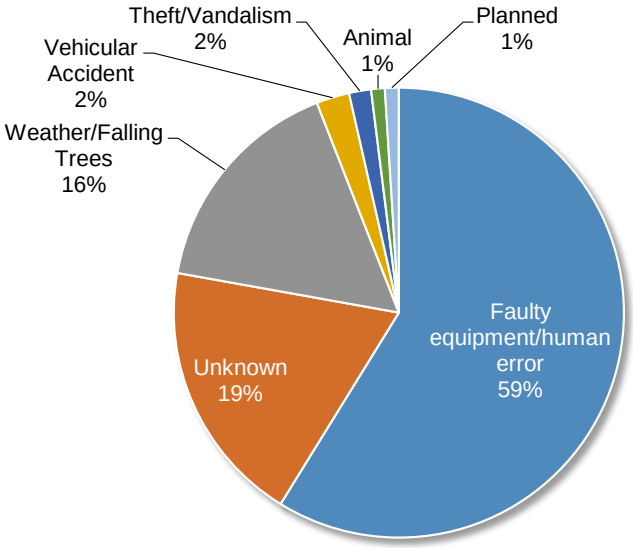

Figure 8: Summary of 2013 UK power outage causes (Eaton, 2013).

meaning that there is little room for error (Davies, 2015).[14] At present, Ofgem estimates that the highest demand period will occur during the week of 11 January 2016. This information has heavily informed the decision to set the attack during the winter at a time of peak demand and bad weather.

Although outages in the UK are less common there have been several notable outages in the past. The annual power outage report from Eaton suggests that the main causes of outage are equipment failure and human error, with weather coming in third (Eaton, 2013).[15] Some examples of real effects are discussed below to give some background evidence to the impacts of outages.

1987

- Wind storm caused the link between UK and France to go out resulting in the loss of power to most of South East of England for approximately 6 hours (Burt and Mansfield, 1988).[16]

2003

- Back to back transmission system faults caused a 34 minute power outage in parts of London. Disruptions were felt throughout the day due to delayed trains and increased road traffic (London Assembly, 2004).[17]

[14] Davies, Rob. "Will the lights go out in the UK this winter?" 12 Nov 2015 *The Guardian*

[15] Eaton, United Kingdom Annual Report 2013, "Blackout Tracker", 2013

[16] Burt, S. D. and D. A. Mansfield. "The great storm of 15-16 October 1987". *Weather* 43(3). Pages 90-110.

[17] London Assembly. "The power cut in London on 28 August 2003 – A report from the London Assembly's Public Services Committee." February 2004.

2009

- A power cut due to arson at a cable installation left 94,000 customers without power for four days (BBC, 2009).[18]

2010

- A blackout in Portsmouth was caused by a substation fire, leaving a maximum of 47,000 people without power (BBC, 2010).[19]

2013

- Two severe winter storms in December damaged parts of the distribution network affecting almost 1 million customers. Supply restoration took up to 48 hours. (Cabinet Office, 2015).[20]

2015

- An underground fire in Holborn cable tunnels caused a power outage. It took 36 hours to put out the blaze, badly disrupting business continuance in the area. (BBC, 2015).[21]

Ofgem monitors two quality-of-service metrics to measure a DNO's performance concerning outages: customer interruptions (CI) and customer minutes lost (CML).

- **Customer interruptions (CI)**

  The number of customers that experience supply interruptions lasting for three minutes or longer per 100 customers per year over all incidents, excluding re-interruptions to the supply of customers previously interrupted during the same incident.

- **Customer minutes lost (CML)**

  This is the average customer minutes lost per customer per year, where an interruption of supply to customer(s) lasts for three minutes or longer.

DNOs are encouraged to improve reliability of the network under the Interruptions Incentive scheme (IIS). The IIS is designed to encourage DNOs to manage the number and duration of supply interruptions. The IIS financially rewards or penalises DNOs depending on performance against targets for the number and duration of interruptions. It costs a DNO on average £5 per interruption per customer (Ofgem, Hope, 2012).[22]

The future of the grid

The electric grid is becoming ever more interconnected through the implementation of Smart Grid technology. Smart Grid improvements enable better monitoring, performance and reliability of the system using thousands of remote controlled measurement devices installed at various points in the grid. One example of the many and diverse Smart Grid projects are Smart Meters, which allow real-time information about demand to flow back to the DNOs and National Grid, who can use such data to do real time purchasing of supply or price incentives, instead of relying so heavily on predicting demand in advance.

Key to the Smart Grid development "is a modernised electricity grid that uses information and communications technology to monitor and actively control generation and demand in near real-time, which provides a more reliable and cost effective system for transporting electricity from generators to homes, businesses and industry" (DECC and Ofgem, 2014).[23] Some devices may embed a possible systemic vulnerability into the grid.

This is a best practice that potentially will reduce the cyber threat by improving the mitigating controls that can prevent or reduce the impact of cyber attacks (DECC, 2014).[24] The Energy Networks Association (ENA) developed a cyber security plan concerning the future Smart Grid to ensure that cyber security is continually addressed throughout the system. (Tritschler, M. and W. Mackay, 2011)[25]

[18] BBC. "Over 10,000 still without power. 22 July 2009.

[19] BBC. "Fire cuts power to thousands of Portsmouth homes." 26 June 2010.

[20] Cabinet Office. "National Risk Register of Civil Emergencies." 2015 edition. March 2015.

[21] BBC. "Holborn underground fire: Electrical fault caused 36-hour blaze." 9 April 2015.

[22] Ofgem. Hope. James. "Strategy consultation for the RIIO-ED1 electricity distribution price control." 28 September 2012.

[23] DECC and Ofgem. "Smart Grid Vision and Routemap". February 2014.

[24] DECC. "Energy Emergencies Executive Committee Annual Report 2014".

[25] Tritschler, M. and W. Mackay. "UK Smart Grid Cyber Security". 25 June 2011. London. Energy Networks Association.

This scenario describes a cyber attack that disrupts the distribution of electricity in the eastern part of the UK, including London. In the S1 variant, approximately nine million people are left without power for 1.5 weeks total during a period of rolling blackouts that lasts three weeks.

We carried out a set of stakeholder interviews where we interviewed representative organisations of the UK electricity industry, UK electricity industry regulators and UK government. We carried out a literature review on cyber-physical attacks against electrical grids and compiled a catalogue of major industrial control system cyber events. We studied the structure of the UK electricity industry and carried out a scoping review of UK power grid models.

This data gathering phase formed the basis for a scenario development workshop which was attended by representatives of the UK electricity industry, UK government, insurance industry, security specialists and subject matter experts. This workshop defined key parameters of the cyber scenario, reviewed several potential narratives and developed key narrative elements for the selected scenario, which is described below.

Attack on Electricity Distribution

The attack focuses on the UK distribution network as opposed to the generation and transmission facilities of the electrical grid.

The key element of a distribution network is the substation. Substations form the nodes of the network with underground cables forming the links (sometimes these cables are over ground, but most are buried for safety and resilience reasons). There is resilience in the network and large scale blackouts will only happen when several connected substations are simultaneously disabled.

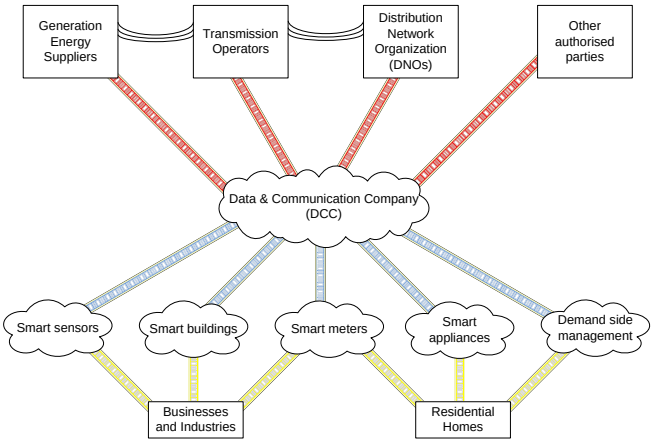

Figure 9: Current UK electricity grid data network, with developing SmartGrid system dimension (Source; adapted from DECC and Ofgem, 2014)[27]

[26] DECC and Ofgem. "Smart Grid Vision and Routemap". Smart Grid Forum. February 2014.

5 Defining the Scenario

Our 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 X1 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.

Elements from real-world events have been blended into the scenario, along with errors in human judgement relating to security architecture and attack detection. To extend the blackout to other parts of the UK, the attackers would have to replicate the same effort in the other eight distribution regions. If the objective of the attack were to disable the entire power supply of the UK, they would have to enact a much larger plan, involving greater access to resources, attackers' sophistication and coordination than is assumed here. Such an undertaking may be impossible, given the amount of coordination and secrecy required. In this scenario, however, we assume that the intent of the attacker is to demonstrate capability and to achieve a regional blackout rather than to leave the UK entirely in the dark.

This scenario represents one improbable - though not impossible - narrative. We consider who might have sufficient motivation and skills to carry out this attack below. However, regardless of access to resources or funding, it is important to highlight how difficult it is to carry out an attack that could achieve this objective and result in this level of disruption.

Overall logistical burden

Considerable skills and resources would be required to successfully execute a cyber attack to disrupt power distribution in the UK.

The 'logistical burden' to the attacker in implementing an attack of this type would be high. The attackers would need to research and understand the systems that they are attacking in great detail both from software and an electrical engineering perspective. They need to identify vulnerabilities they can exploit and they need those vulnerabilities to remain unfixed for long enough for them to design and implement a plan to exploit them.

Over time, vulnerabilities are addressed and remedied, so there is a limited window of opportunity. A successful plan is likely to require the identification of multiple vulnerabilities – for example, a way of disabling substations through software controls, as well as a vulnerability to enable malware to be inserted into the control systems. The attackers are likely to need a skilled team of operators to create these different code components, to coordinate, monitor and plan, and then to carry out the attack.

In our scenario, we envision that the perpetrators will need to compromise at least 65 (S2 95, X1 125) different substations, an endeavour which is likely to take time, patience and extensive resources. It will be critical for the attacker team to remain undetected during their preparation and the implementation of the attack, which means that they need to evade the active scrutiny of maintenance teams, supervisors, inspectors and law enforcement agencies, to ensure that any dealings with other parties are secure, and to route all their activities through untraceable channels. They will also want to remain undetected after the event to avoid retribution. This requires careful design of the malware and hardware which will be forensically examined afterwards, and the channels by which it is delivered. They may need to obtain some level of assurance that their plan will succeed before they invest in the resources required, and may embark on tests, possibly including practice penetrations of their target facilities. If security operators within the facilities detect these tests then the attackers may give themselves away, inviting law enforcement response, and the swift address and resolution of the vulnerabilities that they were planning on using.

Overall, the implementation of an operation that successfully disrupts the power supply in the UK would require a significant team of personnel, a high level of skill to create undetectable hardware and malware with the functionality required, and many months of careful research, preparation and operational implementation. If this resource requirement were monetised, the attack would require the perpetrators to invest multiple millions of dollars to achieve success.

Who might do such a thing?

In this scenario, we assume that the attack is never officially attributed to a specific perpetrator. One of the characteristics of cyber attacks is the difficulty of

attribution. However, the likelihood and realism of a scenario of an attack of this type depends ultimately on whether there are people with the motivation and capability to carry it out. The sophistication of the attack, and the logistical burden required, means that this type of attack is beyond the capability of amateurs, 'script-kiddies', or individual lone actors – it requires an organised team that is well resourced with appropriate infrastructure. The scenario describes a disgruntled insider working in conjunction with a well-funded, hostile nation state, a combination of particular concern to the UK power industry.

Disgruntled insiders

Insiders working within the particular industry are those commonly most informed of the system's operation and potential vulnerabilities. There are many examples of insider attacks in companies, institutions and government departments that come about as a result of job dissatisfaction or 'whistle-blowing' on wrong-doing. An employee of the power industry may wish to draw attention to vulnerabilities by mounting an attack for demonstrative purposes. Insiders could also be bribed to sell their domain knowledge to external teams of attackers or participate in an attack for ideological reasons. A single rogue employee would not have the resources to mount the scale of attack that we have specified in this scenario and could not achieve the level of disruption that leads to the losses we describe but could be an important resource to facilitate an attack by another group.

The UK power industry is particular concerned about security vulnerabilities arising from third-party vendors, as the vendors do not necessarily share equal standards of cyber security or culture of awareness of cyber threats. Improved third-party cyber security vendor management is needed to prevent scenarios such as the one described in this report.

State Sponsored Cyber Teams

More than 20 countries are now known to maintain or be developing national cyber teams, with at least six countries having capabilities that analysts consider as 'advanced'.[27] Most of the countries that maintain significant military capability now have cyber units. Several of these countries are potential adversaries of the United Kingdom, including Syria and Iran.

Foreign state-sponsored cyber teams from a number of countries are suspected of conducting espionage and information gathering by penetrating systems in the UK; their focus has to-date tended to be on military secrets and industrial intellectual property. 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 meaningful impacts against the target.

State-sponsored cyber teams have the capability and resources to mount an operation such as the scenario envisioned in this report. However, even adversaries have generally avoided any direct action that would provoke a response. Our scenario avoids having an attack that is recognised as a formal act of war. It is possible to imagine situations of either miscalculation by a potential sponsor state or a state using a proxy organisation to carry out a demonstration attack, perhaps as a warning or deterrent to UK foreign policy.

It would likely involve concealment or complex routes of attribution to avoid or complicate UK response. There are strong deterrents for nation states in executing a physical attack on the UK but hostile state-sponsored cyber teams are one of the few potential candidates with the resources to perpetrate a scenario of this type.

Access to Substations

The most complex part of an attack of this type is likely to be the introduction of the malware into the substations themselves. Distribution companies are fully aware of the possibility of cyber intrusion into their systems and have sophisticated security processes, personnel, and system architecture dedicated to preventing it. Usually, the substation systems are separated from the general communications systems of the outside world by a firewall; places where information needs to transfer between the regional control centre and the substations are heavily screened and policed. All systems have weaknesses with potential for a determined attacker to find ways through. A sophisticated attacker may be able to devise ways that could exploit vulnerabilities in the defences.

The technique in this scenario is to plant rogue physical hardware inside the substation, connected to the local area network (LAN) from which a tailored cyber attack can originate -- a 'Trojan horse'. The nation state develops the hardware and manufactures a large number of them (100+) and ships them to the disgruntled insider who then installs them in the substations. We imagine the insider is a contractor whose job is to regularly visit substations and has

[27] J. Lewis, (2012), "Cybersecurity, Threats to Communications Networks, and Private-sector Responses: Testimony to House Committee on Energy and Commerce, Subcommittee on Communications and Technology"; Centre for Strategic and International Studies.

access to important critical information, such as virtual LAN (VLAN) configurations, substation cyber defences, important cryptographic credentials, and network diagrams, and of course can physically access the substation premises under legitimate pretences.

Simultaneity of attack

To achieve a power blackout it is important that the attack disables multiple substations in such a way to defeat the inherent redundancy in the distribution network. The attackers will take time to select substations for simultaneous disabling with a detailed understanding of the network topology. An attack that attempted to damage one substation after another over the course of several days would be thwarted by operators identifying a suspicious issue after the first two or three incidents before taking substations safely offline to diagnose and remove the problem. During this, power could be rerouted through other substations.

This requirement for the attack to occur simultaneously is one of the most technically demanding aspects of the sophistication of the attack. It requires malicious software to be secretly put into place over time and to remain completely undetectable throughout routine security checks before being activated by an external signal or a precise internal timer mechanism.

Rolling Blackouts

One characteristic of the attack is that the attackers are able to assume control over a large number of substations but know that the defenders will be able to bring each substation back online in a relatively short time (between 8 and 48 hours, with an average of 24 hours). Therefore, in order to create an outage lasting several weeks they must roll the outages around their infected set of substations, carefully selecting the right substations to inhibit so as to take the maximum number of customers off power supply at any one time.

Discovery of rogue hardware as the infection vector will be a key moment in the scenario's timeline. Before that, a substation can be impacted repeatedly with a new (potentially different) cyber attack and attacked again, meaning that there is a continuous exhausting workload for defenders in dealing with individual attacks.

Once the rogue hardware has been recognised as the source of the attacks then defenders will wonder how many substations have the same problem and begin a response plan on a scale necessary to regain control of the system. Potentially every substation in the UK will need to be visited to see if it is present and remove it. This may not be as easy as it sounds, with many thousands of substations in the UK. Care has to be taken with access, security and safety in hazardous environments. A likely approach would be two-fold with teams sent in to identify presence of the rogue device and a separate coalition of teams who then remove the devices once identified.

Even once the rogue hardware is removed, the substation might still contain malware set to inflict an impact at a pre-arranged time.

There is some evidence that the unpredictable rolling nature of blackouts may be more damaging to public morale than one big outage, in particular for those outside the attack zone. The UK public will worry about whom and where will be next affected. Even once the final rogue device has been removed, some outages will continue to occur.

Estimating the time it takes to mobilise safety engineers and security professionals to visit all compromised substations is controversial. Optimists believe all substations can be cleaned up within one week of identifying and analysing the hardware attack platform. Pessimists tend to think it would take six weeks or more. Thus our scenario variants take both of these expert opinions into account, and provide a sensitivity analysis to this variable.

Another key metric is that even with the threat of rolling blackouts; power may be restored quickly, even when the proximate cause of the cyber attack is not clear. Consequently, we consider another variable in the scenario: the effective length of the outage. Lastly, and crucially, the time that the attackers attempt to continue their malicious behaviour is obviously important as well. In fact any cyber scenario could be defined as the logistical capacity of the attackers pitted against that of the defenders. We imagine three different durations of intended attack in the scenario and its variants; 3, 6, and 12 weeks. Additionally, in the X1 scenario we imagine that two different types of attack hardware platforms are introduced, which increases the defenders' logistical burdens substantially.

Timing of Attack

The attackers want to ensure the attack causes broadest spectrum of chaos possible, so execute the attack during the winter season when electricity demand is at its highest.

Side Effects in Distribution System

When substations disappear from the communications network of the distribution company, power will re-route along surviving paths potentially overloading

transmission lines and transformers. When delivered load is lost, power generation plant frequency will rise which can cause generators to 'trip out'. Both these situations would extend the power outage to a wider area beyond the attacked substations. Studying the likelihood and severity of potential cascading outages is beyond the scope of this report but is an established domain of electrical engineering. This report extends the concept to modelling cascading outages in a world where some substations are under the control of others but in relation to cascading economic effects.

Limitations on damage severity

The main limitation to an attack of this type is the ability of a single disgruntled insider to plant rogue devices. There is a limitation in both time and space – the insider are limited in how far they can travel – by the boundaries of their own authority to gain access to substations and travelling time - and they can only install a finite number of devices in the available time before potentially one is discovered.

It is difficult to completely disable large numbers of substations through a cyber attack. Vulnerabilities are specific to types of substation hardware, manufacturers, the set-up and configuration of the substation, the brand of software control system used, the version of that software, the communication protocols, the security operating environment, and all the different components of security that need to be overcome to enable the plan to succeed. An attack can be customised to exploit a number of known vulnerabilities in one specific substation but attempting to exploit systemic vulnerabilities across large numbers of substations that operate different combinations of the above is more difficult.

In this attack, by using an insider with detailed local knowledge in conjunction with the substantial resources of a nation state, the attackers can individually customise their attack to each substation. This gives a high success rate in substations that the attackers manage to penetrate.

The scalability of the attack depends on the standardisation of components and systems in place. In previous cyber scenario research we have identified this concept as 'systemically important technology enterprises' (SITE). In the power distribution industry there is significant standardisation, but there is also sufficient variety and diversity in systems to give confidence that the scalability of attacks will be constrained.

Physically Damaging Transformers

September 14, 2011 (CHICAGO) -- A fire at a ComEd substation on the city's Southwest Side. (Image: ABC News)

Transformers are naturally prone to overheating and thus have built-in cooling systems and di-electric mediums to prevent arcing. Common di-electric mediums are oil, cast resin and sulphur-hexafluoride. Both cooling and di-electric systems must be functioning for the transformer to operate safely and abusing either of them could lead to a fire or explosion. Additionally, each transformer that fails increases the load on the power grid causing instability and, potentially, a cascading power failure. Physical damage to the substation can be achieved by a cyber attack but it is likely that most substations targeted would ultimately be reparable.

Literature on transformer damage includes:

- Fire and Explosions in Substations (Allan, Fellow, IEEE, 2002),
- Using Hybrid Attack Graphs to Model Cyber Physical Attacks in the Smart Grid (Hawrylak et al, IEEE, 2012),
- A Coordinated Multi-Switch Attack for Cascading Failures in Smart Grid (Liu et al, IEEE, 2014),
- The Potential For Malicious Control In A Competitive Power Systems Environment (DeMarco et al, IEEE, 1996),
- Modelling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information (Srivastava et al, 2013)

The Extreme X1 Variant

The X1 variant has an extended time period and expanded geographical coverage. We have imagined this is due to additional factors not present in the S1 and S2 variants:

- Inclusion of the main substation that serves Heathrow airport.
- Two rogue devices in some substations. The attackers produce two different types of rogue devices and some substation have both types installed. Defenders think they have discovered the source of attack when they identify the first type of rogue device, but in fact they need to discover a second type too. This extends the period before effective recovery can begin.
- Physical damage to transformers. Some of the cyber attacks result in physical damage to transformers in some substations. We have not quantified how many of these damaging events occur but assume that this will extend outages as damaged equipment will need to be replaced.

6 The Scenario

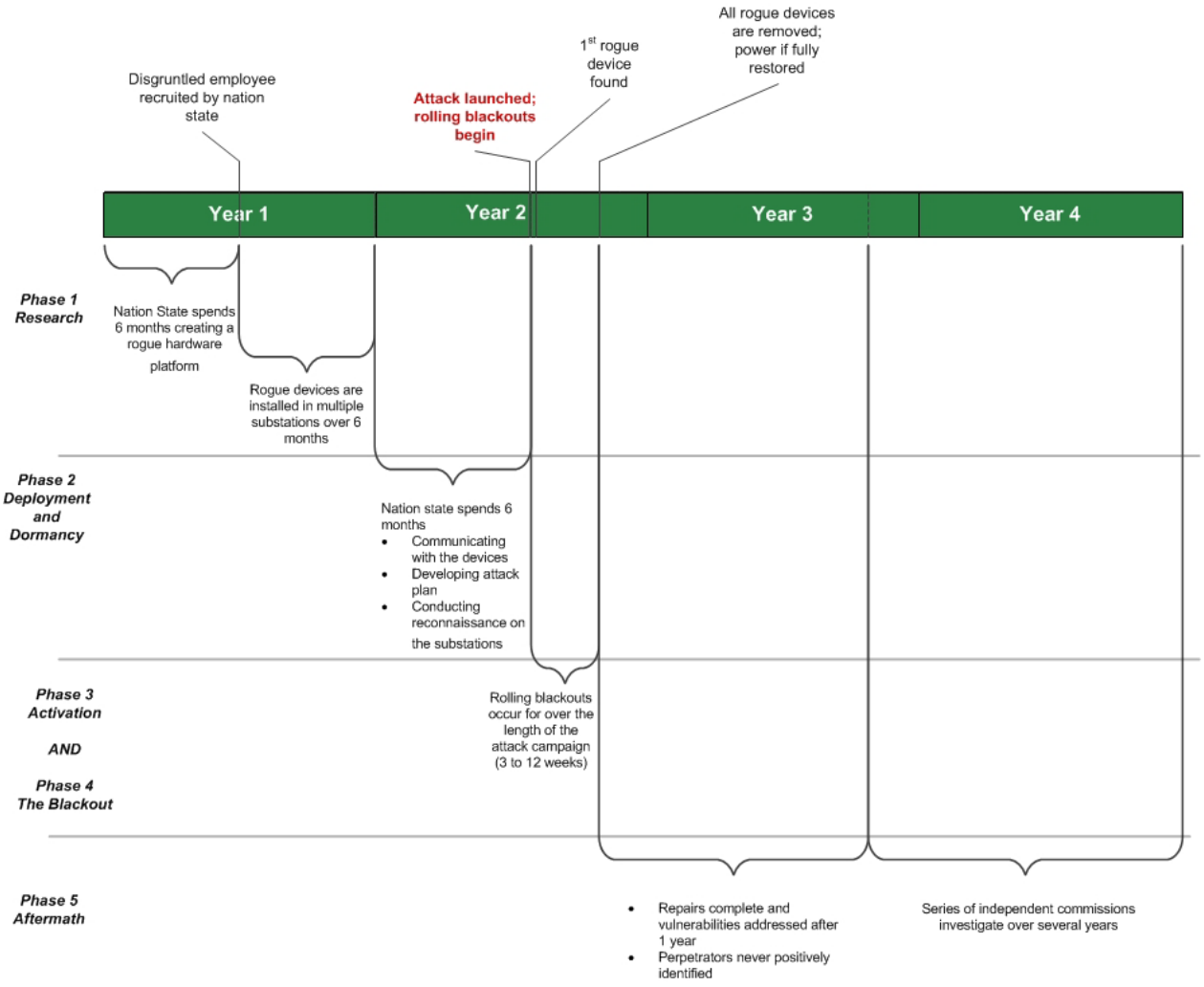

Figure 10: Timeline of the Cyber Blackout Scenario

Phase 1: Research and Development

A nation state hostile to the United Kingdom plots to disrupt electricity supplies in London and the surrounding areas.

The attack targets 132 kilovolt distribution substations that form the nodes of the UK electricity distribution network, which is structured into the regions of the UK's DNOs.

The nation state spends six months creating a rogue hardware attack platform which, once installed on the local area network of an electrical substation, is capable of performing a full spectrum of cyber attacks inside the substation.

To provide communications with the rogue hardware, so that they can establish command and control from a distance, they use 3G/4G mobile phone signals.

For this, they acquire Subscriber Identification Module (SIM) cards to put in the rogue hardware and sign up with several different cell phone (GSM) providers. To make it difficult to physically detect the rogue hardware inside the substation they disguise it as a programmable logic controller (PLC) (Hilt, 2014), a device commonly found in substations. They create a large stock (100+) of these devices.

The attackers identify a disgruntled employee of a subcontractor to several electricity distribution network operators in London and the southeast of England – and employ him to install their hardware.

His role as a site inspector allows him to visit multiple substations in the course of his duties without creating suspicion and significantly increases the attackers' power to pick and choose the largest and/or most critical sites for compromise.

Evidence of overlooked rogue hardware

The PLCpwn (Hilt, 2014) and Power Pwn (Power Pwn, 2015) rogue hardware devices were plugged into equipment rack in a demo room at the S4 Industrial Control System Security conference in January 2015. They were deployed there in plain view and in an environment where people were encouraged to pick the devices up and examine them. Over the course of three days, 200 control system security experts came and went through the environment. None of them questioned the provenance of either device.

Once the employee starts receiving shipments of the rogue hardware devices, he begins to install them inside substations connecting them to the substation LAN and placing the device amongst other similar devices to make them difficult to physically detect. The employee gets one to five substation maintenance works orders per week, thus over a six month period he is able to install rogue devices in 65 substations within one DNO region of the UK.

After the six month period passes, the disgruntled employee quits his job and moves overseas.

Phase 2: Deployment and Dormancy

Identifying Critical Substations

With the inside support, the nation state is able to target key substations that supply electricity to elements of UK Critical National Infrastructure, including:

- Heathrow (X1 only), Gatwick, Stansted and City Airports
- London Financial District
- Ports of London and Dover
- Felixstowe Container Port

Once the rogue hardware devices are present and credentialed within a substation, the attackers can communicate with them via the 3G/4G cell phone channel.

The nation state spends 6 months communicating with the devices. They use this period to construct (but not yet execute) a set of cyber attacks within the substation that are capable of sending commands to open circuit breakers or manipulate electrical busbars and thus take over control of the critical functions of the substation within the electrical distribution system.

The nation state will design all attacks so that they cannot be fixed remotely and require physical presence in the substation. Different cyber attacks are assigned to different substations so responders will not know what kind of cyber attack they are facing when they enter a compromised site. Note that the rogue hardware is capable of re-infecting a substation with a new attack and covering attacks even after a previous attack has been cleaned up. Only once the rogue hardware is removed is it possible to reliably bring customers back onto supply without continuing concerns for the safety of substation workers.

In addition they create (but do not yet execute) a set of "covering attacks" in addition to the main attack that are to be used after the power has been switched off designed to thwart attempts by responders to restore power. These covering attacks include internal DDoS attacks, deletion of files, altering credentials and access control lists and compromises to safety systems.

They also spend this time conducting reconnaissance on the substations networks by:

- Watching for signs that the hardware has been detected
- Recording and analysing network traffic
- Exfiltrating data and performing remote analysis
- Mapping substation network
- Identifying relevant control messages
- Harvesting credentials
- Developing the ability to replay traffic and protocol messages, enabling the control of switching systems in the substation
- Exploiting other connected machines and lateral movement
- Constructing ability to deny communications access to substation
- Planning physical damage attacks

One utility discovers the rogue device but assumes that it was installed by mistake or perhaps by another utility that shares the same buildings.

During this period, the attackers are able to assess the achievable range of control they have within the electrical distribution network. Chief amongst their observations is that they have successfully gained control of 65 substations where the rogue hardware is installed.

Phase 3: Activation

The attack begins during a cold period during winter when electricity demand is at its highest. The general pattern of the attack is to attack a set number of

substations every 12 hours moving through the 65 infected substations in an apparently random but carefully planned order.

Each attack involves issuing commands to open circuit breakers and switching off power to consumers and then thwarting, by a variety of cyber attack techniques within the substation communications network, the attempts by control and field engineers to switch the power back on.

The substations selected for simultaneous attack will have been carefully chosen to cause outages wider than the immediate coverage of the substation, by choosing key critical nodes in the network with high connectivity, and to frustrate attempts to re-route power.

When the attackers "use up" all their infected substations, previously attacked substations are again selected. This is possible providing the rogue hardware is still in place which will be the case for at least the first week.

Scenario Variants

This narrative describes the S1 scenario; however we have modelled two additional variants. In terms of the effectiveness of the response, S1 describes an 'optimistic' scenario where responders are rapid and efficient. The S2 scenario is a more realistic 'conservative' scenario that assumes that the speed and quality of the response is average. In X1, the response is poor but the attack is more intense.

In terms of the number of people affected, each scenario sees an increasing number of customer disruptions. For example, the total UK population affected by substation attacks at some point during the campaign is 14% (S1), 18% (S2) and 20% (X1) for each scenario variant. These are estimates derived from approximating the number of customers served by each substation.

In the most extreme scenario (X1), a slightly larger geographic area is affected which includes substations serving Heathrow airport (Europe's busiest airport). In addition, some substations feature two rogue devices as well as some physical damage to transformers.

The Days 1 - 2

In the first three days of the campaign a typical individual attack plays out as follow. When a substation circuit breakers are opened, control signals are spoofed and the DNO control centre is unaware it has happened. After about an hour, consumers calling the DNO support call-centre alert the control centre that there is a significant outage around that substation. As the control centre cannot see the outage on their system, they dispatch a field engineer who travels to the substation. The engineer is met by a confusing situation on the substation LAN but is unlikely to have the cyber security expertise to understand what the problem is.

The engineer is able to reconnect power manually after eight hours of outage. When colleagues with sufficient expertise arrive, they identify that there has been a cyber attack within the substation and clean it up in a timescale between 12 and 48 hours.

A defence response by the DNO does not begin until the second or third outage is reported. DNO responders initially focus on evaluating logs in substation control rooms for the times and locations

Table 2: Summary of UK cyber 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	>1 region	Yes

of the outages. While an insider is suspected, no actions correlating with insider behaviour can be identified in the central control room.

The logs files take a few days to analyse and the outages continue, putting pressure on the investigation to come up with answers and sowing discord in the control room. Any intrusion detection systems in the control facility only show normal traffic with no anomalous behaviour. Eventually, the engineering team demands a control room free of fruitless investigations in order to concentrate on restoring power to customers in peace.

The Days 2 – 7

Defending engineers start to move more quickly to put substations back on line manually but one engineer is electrocuted by a compromised safety system. This immediately has the effect of ruling out engineers using manual override which lengthens the outages. Engineers now have to rid the substation of the cyber infection completely (but not the rogue hardware which has still not been identified) before power can be restored.

Note that the average restoration time for an individual substation (12 to 48 hours; with an average equal to 24) will depend on a number of factors:

- Availability of skilled personnel with cyber security expertise
- Travel times to substations
- Provisions of permits to work
- Safety procedures
- Number of hours worked
- Delays in inspectors sign off before reconnecting

We assume the same restoration time for all substations, though there is a case to be made that the restoration of critical substations may be prioritised.

By now the investigation moves on to inspecting the substations themselves and discovers that the outages are caused by authorised commands coming from inside the substation but that are anti-correlated with control room records. Following this discovery, investigators begin to seek an inside-attacker within contractor and substation personnel.

Phase 4: The Response

Days 7 – 14

The attacks continue. Rolling blackouts effectively spread the impact of the attack wider than the compromised areas. Confusion and suspicion lead people outside the attack footprint to plan for outages (leading to panic buying, shortages, scaling back production, etc.), fearing that they may be soon affected, even if their nearby substation network is not actually within the attack zone.

Once it becomes clear that the blackouts are rolling apparently randomly and unchecked around a certain region, concern over the true scale and spread of the phenomenon and future blackouts will become intense, effectively spreading public alarm to the entire UK.

The Cabinet Office and CPNI issue a statement alerting the public that they suspect the outages are the result of a cyber compromise somewhere in the power grid system. At this stage, national intelligence and security services become involved.

The nation state cyber actors have designed all attacks so that they cannot be fixed remotely and require physical presence in the substation. Different covering attacks are assigned to different substations so responders will not know what kind of cyber attack they are facing when they enter a compromised site. Note that the rogue hardware is capable of re-infecting a substation with a new attack and covering attacks even after a previous attack has been cleaned up. Only once the rogue hardware is removed is it possible to reliably bring customers back onto supply without continuing concerns for the safety of substation workers. Sometimes a previously attacked substation is attacked again using a different cyber technique.

Discovery of the Rogue Hardware Device

After one week, an engineer on site in a substation discovers a suspicious piece of hardware, removes it, and submits it for inspection by the investigating authorities.

The process of analysing the device in order to determine whether it is related to the attacks starts, and efforts to reverse engineer the devices and discover its capabilities begin.

Once it becomes apparent that the device is at the heart of the attack, the authorities put together a plan for removing any other suspicious hardware from potentially every substation in the UK, focussing first on substations where attacks have already been carried out and those that are most critical to the network. Staff have to be certified to be competent to work on equipment and systems and the issue would have to be addressed of resourcing sufficient manpower to visit all the substations. The DNO would provide some personnel with additional pulled in from other DNOs. It may be possible to draft some military personnel though they would require time-consuming training. The time span between discovery of the first device and the time the concerted removal plan is executed

is one week in S1, two in S2 and four in X1 – note the extension of X1 times is due to two different types of rogue devices, a larger attack area, and the diversion of resources to deal with physical damage.

Days 14 – 21

The next week (three in S2; six in X1 (though in X1 this includes additional repair of physical damage) is spent hunting down and removing all the other rogue devices. The presence of the army and other agencies requires significant coordination with the DNO administrator who is not accustomed to such situations or such national and international attention.

One particular challenge is the efficient location of all the other rogue devices. Pictures and specification sheets of the malicious devices need to be distributed to substation inspectors be they private or government forces. This leads to inefficient external investigations and delays the efforts to visit every substation. Meanwhile, outages continue in the region.

In X1, physical damage of transformers occurs[28], so the removal of rogue devices takes place in parallel with repair of physically damaged equipment.

While rogue hardware is present it is possible to repeat an attack on a previously attacked substation using a different cyber thwarting technique and that once a substation is attacked, removing the rogue hardware will not in itself clean up the cyber attack. Removing a rogue device does not mean the substation cannot be attacked, only that its covering attack capabilities are limited – the attack may be in place and lying dormant.

The attackers will take care to maintain power to mobile phone masts so as not to interrupt their own command and control channels, though it should be noted that attacks can still be left as logic bombs or timed events without the presence of the rogue hardware – only re-infection cannot take place.

Once all rogue devices have been discovered and removed, some substations remain infected with cyber attacks that still execute later, meaning that occasional outages will still affect the region. However, defenders are now well equipped to clean up these attacks relatively quickly. In the X1 scenario, physical repairs are needed too.

Phase 5: The Aftermath

The vulnerabilities are addressed and repairs of the damaged transformers (in X1) are complete within one year of the incident. The perpetrators are never positively identified. There are a series of independent commissions to investigate the incident in the years that follow.

The wider influence of the scenario would impact the UK's economy for at least three years after the event. Public confidence would be shaken in a similar way as after a major terrorism event, with the public becoming aware of the new possibilities of cyber as a means of attack on daily life. Internationally important aspects of the UK critical infrastructure impacted in the attack may find themselves overtaken by nearby competitors such as such as Heathrow by Schiphol and the City of London by Frankfurt. There may be a move towards diversification of important continental connection points such as Felixstowe being diversified by the enhancement of the container port in Hull.

Cyber security budgets would increase and there would be a concerted effort to improve security in the development life cycle of ICS. The third party contractor who employed the malicious insider would be sued for inadequate hiring procedures. Third party contractors working in the critical national infrastructure space would be under increased scrutiny with requirements for better hiring procedures, segregation of working patterns and may become regulated. Substation security would be overhauled with new physical and IT measures, and regular audits, which would result in higher energy bills for consumers. In particular there would be new techniques installed for substation network access control (NAC) to detect unexpected devices on their networks.

There would be an increasing awareness that the move in the electricity industry towards smart grids – the move towards algorithmic control of the electricity generation, transmission and distribution system – will only exacerbate the risks explored by this scenario, by increasing the amount of computation driving all parts of the system. It would be perceived that: 'the cyber risk in the electricity supply sector and therefore Critical National Infrastructure is only going to increase'.

Restoration curves

The electricity restoration curves for these scenarios are shown in Figure 11 where 100% represents the total population within the attack regions in London, the South East and the East England. This graph illustrates how both the geographical extent of the outage (percentage of customers without power) and the temporal duration of the campaign are amplified from S1 to X1 and how the campaign peaks at different times and magnitudes for each of the three scenarios.

[28] (Allan, Fellow, IEEE, 2002), (Hawrylak et al, IEEE, 2012), (Liu et al, IEEE, 2014), (DeMarco et al, IEEE, 1996), (Srivastava et al, 2013)

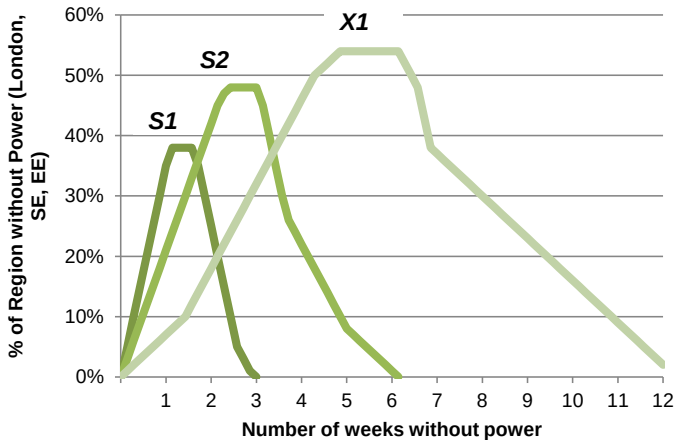

Figure 11: Rate of electricity restoration in the affected area across all scenario variants

The area under the curve therefore represents the number of 'outage-days' caused by the campaign. One outage-day is equivalent to one day with 100% no electricity. These curves are derived from an estimate of the number of customers served by each substation, and serve as an illustrated guide for the behaviour of the attacker during the campaign.

7 Methodology

This research uses three methodologies with each providing specific insight into particular aspects of critical infrastructure failure. In this section an overview of these methodological techniques will be provided. Figure 12 is a flow diagram which illustrates the methodologies utilised in this report and the sequence in which they are used.

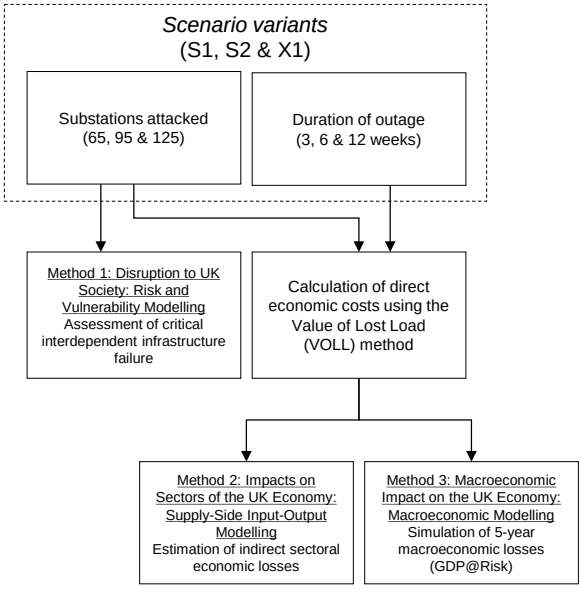

Figure 12: Flow diagram of methodologies

This consists of:

- **Method 1:** Disruption to UK Society: through Risk and Vulnerability Modelling, the number of customers disrupted from cascading failures between critical infrastructures;
- **Method 2:** Impacts on Sectors of the UK Economy: through Supply-Side Input-Output Modelling, the economic losses incurred by different industrial sectors of the UK;
- **Method 3:** Macroeconomic Impact on the UK Economy: through Macroeconomic Modelling, the long-term GDP@Risk to the economy over a five year period.

Method 1: Disruption to UK Society: Modelling Risk and Vulnerability in Critical Infrastructure

An infrastructure vulnerability assessment model by the Environmental Change Institute at Oxford University (*www.eci.ox.ac.uk*) is used to analyse the disruptive consequences associated with a cyber attack on 132kV electricity substations. This disruption is measured in terms of the number of user disconnections across multiple infrastructure types.[29]

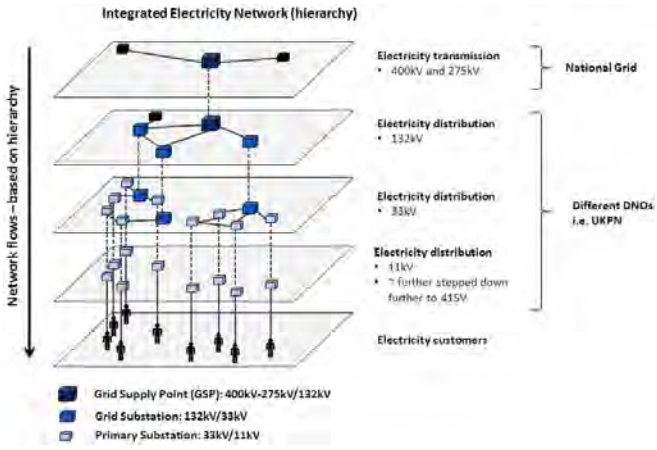

Figure 13: Generalised overview of electricity transmission and distribution in England. Highlighting three different recognised substation types: Grid Supply Points (GSPs); Grid Substations and Primary substations.

Infrastructure	Direct connection
Airports	Primary
Ports	Primary
Railways	Grid
Waste water treatment works	Primary
Water towers	Primary
Telecoms masts	Primary

Table 3: Mapping between critical infrastructure assets and electricity distribution substation types.

Network assembly

Figure 13 provides a generalised-abstract overview of electricity transmission and distribution in England. The integrated network forms a hierarchy of flows, from power generation to electricity users, where the electricity is sequentially stepped down from high voltage transmission networks to low voltage distribution networks. 'Stepping-down' is performed by electricity transformers that are located within substations, the figure represents three specific

[29] Pant, R., Hall, J.W., Barr, S., & Alderson, D. (2014). *Spatial Risk Analysis of Interdependent Infrastructure Networks Subjected to Extreme Hazards. Vulnerability, Uncertainty and Risk*, pp. 677-686; Pant, R., Hall, J.W., Blainey, S.P. (2016). *Vulnerability assessment framework for interdependent critical infrastructures: case-study for Great Britain's railway network. European Journal of Transport and Infrastructure Research*, 16(1); Thacker, S., Pant R., and Hall, J. W. (2016). *System-of-Systems Formulation and Disruption Analysis for Multi-Scale Critical National Infrastructures. Reliability Engineering and System Safety*. In Review.

substation types, generally characterised by their function and operational voltage: Grid Supply Points (GSPs); grid substations and primary substations.

Critical infrastructures typically derive their electrical power needs from a direct connection to distribution networks. The exact voltage level to which individual critical infrastructure assets are connected may vary. However, the majority of each asset type connects to the same voltage level (the same substation type).

Table 3 provides a typical mapping between critical infrastructure assets and electricity distribution substation types.

Method 2: Impacts on Sectors of the UK Economy: Supply-Side Input-Output Modelling

To estimate the second order consequences on the UK economy an input-output (IO) modelling approach has been implemented[30]. Using the most recent data (2011) from the Office of National Statistics (ONS)[31], a supply-side inoperability model has been developed which enables a direct shock to be administered to the different economic sectors of the UK economy, proportional to the value-added of the DNO attack region for each scenario. This direct shock must first be estimated in order for it to be used within the economic model.

Estimating direct economic impacts

Direct losses are estimated using the Value of Lost Load (VOLL) method. Within the literature, VOLL refers to the monetary loss associated with a disruption to the electricity supply. It can occur as a result of failure to production, transmission or distribution within the electricity network. It is therefore widely used as an indicator for energy supply security of a country, region or economic sector (van der Welle and van der Zwaan, 2007). Estimates of VOLL vary widely across different studies dependent upon the regions or sectors analysed and methods used (London Economics, 2013).

VOLL is a non-price responsive quantity and as such cannot be directly observed in the market. It is necessary, therefore, to consider indirect indicators of its value. Indirect methods for estimates introduce several layers of complication that may vary by consumer, season, time of day, duration and frequency of outage, and their ability to anticipate and adjust to the interruption of electricity service.

These values present a challenge in capturing a precise estimate on what the value of a marginal kWh of electricity to business represents.

Within the literature, four methods have been used to provide estimates of VOLL across different economic sectors: the survey method (stated preference); the proxy method; consumer surplus method; and estimates based on the contribution of electricity to Gross Value Added by sector (revealed preference).

The stated preference survey method asks consumers to provide information on how much they would be affected by an outage. This somewhat subjective approach asks about a consumer's willingness to pay (WTP) or willingness to accept (WTA) an electricity outage of predetermined duration. The weakness of this approach is that it can be highly dependent on respondent perceptions and is considerably hypothetical. Relevant experts believe that this can give rise to an overestimation of the value of electricity supply, especially for low probability high severity events (Royal Academy of Engineering, 2014). It is not clear whether those commercial or non-commercial respondents would actually be willing in reality to accept electricity supply interruptions in return for financial compensation.

The proxy method estimates the cost of what is actually spent on purchasing replacement equipment during an outage; an example of replacement equipment includes the purchase of additional generation capacity such as a diesel generator. For those countries with few electricity interruptions, such as the UK, the use of this method makes it very hard to estimate the upper bound of disruptive events (de Nooij et al. 2007).

The consumer surplus method estimates the extra value that is derived over and above what is actually paid for the electricity. Studies have shown that consumers are willing to pay as much as 100 times what they already pay in a completely free market. In reality however, this method does not guarantee that commercial or non-commercial consumers would actually be willing to pay this if the situation actually arose.

A recent study by the Royal Academy of Engineering (2014) entitled *Counting the cost: the economic and social costs of electricity shortfalls in the UK* concludes that revealed preference methods can be much more robust. Relevant experts interviewed in this report identify that stated preference methods such as survey approaches can be particularly unreliable, especially for companies. One such revealed preference method is the production function approach which uses the proportion of value added provided by electricity by each economic sector (Leahy & Tol, 2011).

[30] For an overview of the different methods that have been used to model infrastructure interdependency and their limitations see Kelly (2015).

[31] Office for National Statistics, *Input-Output Supply and Use Tables - 1997-2012*, 2014 Edition

Sector	GVA (£ million)	Elec Use (Twh)	VOLL £/kWh
Real Estate Activities	£134,690	1.0	137.0
Construction	£88,547	1.9	47.3
Professional Services	£102,536	3.2	32.0
Information Technologies	£38,466	1.3	29.5
Administrative Services	£67,554	2.3	29.4
Financial Services	£117,835	6.3	18.8
Education	£82,645	5.4	15.4
Communications	£46,617	3.3	14.1
Transportation	£47,637	4.1	11.7
Wholesale and Retail trade	£146,957	14.9	9.9
Government And Emergency Services	£71,026	7.4	9.6
Accommodation and Food Service Activities	£43,813	4.6	9.5
Other Services Activities	£22,351	2.7	8.4
Arts, Entertainment and Recreation	£17,895	2.2	8.3
Health	£100,352	17.2	5.8
Defence Manufacturing	£15,529	4.1	3.8
Agriculture, Forestry and Fishing	£8,495	3.9	2.2
Food	£19,971	10.7	1.9
Mining	£4,411	3.3	1.3
Electricity	£9,429	7.3	1.3
Water Supply and Waste Management	£15,071	11.7	1.3
Energy	£34,720	27.5	1.3
Manufacturing	£91,377	79.4	1.2
Emergency Services	3,233	0.1	0.3

Table 4: Estimates of GVA, Electricity Use and VOLL by Economic Sector

This is estimated by dividing total Gross Value Added by sector by total electricity consumption by sector, thus giving an estimate of £/kWh. This approach assumes that electricity is a necessarily factor input for production, therefore even sectors with high GVA and low electricity requirements will be given a high VOLL. The main weakness associated with this approach is that each sector's ratio of GVA to electricity consumption only reveals the average productivity of electricity (Poudineh & Jamasb, 2015). Nevertheless, this approach provides the most accurate tool available for estimating the direct costs of disruption to electricity supply. Therefore, in this analysis we estimate VOLL on a sector by sector basis using the Gross Value Added approach. Estimates of GVA, electricity use and VOLL by sector are noted in Table 4.

Estimating Indirect Economic Impacts using Supply-Side Input-Output Modelling

The classic IO approach is based on the Leontief framework which is able to capture the economic interdependencies (as capital flows) between different sectors of the economy. A system of linear equations represents each economic sector's dependence on production inputs from other parts of the economy. It uses the accounting framework of double entry book keeping to ensure that total outputs of an economy equal total inputs thus providing a relationship between final demand, total output and value-added by each economic sector. For further reference of the basic IO model, the most comprehensive overview is provided by Miller and Blair (2009).

In this model, the economy is comprised of n economic sectors, with x_i representing the total output of Sector i. The amount of input required from Sector i to produce x_j (the output of Sector j) is represented by x_{ij}. The supply-side balance equation is as follows:

$$x_j = \sum_{i=1}^{n} x_{ij} + f_j \quad \forall j \qquad (0.1)$$

In the original Leontief equation, a_{ij} is shown as the fixed input coefficient of Sector i related to total output of Sector j (x_j). This relationship is converted in the supply-side model whereby the sectoral gross output of each sector is related to the primary inputs. Each *row* of $\boldsymbol{z}$ (the inter-industry matrix) is divided

by the gross output of the sector associated with that *row* (as opposed to dividing each *column* of $\boldsymbol{z}$ by the gross output of the sector associated with that *column*). Matrix $\mathbf{B}$ is used to denote the direct-output coefficients matrix with elements b_{ij}.

This set of coefficients represents the distribution of Sector *i*'s outputs across the sectors (*j*) that purchase interindustry inputs from *i*. The relationship between total output $\boldsymbol{x}$ and value added $\boldsymbol{v}$ can therefore be written as:

$$\Delta \mathbf{x} = \Delta \mathbf{v}(\mathbf{I} - \mathbf{B})^{-1} \qquad (0.2)$$

where, $\mathbf{I}$ is the identity matrix of rank *n* and $(\mathbf{I} - \mathbf{B})^{-1}$ is known as the Ghosh inverse (Ghosh, 1958). The perturbation vector $\Delta \boldsymbol{v}$ represents the degraded value added caused by an electricity outage for each economic sector. The supply-side or Ghosh variant of the IO model is used as opposed to the demand-side Leontief approach because the supply side approach is able to utilise the direct impact of degraded electricity supply on value added. It is therefore able to calculate the indirect down-stream effects on other sectors in the economy that rely on the goods and services from those sectors originally disrupted.

In doing so, we are able to rank those economic sectors which feature the largest loss in economic output. This provides insight which can be used for supporting decision making in resilience planning, as limited resources can be targeted at those vulnerable sectors with the largest cascading effects. This can also help to bolster private and public investment into protecting interdependent critical infrastructure assets with the aim of avoiding catastrophic events.

Method 3: Macroeconomic Impact on the UK Economy: Macroeconomic Modelling

This method enables the quantification of both the direct and indirect economic consequences resulting from systemic power-system failure revealing the overall impact to the UK Economy in terms of our standard metric for scenario impact – GDP@Risk. Measuring different types of catastrophes using a standardised metric enables the comparison of a wide range of natural, technological and financial catastrophes.

The model used in this analysis, The Oxford Global Economic Model (GEM), is the most widely used international macroeconomic model with clients including the IMF and the World Bank. The model provides multivariate forecasts for the most important 47 economies of the world with headline information on a further 34 economies. Forecasts are updated each month for 5-year, 10-year and 25-year projections.

The GEM is best described as an eclectic model, adopting Keynesian principles in the short run and a monetarist viewpoint in the long run. In the short run output is determined by the demand side of the economy, and in the long term, output and employment are determined by supply side factors. The Cobb-Douglas production function links the economy's capacity (potential output) to the labour supply, capital stock and total factor productivity. Monetary policy is endogenised through the Taylor rule, where central banks change nominal interest rates in response to changes in inflation. Relative productivity and net foreign assets determine exchange rates, and trade is the weighted average of the growth in total imports of goods (excluding oil) of all remaining countries. Country competitiveness is determined from unit labour cost.

"Sector Direct Losses" refers to economic losses sustained directly by sectors as a result of not receiving electricity over the outage period. This is calculated in the same way as outlined previously. "Sector Indirect Losses" refers to those economic losses in the industrial sectors which depend on other sectors in the economy both upstream and downstream on those sectors which do not have power for the duration of the outage. Indirect losses have the potential to extend outside the footprint of the blackout zone and affect commercial activity elsewhere in the country. GDP@Risk captures these additional losses and is the aggregate total losses on the economy and takes into account losses in confidence, business failure and losses resulting from decreases to international trade etc. The total GDP@Risk also extends beyond the outage period to include the recovery of the economy up to five years after the outage has occurred.

The justification for using two different macroeconomic methodologies is as follows. As previously identified in this section, the IO modelling approach (Method 2) provides insight into the expected immediate losses by different economic sectors over a one year period. Alternatively, the macroeconomic modelling approach detailed here (Method 3) provides a five year picture of how shocks to labour, consumption, trade and business confidence lead to a standardised GDP@Risk figure which can be compared with other types of catastrophes.

8 Disruption to UK Society

In this section we analyse the impact of the scenario in terms of disruption to consumers due to not only the electricity outage but other components of critical infrastructure. All critical infrastructures - airports, telecoms masts, water towers, waste water treatment works, rail stations - require electricity for their operation and therefore are critically dependent on a fully functioning electricity network.

We are able to estimate the number of people disrupted, by critical infrastructure type, for each scenario variant. This disruption spreads beyond the areas impacted by power outages, and in the case of highly networked infrastructures such as the rail network, the disruption will spread all around the country.

This kind of analysis is useful in estimating societal impacts, and was carried out using the infrastructure network vulnerability assessment methodology, as described in the previous section.

Customer demand assignment

The direct daily customer demand is estimated for each critical infrastructure. To summarise, airports are derived from annual flight statistics and are calculated as the total number of terminal passengers for an average day in 2009. Similarly, average daily port cargo is derived using 2009 national port usage statistics.

In the absence of data for point asset demands for the electricity distribution substations, water towers, wastewater treatment plants and telecommunication towers assets, we estimate these using a Voronoi decomposition technique.[32] Assignment of customer demand is a two part process comprising: (i) deriving infrastructure asset footprints to estimate the spatial area of influence around each distribution level asset, and (ii) assigning customer values to each distribution level asset based on a spatial union of asset footprint with census derived population estimates. For each scenario the number of electricity customers affected is estimated and reported.

By transferring assigned non-electricity customers to their supporting electricity assets via corresponding dependency link, we perform a location allocation assignment to distribute them along paths in the integrated electricity network based on source capacities and source-sink flow strengths.

Customer demands for the railway network were derived using a model of station entries, interchanges and exits.[33] By combining this with train frequencies along routes, daily origin-destination trip assignments were able to be created for passengers in the railway network.

Selection of compromised substations

Within the DNO area, substations were initially ranked based on the number of customers served from each asset. For each scenario variant (S1, S2 & X1), the top 20, 30 and 40 substations serving the most customers from each geographic region (London, South East, and East of England) were selected. This formed the basis for each scenario and was supplemented by the addition of five other substations which were included because they provide power for critical infrastructure assets of national importance such as major ports, airports and railway stations. As a consequence of these substation selections, each scenario provides a different geographical footprint. This customer disruption data is consequently used to produce the economic shocks for wider analysis.

Failure and disruption estimation

We define *failure* as a condition of the node or edge asset such that it is no longer able to perform its functional purpose. In our description of infrastructure provision this means that the service demand satisfied by the affected node is lost and all its connections are severed. This will reduce, or in the extreme case, disrupt the whole demand of other connected assets.

Based on the S1, S2, X1 scenarios, it is assumed that all the selected electricity substations have failed and subsequently the number of disrupted electricity customers is estimated. For other critical infrastructures such as airports, ports, telecoms masts, water towers and waste water treatment works customer disruptions are estimated based on whether the connected electricity substation has failed. For the railway network disruptions we first consider the stations disrupted due to connections to the failed electricity substations. Following which we consider all origin-destination journeys that are lost even after rerouting due to disruption of the selected stations.

The aggregated number of customers affected by each critical infrastructure sector provides the disruption estimates is reported in Table 5.

[32] Thacker, Pant, Hall, *Characterizing the vulnerability of future configurations of Great Britain's electricity network*, 648-657.

[33] Pant, Hall, Blainey, *Vulnerability assessment framework for interdependent critical infrastructures*, 174-194

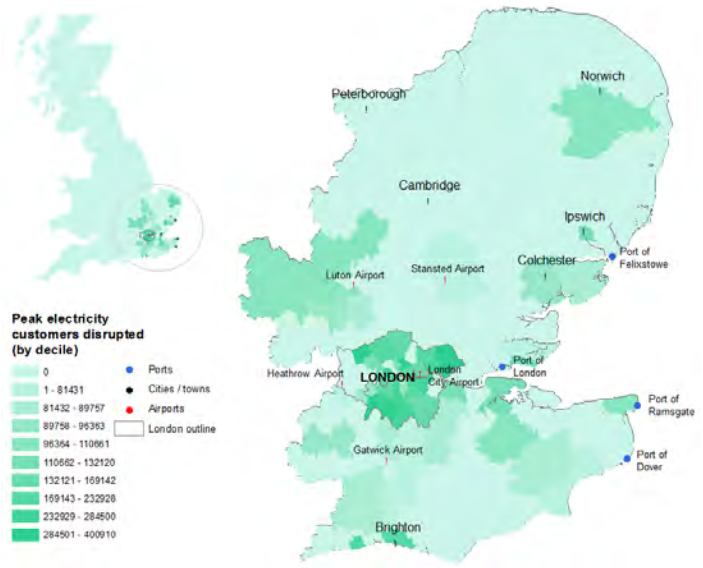

Figure 14: Electricity Customers Disrupted

Impact on the population

A total of 36% of the UK population (23.4 million citizens) reside within the geographical regions of London, the South East and the East of England (ONS, 2015)[34]. Attackers target a proportion of substations within these regions to cause maximum economic and psychological impact. Customers within these regions affected by the substations under attack represent between 14% and 20% of the UK population across each variant of the scenario.

In the S2 scenario, the worst afflicted region is London which contains 38% of all those affected, followed by East England (32%) and then the South East (30%). The attackers target substations in hot-spot areas that will cause the most disruption to critical infrastructure systems such as airports and sea ports, hence, disrupting the greatest number of customers.

Table 5 also outlines a summary of the direct impacts caused by the initial electricity outage across different infrastructure types.

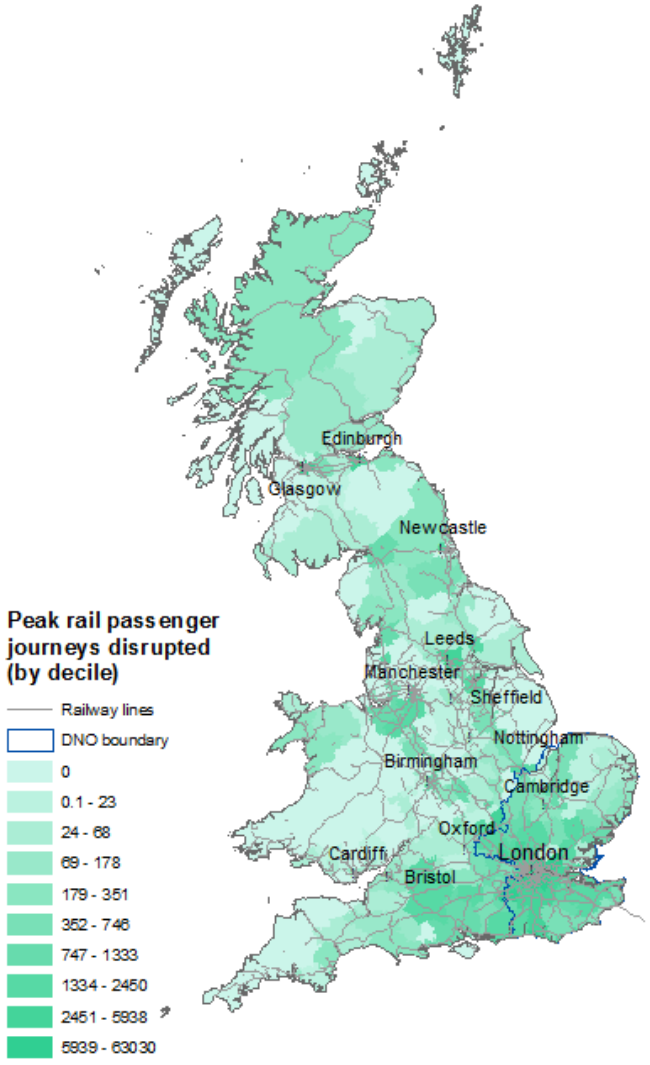

Figure 15: Peak Rail Passenger Journeys Disrupted

Table 5: Number of people disrupted, by critical infrastructure type

Scenario	Electricity	Airports	Railways	Ports	Digital communications	Water	Waste Water
	peak customers disrupted per day	peak passenger trips disrupted per day	peak passenger trips disrupted per day	peak tonnes disrupted per day	peak customers disrupted per day	peak customers disrupted per day	peak customers disrupted per day
S1	8.9 m	150,300	0.85 m	76,200	8.6 m	7.9 m	9.6 m
S2	11.3 m	150,300	1 m	216,000	11.3 m	10.4 m	11.0 m
X1	13.1 m	330,200	1 m	287,000	12.8 m	11.8 m	12.6 m

[34] Office for National Statistics. "Annual Mid-Year Population Estimates for the UK". Date published: 26 January 2015. Release number: MYE7PE3

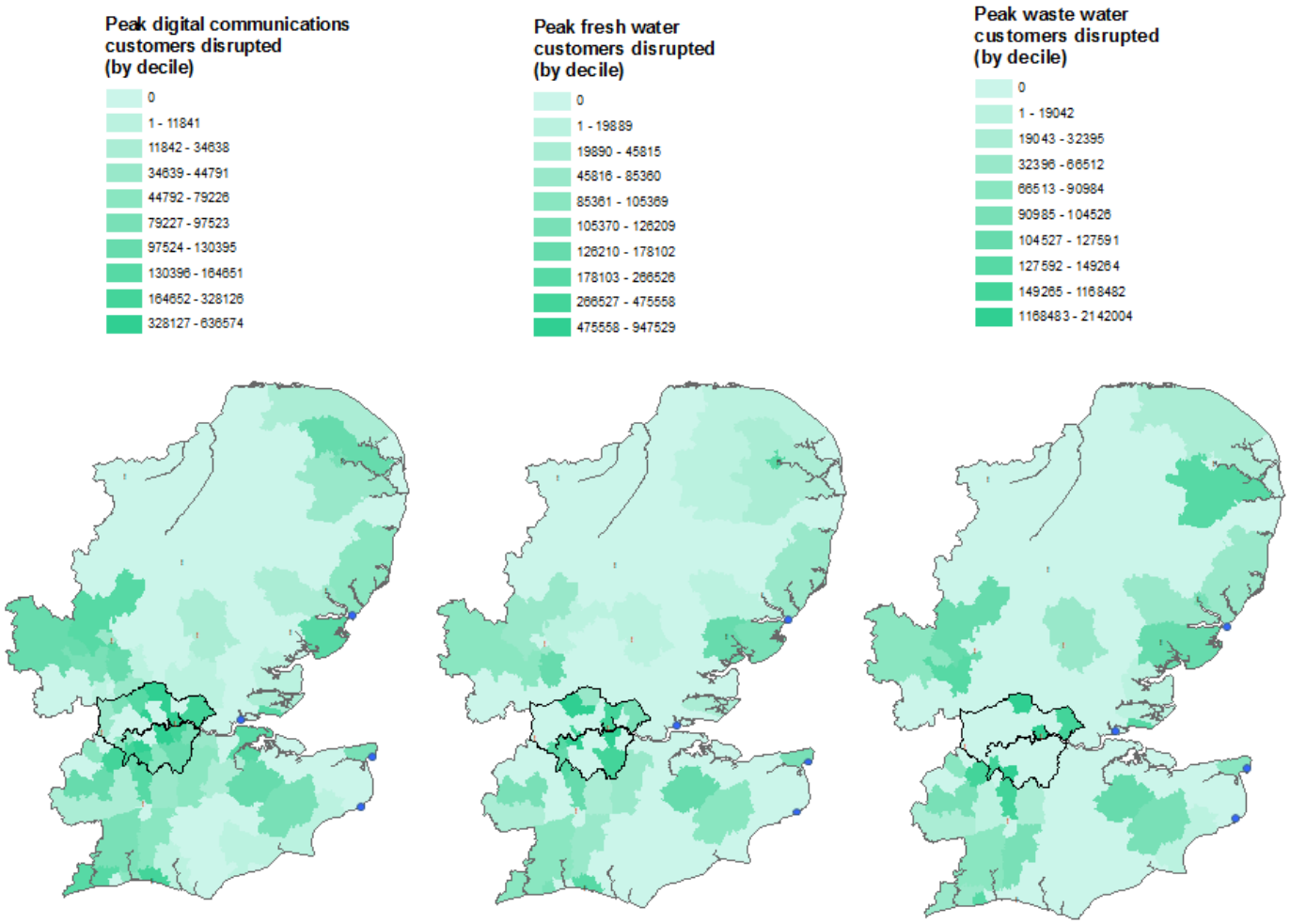

Figure 16: Peak digital communications, fresh water and waste water customers disrupted

9 Impacts on Sectors of the UK Economy

In this section we analyse the impact of the electricity outage on individual sectors of the UK economy. An input-output (IO) macroeconomic modelling technique is used. This kind of analysis provides an understanding of the relative impacts on different economic sectors, and can support decision making for resilience investment.

Infrastructure interdependency

As with all complex systems, infrastructure systems are connected through multiple layers of interdependence (Rinaldi et al., 2001). This poses a non-trivial problem in understanding the effects on the system as a whole as failure in one subsystem may spread to other parts of the interdependent network. The analysis of this dynamic is often referred to as "system-of-systems analysis".

The five "layers" of interdependence active within the critical infrastructure network include: physical, cyber, logistical, spatial and economic:

- "Physical" connections refers to literal structures which facilitate system connectivity, such as power cables or digital communications lines;
- "Cyber" connections are links that exist through virtual means and may include software updates, computer viruses or targeted hacking;
- "Logistical" connections incorporate an organisational characteristics and systems of operation;
- "Spatial" connections refer to infrastructure systems that co-located or located within the same risk footprint;
- "Economic" connections are interdependencies that arise from supply chains both up and downstream of the affected critical infrastructure.

Critical infrastructures are often referred to as Complex Adaptive Systems (CAS) and are hard to decompose for analysis and therefore represent more than just an aggregation of their components.

As different infrastructures are brought together and interact with another, synergies emerge. Analysis of co-dependencies and coupling within the system thus requires an understanding of the system as whole so as to understand how different components of the system are impacted when failure occurs.

Infrastructure interdependency and secondary consequences

Substantial direct and indirect economic losses are evident across all critical infrastructure and non-critical economic sectors. Total lost value-added for the S1 scenario amounts to £11.6 billion.

Of every £1 lost directly in the cyber attack, roughly £0.62 is lost directly and £0.38 is lost indirectly in commercial production activities. The loss of electricity to 8.9 million customers leads to disruptions in digital communications (8.6 million customers), fresh water supply (7.9 million customers) and urban waste water treatment (9.6 million customers) (See Table 5). Business operations cease as a considerable proportion of the workforce are unable to physically get to their place of work. This is exemplified in that fact that 850,000 passenger trips are affected per day on the rail network, and 150,300 per day through airport chaos.

Both domestic and international travel is hampered, particularly into and out of key commercial districts in London and the South East. Delayed processing and trading of agricultural products leads to a large loss in perishable products. As a result, many food processing and manufacturing plants in London, the South East and the East of England cease production. Food prices increase as a consequence of limited supply.

The results illustrated in Figure 17 show that the Financial Services sector is the worst affected with a total loss of £1.3 billion. The largest losses to other critical infrastructure sectors include Health (£0.7 billion), Transport (£0.6 billion) and Government and Emergency Services (£0.5 billion).

Table 6: Total economic losses by scenario (from IO modelling)

Scenario	Length of campaign	Substations attacked	Direct losses (£millions)	Indirect losses (£millions)	**Total Losses (£millions)**
S1	3 weeks	65	£7,211	£4,373	**£11,584**
S2	6 weeks	95	£18,055	£10,915	**£28,971**
X1	12 weeks	125	£53,643	£31,841	**£85,484**

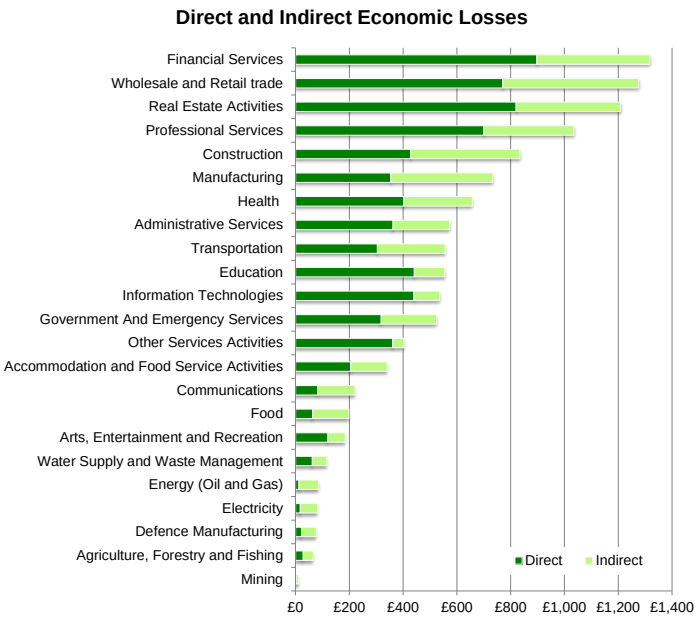

Figure 17: Direct and indirect economic losses by sector (S1) (from IO modelling)

Out of the economic sector sectors analysed, the largest losses were evident in Wholesale and Retail Trade (£1.3 billion). This was followed by Real Estate Activities (£1.2 billion), Professional Services (£1 billion), and Construction (£0.8 billion).

Although critical infrastructure sectors suffer smaller losses than other economic sectors on the whole, these sectors are vital for supporting production, distribution and consumption throughout the economy. Therefore, their in-operability has a dramatic indirect effect outside the domestic attack zone, disrupting supply chains across Europe and the globe.

Even if some firms are prepared to provide mission-critical infrastructure services from backup generators or other inventory stores, these measures ultimately become inadequate over the long-term. Indeed, although power may be provided locally there is no guarantee that other necessary critical infrastructures will be in operation, such as digital communications, data storage and back-up channels.

Table 7: Direct and indirect sector losses (£millions) from IO modelling

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

10 Macroeconomic Impact on the UK Economy

This chapter quantifies both the direct and indirect economic consequences resulting from systemic power-system failure and reveals the overall impact to the UK Economy in terms of our standard metric for scenario impact – GDP@Risk.

This quantification takes into account:

- **Direct damage to assets and infrastructure** such as the cost associated with replacing damaged assets. The electricity system can fail for many reasons but, when this involves the malfunction or damage to hardware, the failure incurs a cost that must be included in economic loss estimations.
- **Direct loss in sales revenue to electricity supply companies** such as the revenue that would have been generated in the event of no electricity failure. Estimating revenue losses is achieved by multiplying the expected price of electricity by the amount of electricity that would have been sold by the total amount of unsupplied electricity. In practice, lost revenue to the electricity industry would be split between the generation, transmission and distribution facilities and electricity suppliers.
- **Direct loss in sales revenue to business** such as the revenue that a business would have received if the supply of electricity did not fail. It is therefore the integrated difference between the projected 'no-disaster' trajectory and the trajectory defined by the scenario where electricity fails. This value varies greatly by sector and from one business to the next and depends on how the firm is structured; the goods and services it provides; how dependent it is on electricity under normal operating conditions; and, if the firm has backup electricity supply systems in place.
- **Indirect losses through value chains** such as the losses upstream and downstream caused by direct interruption to production activities. Downstream economic loss concerns the impacts on businesses located "downstream" of those impacted by electricity failure. These upstream businesses may not be directly impacted by electricity failure. Unsupplied electricity will prevent goods and services from being produced and therefore lead to losses downstream in the supply chain.
- **Losses resulting from upstream impacts** such as those losses to businesses who supply goods and services to business that are impacted by electricity failure. A business rendered unproductive by power loss does not have a demand for further inputs and therefore does not purchase goods and services from businesses located upstream. When upstream and downstream supply chain interruptions are included in economic loss estimates the losses can be significant. Kelly et al. (2015) estimates the relative importance of backward and forward linkages in estimating economic losses from infrastructure failure in the UK.
- **Long term economic effects** including the economically relevant changes in the behaviour of market participants as a result of perceived long-term changes in the level of supply-security. Part of these losses includes the choice of business location, the potential increase in prices due to an increased need for back-up facilities and customer churn due to unreliability regarding delivery deadlines. These effects are difficult to estimate and typically are not included in most economic estimates.

Simulating economic impacts

The economy suffers both supply and demand side shocks as a result of the rolling blackout attack. All of these factors have serious negative consequences on market confidence which is also modelled as a shock.

In the areas affected by electricity failure it is assumed that there is a 50% drop in labour productivity in those areas without electricity. Consumption also declines in these areas because businesses close and this has the effect of reducing foot traffic for the entire area. Exports and imports decline as a direct proportion to the volume of cargo going through Dover, Felixstowe and London for the duration of the electricity outage. Tourism levels are shocked as a direct proportion of the total number of passengers that cannot fly in or out of the six airports affected by the outage. The GEM is a national quarterly model so the relative size of each shock is estimated as a proportion of the population affected compared to the UK as a whole. Model inputs are provided in Table 8.

By applying these shocks to the Oxford GEM, we are able to derive estimates for the total UK 'GDP@Risk' under each scenario variant. The GDP@Risk captures the loss in economic output over a five year period and is estimated as the integrated difference between two curves, namely the business as usual scenario and the stress test scenario that is being applied. This is shown in Figure 18 for each of the scenario variants.

Scenario	Outage-Days	Labour shock	Consumption shock	Exports and imports shock	Tourism shock	Confidence shock
S1	10.5	-0.83%	-0.83%	-1.1%	**-2.8%**	**-2%**
S2	21	-2.02%	-2.02%	-6.0%	**-11.5%**	**-4%**
X1	42	-4.60%	-4.60%	-15.8%	**-23.0%**	**-6%**

Table 8: Macroeconomic shocks applied to the Oxford Economics Model at the national scale

These results suggest that although the initial shock on the economy is severe, it reverts to pre-shock equilibrium levels after about two years for the S1 scenario and four years for the X1 scenario. In the standard variant scenario (S2) when the crisis lasts for six weeks, the total expected GDP@Risk is £129 billion. If all goes well and the major impacts of this co-ordinated attack can be averted by well organised and fast response times, we still estimate a five year GDP@Risk of £49 billion. In the most extreme variant of this scenario we estimate a GDP@Risk of £442 billion.

It is important to note that these economic impacts are non-linear with respect to the size and duration of the outage. Even though the marginal cost of electricity failure decreases for direct losses as the length of the outage increases, the reverse is true for indirect losses. The marginal cost of indirect losses grows as the severity of the outage increases and the duration is extended across scenario variants.

In the more extreme variations of these scenarios the economy is slow to rebound to pre-disaster levels. For extended outages like in X1, businesses may relocate to other regions, market confidence will wane for several quarters, international competitiveness will drop, and investments from overseas will be diverted elsewhere. Table 9 shows a summary of the macroeconomic impacts caused by each variant of the scenario.

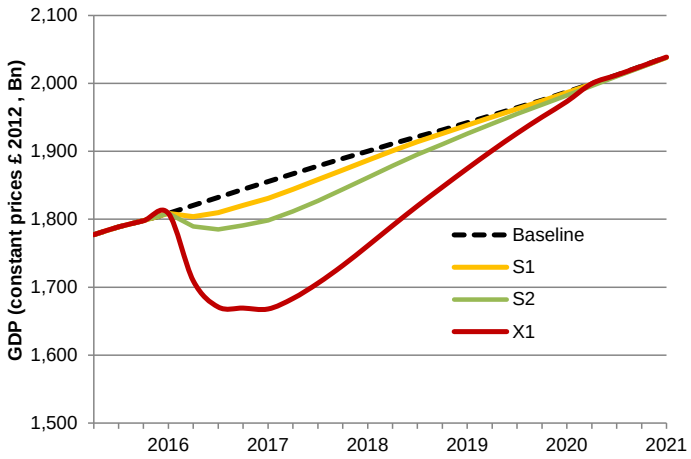

Figure 18: Domestic UK GDP@Risk under each scenario variant (from OEM modelling)

Table 9: Summary of macroeconomic losses, with sector losses for comparison.

Scenario Variants	Lost power (TWh)	Sector Direct Losses to Production (1 Yr) £ billion (from IO modelling)	Sector Indirect Losses to Supply Chains (1 Yr) £ billion (from IO modelling)	GDP@Risk to whole UK economy (5 Yr) £ billion (from OEM modelling)
S1	10.3	7.2	4.4	**49**
S2	19.8	18.0	10.9	**129**
X1	39.6	53.6	31.8	**442**

11 Overall Socio-economic Impacts on the UK

The impact to the UK is not solely confined to the direct costs to the electricity companies for unsold power but contains the diffuse effect of disrupted supply chains, psychological strain, and other secondary consequences on the UK's overall economic health. This chapter analyses both the direct and indirect socio-economic consequences resulting from systemic power-system failure.

Importance of London and the South East

Figure 19 shows the Gross Value Added (GVA) provided on a production basis for each economic region in the UK.

It is shown that the combined contribution from London, South East and East of England – the area directly impacted by the attack -- accounts for approximately 46% of total UK GVA. London alone represents almost one-quarter of total economic output. This underscores the significant economic impact that could result in the event of unscheduled and prolonged power outages across these regions.

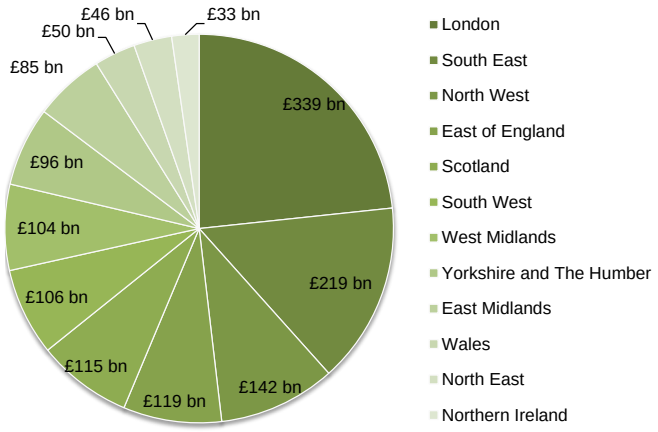

Figure 19: Economic output (GVA) at current basic prices production approach (£2012)

In Figure 20, we show economic output by broad industrial group for the London region. Financial and insurance activities are evidently the most important sector for economic output, closely followed by real-estate activities, professional and technical services, and information and communication technology.

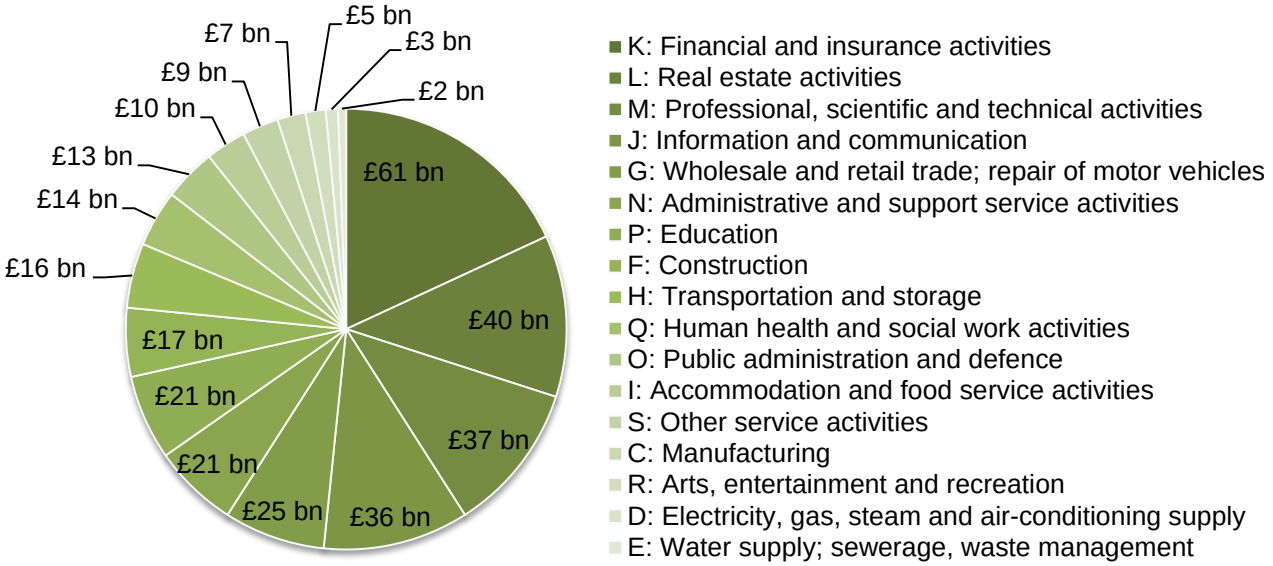

Figure 20: Economic output by sector for London region (£2012)

Table 10: Summary of direct impacts

Scenario	Length of campaign	Substations affected	Population without power	% UK population without power	Direct revenue losses	Peak customers disrupted per day	Peak customers disrupted per day
S1	3 weeks	65	8.9 m	13.8%	£7.2	7.8 m	9.6 m
S2	6 weeks	95	11.3 m	17.6%	£18.0	10.4 m	11.0 m
X1	12 weeks	125	13.1 m	20.2%	£53.6	11.8 m	12.6 m

Figure 21: Domestic and Non-Domestic electricity consumption by UK Region

Direct impacts on the electricity sector

Figure 21 shows the mean annual electricity consumption by UK region for domestic and non-domestic customers. The distinction between domestic and non-domestic electricity consumption is important because non-domestic electricity consumption has potential to cause much larger economic impact than domestic consumption. London not only consumes the most electricity but also has the highest share of non-domestic electricity consumption (68%) therefore placing a higher share of economic productivity at risk in the event of electricity failure.

Figure 22 shows the total amount of undelivered electricity in each region during the affected period and across each of the scenario variants.

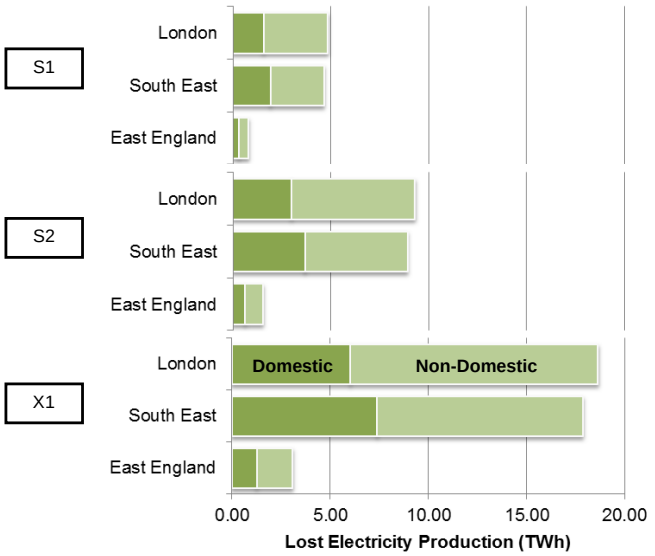

Figure 22: Lost electricity supply as a result of substation failure

Further economic consequences

Consumption

Although the first few days of the outage see an upturn in the rate of consumption due to panic buying, this effect is quickly overtaken by the far more disruptive impact of the failure of electronic payment. Cash quickly becomes the only accepted form of payment but the shortage of serviceable ATMs means that many citizens are unable to obtain paper money. As a consequence, consumption levels in the footprint of the blackout remain low until power returns.

It is assumed that a proportion of consumption (50%) is diverted to surrounding districts and neighbourhoods that still have power.

Panic buying takes place over the first week due to uncertainty over how long the outage event is likely to last. However, the rolling nature of the attack means that panic buying is both delayed and staggered by the fact that the power is regularly restored after a few hours.

Consumption over the medium and long-term is depressed as consumers are unable to use electronic payment systems to buy goods and services. Simultaneously, there is a lack of available goods and services to purchase due to the ongoing chaos. Supermarket shelves remain un-stocked in the attack area, but also across the country. Imported stock is unable to be distributed to the point of sale.

Production

The economic impact of power system failure on the production side of the economy has the potential to cause significant economic disruption. Electricity is a fundamental input required in the production of goods and services which are ultimately used in other sectors of the economy. Thus localised electricity failure has the potential to cause cascading effects throughout the whole economy due to economic interdependencies.

For example, the failure of a manufacturing facility will cause disruptions both upstream and downstream of the manufacturing supply chain disrupting businesses that depend on the intermediate products produced. In the financial services and insurance sector, the absence of power and communication means that financial transactions cannot be undertaken.

The power outage causes a decrease in business productivity as workplaces close and people are unable to get to work. Although some manufacturing and commercial facilities have backup generators, these typically provide only partial replacement and refuelling these generators may be impossible during an outage when electric gas pumps fail.

While some workers may be able to perform duties even without electricity, many, particularly in the cities, are unable to get to their place of employment due to the wider disruptive impact of the blackout on public transportation and gas stations. Table 10 lists the direct impacts on the UK caused by the initial power outage.

Secondary consequences across different sectors

Road Transport

Initially, there are widespread traffic problems due to signal failures. Both accidents and gridlock occur, especially in London. Tube stations close, adding to problems around the movement of the labour force. Some employees work from home but this only provides a short-term solution, even if these workers are fortunate enough to have power and a working Internet connection.

When news of the outage is broadcast there are predictions of fuel shortages by media channels akin to the 2012 fuel crisis and this induces mass panic buying of petrol as consumers attempt to stock up on fuel, unsure how long the blackouts will last. As rolling outages cause mass uncertainty around the ability to fill up vehicles with fuel, business and recreational travelling is widely postponed.

The UK relies on inland freight transport and logistics to move goods around the country as efficiently as possible. In this crisis, freight companies are forced to reassess distribution networks and ensure their fleet is able to be refuelled. This prompts some freight companies to temporarily relocate and purchase additional fuel and generators to ensure their business can remain operational. This adds additional expense to the cost of doing business causing prices to rise.

Railways and Underground

Large sections of the London Underground are shut down permanently due to the unpredictability of further blackouts and concern for the safety of passengers. Some parts of the London railway network remain operational but large sections of Central London and the South East are left isolated. This has a huge psychological effect on the population and prevents many people from getting to work or going about their daily business. The additional passengers travelling by bus and car add further congestion to the roads more than tripling the average length of travel time.

Air Travel

The UK economy is highly reliant upon the movement of people for both business and tourism. Aside from merely ferrying passengers, flights also facilitate

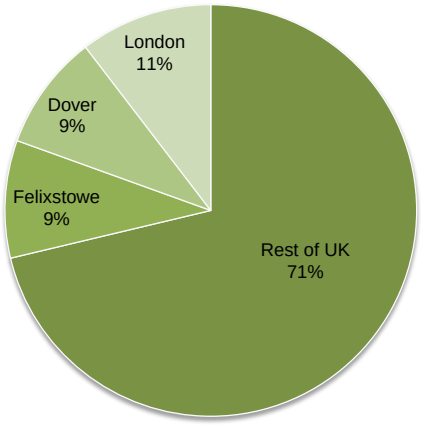

Figure 23: UK Port traffic as percentage of total tonnage

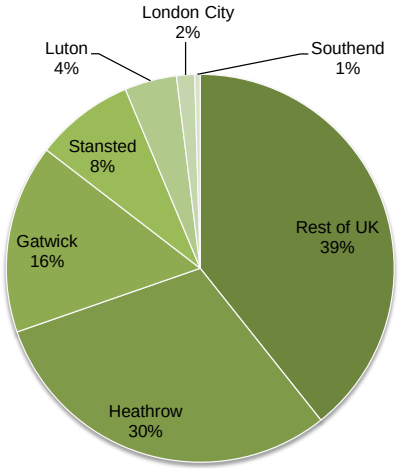

Figure 24: UK airports by total number of passengers

the transport of high value goods and time-critical products. The closure of just one airport for several days could lead to chaos, triggering a breakdown in the supply chain of high value products, harm international relations and lose business to international competitors.

The region affected by this electricity outage is home to six international airports that service over 60% of UK passenger flights. Heathrow is the largest airport carrying 73.4m passengers per year, this is followed by Gatwick (38 million), Stansted (20 million), Luton (10 million), London City (3.6 million) and Southend (1.1 million).

Outbound and transfer passengers are stranded at airports due to the loss of power. Security systems cannot be operated as a consequence and planes are unable to be refuelled. Many flights are diverted away from airports in the attack zone, and many passengers choose to fly or transfer via other destinations. Over the long-term the number of planned flights through UK airports diminishes as both companies and passengers decide to fly via more reliable destinations.

Tourism is especially affected as international travellers reroute to other major tourist destinations. Domestic tourism drops significantly as all unnecessary travel is postponed due to worries over fuel shortages. The sector gets a minor boost part the way through the campaign as people relocate to other seemingly unaffected regions.

Ports, International Trade and Supply Chain Disruption

The UK economy is dependent on international trade for imports and exports. The ports within the attack zone represent almost a third of total trade volume by tonnage for the UK. Felixstowe port is strategically very important as it is the UK's largest container port, moving over 3.72 million containers per year. It is also the largest and busiest container port in the UK representing over 40% of all UK Lo-Lo (load-on, load-off) container traffic.

The port at Dover is the busiest passenger port and the largest port in the UK for Ro-Ro (roll-on, roll-off) traffic. London Port also accounts for 10% of non-oil and gas traffic, and 10% of the UK's load-on-load-off container shipping.

The loss of electrical power at ports in the attack zone, including Felixstowe and London, lead to an accumulated disruption of 215,956 tonnes of cargo per day. Shutting down any one of these ports causes an economic shock that sends ripples through supply chains across the entire UK and beyond. Supermarket shelves would be left empty and a backlog of products would remain idle on ships and in the docks. Figure 25 shows the proportion of UK cargo by type affected by the electricity outage.

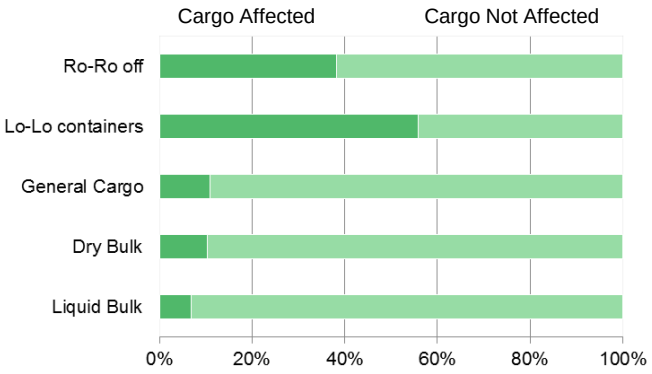

Figure 25: Type of cargo affected by electricity failure

As a consequence of the power outage UK businesses are unable to ship their goods to European and global consumers, having long-term detrimental effects on the economy with the prospect of losing future business.

The secondary consequences of a port disruption mean that exports are not shipped creating a backlog of cargo that sits idle on the docks. This delays the process of invoicing and receiving payments potentially causing cash flow problems, eventually leading to some business failures. Over the medium-term container ship cargo is rerouted to other ports such as Grimsby, Southampton and Liverpool but they, too, struggle to cope with the extra demand for containerised load-on-load-off cargo.

Even after the rolling blackouts cease, it takes some time to remove the backlog of cargo waiting to be shipped. Moreover, the behavioural effects associated with catastrophes can have lingering and harmful consequences well after the initial shock of the campaign has subsided. Research has shown that these behavioural effects can cause more significant losses to GDP than the immediate direct economic losses from the disaster (Giesecke et al. 2015).

Communications

Digital communications display strong resilience in the initial part of the campaign thanks to backup generator capacity and dependence on packet switching technology, although this resilience decreases throughout the campaign. Mobile connectivity becomes patchy with a peak of 8.6 million customers disrupted per day. Fixed connectivity is also intermittent.

As all users in an area are forced to use only one method of connecting to the Internet it causes the access network to become saturated. Fixed lines are slow when mobile connectivity is not operational. Equally, when fixed broadband fails, if the 3G/4G network is operational in an area, then it rapidly slows as users tether their devices via their Smartphone.

Data centre resilience problems proliferate causing some content, applications and services to become temporarily inoperable globally, not just in the UK. Even in those data centres which have a large degree of redundancy (multiple geographically dispersed backup operations), users can lose recent work as remote servers are not always updated in real time. Emergency contact numbers remain in use, but some emergency call centres intermittently lose power, slowing the response. The BBC headquarters, located in London, suffer throughout the rolling blackouts forcing several channels to go into automation mode.

Information and communication technology (ICT) is a core activity and a significant contributor to value-added in the economy. All sectors rely on some form of ICT, particularly finance, services and retail. Most sectors depend on electronic financial transactions, email and the Internet for commercial activity.

All these systems fail to work in the event of electricity failure, forcing these businesses to either shut down or find alternative methods of communication. Communication failure makes it very difficult for responders to know which areas are affected and therefore where to prioritise resources. This prolongs the economic disruption.

Water Supply and Waste Water

Water supplies are shut off during the blackout due to the loss of power to pumps. Supplies of potable water become extremely low, prompting the government to make daily water deliveries in the areas affected. Several accidental spills occur from sewage plants suffering power outages, leading to further contamination of the water supply. Malfunctioning and over-flowing sanitary systems force many businesses to shut down due to health concerns.

Finance

The City of London is one of the major financial hubs of the world, where, on a typical day, £5 billion in assets are traded on the London Stock Exchange. Any disruption to the London financial markets will cause turmoil in financial markets around the world. There is panic selling of Sterling and a long-term decline in net purchase of British assets by foreign buyers. Under normal business conditions the UK is responsible for over one third of global foreign exchange trading, but this share steadily decreases during the campaign. As the UK's financial payments systems are out of action there is an immediate and long-term loss of confidence in the UK as a point of financial intermediation, leading to financial capital being redirected to other global financial centres. Many financial institutions are badly affected as a result including insurance companies, pension funds, and investment and commercial banks.

As a consequence of the outage, insurance companies pay out billions in business interruption (service interruption) expenses to cover lost revenues induced from diminished production and consumption. During the attacks, the London Stock Exchange, along with other financial brokerage houses and banks, ceases to operate. London commodities exchanges operate intermittently, hampering the sale and exchange of raw materials, metals and other goods.

Public health

Public health is severely affected during the outage. Although no public deaths occur directly from the cyber attack scenario, a considerable number of deaths occur indirectly. The loss of power during the harsh winter months has the most notable effect on the elderly and vulnerable population.

Estimates show that there are already roughly 40,000 extra deaths between December and March in Britain due to excess cold.[35] The loss of heating to thousands of homes increases this number dramatically as many of the elderly and vulnerable die as a result of the cold. Additionally, this causes significant psychological stress on the affected population due to the extreme conditions that are being endured. Emergency services are overwhelmed by the number of traffic and industrial accidents that take place as a result of no road signals and other electronic safety systems.

Due to the large number of customers frequently experiencing limited potable water in the attack zone there is an increase in the number of infectious diseases, particularly in elderly and vulnerable groups, due to the consumption of improperly treated water. Moreover, waste water from millions of customers is unable to be properly processed. Much of this flows into natural watercourses but, in some circumstances where sewage systems rely on electrical pumps, this overflows into streets and into people's homes. This leakage of hazardous waste water within urban environments affects homes and places of work. Cross contamination leads to an increase in the number of infectious diseases. Many businesses are forced to close due to improper sanitation. Environmental Health services are unable to operate effectively, as the Health Protection Agency laboratories are unable to process any bacterial or viral samples to help in tracking down key sources of infection.

Other effects

Outbreaks of looting and stealing occur as the outage drags on, with criminals exploiting the lack of lighting and security systems coupled with overstretched police forces. Looting begins as people run low on food and water and become increasingly frustrated. By the second week without power, many communities suffer a general sense of social unrest, with many people choosing not to go out after dark.

As the power outage continues to deny basic services, social unrest increases. Health and safety suffers owing to factors such as contaminated water and food supplies, difficulties in using at-home healthcare equipment or securing repeat prescriptions, added noise and air pollution from generators, increased physical exertion and poor emergency response. These factors all contribute to a higher death rate in periods of power outage.[36]

---

[35] National Federation of Operational Pensioners, "Winter death toll to exceed 40,000", *The Telegraph*, 1 February 2015

[36] C. Klinger, O. Landeg, V. Murray, "Power Outages, Extreme Events and Health: a Systematic Review of the Literature from 2011-2012." PLOS Currents Disasters, Ed. 1, January 2 2014.

12 Conclusion

This report has proposed an unlikely yet plausible cyber attack on UK critical national infrastructure via the electricity distribution network and considered the costs to attacker, defenders and society as a whole.

This scenario illustrates that IT departments and industrial security teams need to share information and threat assessments to guard against weak points such as critical substations, which this report focussed on rather than the more obvious control rooms. Given the complexity of power distribution networks and the reliance on electricity infrastructure to deliver essential citizen services, the public may demand evidence of such sharing and assessments. It will be necessary to report near misses and not let unexplained security breaches or missed assessments go unresolved.

Cyber and physical security planning done in silos cannot reconcile the systemic vulnerabilities of an interdependent national infrastructure particularly as natural resources, power, transportation and other aspects of daily life become more integrated in a digital network environment. The macroeconomic impact of an isolated incident does not remain isolated, but affects multiple sectors in a multitude of ways.

Business and government stakeholders must recognise the true costs of an extreme cyber attack and the risk of an erosion of public trust, and allocate resources accordingly.

The scenario primarily involves an attack on operational technology rather than information technology. Security cultures vary between IT and OT and often these cultures don't get along. OT has a traditional engineering safety culture involving long lead times and arguably denial that this kind of attack can happen; whereas IT is more familiar with cyber attacks, more nimble and able to apply security patches rapidly if required. It will take years to remove vulnerabilities in OT equipment.

Society needs to address the issue of how return on investment (ROI) is calculated for OT cyber security measures. With such a small history of OT attacks, individual organisations can find it difficult to justify investment in cyber security using traditional ROI thinking. Governments do not own the infrastructure – companies do, yet the public will look to governments in scenarios like the one in this report. Thought leadership is needed from governments and regulators to change the mentality of how resources are allocated to OT cyber security to benefit society as a whole.

13 References

Allan, D., "Fire and Explosions in Substations", Transmission and Distribution Conference and Exhibition 2002: Asia Pacific. IEEE/PES (Volume:1), pages pp 504-507.

Anderson, Christopher W., Joost R. Santos, and Yacov Y. Haimes. 2007. "A Risk-Based Input–Output Methodology for Measuring the Effects of the August 2003 Northeast Blackout." *Economic Systems Research* 19 (2): 183–204. doi:10.1080/09535310701330233.

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

Cherepanov, Anton, "BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry", *WeLiveSecurity*, 3 January 2016. Online: http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/

DeMarco, C., J. Sarlashkar and F. Alvarado, "The Potential For Malicious Control In A Competitive Power Systems Environment", The 1996 IEEE International Conference on Control Applications (Dearborn, MI, USA), pages pp 462-467.

Dietzenbacher, Erik, and Ronald E. Miller. 2015. "Reflections on the Inoperability Input–Output Model." *Economic Systems Research* 27 (4): 478–86. doi:10.1080/09535314.2015.1052375.

F-Secure Labs, "BlackEnergy & Quedagh", Malware Analysis Whitepaper. Online: https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf

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

Ghosh, A., 1958. Input-Output Approach in an Allocation System. *Economica*, 25(97), p.58–64. Available at: DOI:10.2307/2550694.

Goetz, E. a. (2008). Lessons Learned from the Maroochy Water Breach. In J. a. Slay, Critical Infrastructure Protection V 253. Springer.

Haimes, Y, and P Jiang. 2001. "Leontief-Based Model of Risk in Complex Interconnected Infrastructures." *Journal of Infrastructure Systems* 7 (1): 1–12. doi:10.1061/(ASCE)1076-0342(2001)7:1(1).

Hawrylak, P., M. Haney, M. Pap and J. Hale. "Using Hybrid Attack Graphs to Model Cyber-Physical Attacks in the Smart Grid", 5th International Symposium on Resilient Control Systems (ISRCS), 2012, pages pp 161-164.

Hilt, S. (2014, February 3). PLCpwn. Retrieved July 22, 2015, from Digital Bond: http://www.digitalbond.com/blog/2014/02/03/s4x14-video-stephen-hilt-on-plcpwn/

Kaspersky Lab Global Research and Analysis Team, "Energetic Bear – Crouching Yeti." https://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf [Accessed: Oct 2015]

Kelly, S., 2015. Estimating economic loss from cascading infrastructure failure: a perspective on modelling interdependency. *Infrastructure Complexity*, 2(1), p.7. Available at: DOI:10.1186/s40551-015-0010-y.

Kelly, S., Tyler, P. and Crawford-Brown, D., 2015. Exploring Vulnerability and Interdependency of UK Infrastructure Using Key-Linkages Analysis. *Networks and Spatial Economics*. Available at: DOI:10.1007/s11067-015-9302-x [Accessed September 22, 2015].

Knapton, S. (2008, December 11). *Power station break-in sparks security review*. Retrieved 04 28, 2015, from *The Telegraph*: http://www.telegraph.co.uk/news/uknews/3705073/Power-station-break-in-sparks-security-review.html

Kravets, D. (2009, 3 18). *USA v Mario Azar*. Retrieved 04 28, 2015, from Wired: http://www.wired.com/images_blogs/threatlevel/files/azar.pdf

Leahy, Eimear, and Richard S. J. Tol. 2011. "An Estimate of the Value of Lost Load for Ireland." *Energy Policy* 39 (3): 1514–20. doi:10.1016/j.enpol.2010.12.025.

Lee, Robert M., "Potential Sample", SANS Industrial Control Systems Security Blog, 1 January 2016. Online: https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered

Leung, M., Haimes, Y. and Santos, J., 2007. Supply- and Output-Side Extensions to the Inoperability Input-Output Model for Interdependent Infrastructures. *Journal of Infrastructure Systems*, 13(4), p.299–310. Available at: DOI:10.1061/(ASCE)1076-0342(2007)13:4(299).

Liu, S., B. Chen, T. Zourntos, D. Kundur and K. Butler-Purry, "A Coordinated Multi-Switch Attack for Cascading Failures in Smart Grid", IEEE Transaction on Smart Grid (2014) 5.3 pages pp 1183-1195.

Lipovsky, Robert, "BlackEnergy trojan strikes again: Attacks Ukranian electric power industry", *WeLiveSecurity*, 4 January 2016. Online: http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/

London Economics, 2013. *The Value of Lost Load (VOLL) for Electricity in Great Britain*. OFGEM DECC. Technical report. Available at: https://www.ofgem.gov.uk/ofgem-publications/82293/london-economics-value-lost-load-electricity-gb.pdf [Accessed June 24, 2015].

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

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

Miller, R.E. and Blair, P.D., 2009. *Input-Output Analysis Foundations and Extensions.*, Leiden: Cambridge University Press. Available at: http://public.eblib.com/EBLPublic/PublicView.do?ptiID=451919 [Accessed November 21, 2012].

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

Nigam, Ruchna, "Havex meet OPC server," *Fortinent*, 15 July 2014, Retrieved 9 November 2015, from blog.fortinet.com: https://blog.fortinet.com/post/havex-meet-opc-server

de Nooij, Michiel, Carl Koopmans, and Carlijn Bijvoet. 2007. "The Value of Supply Security: The Costs of Power Interruptions: Economic Input for Damage Reduction and Investment in Networks." *Energy Economics* 29 (2): 277–95. doi:10.1016/j.eneco.2006.05.022.

Pant, R., Hall, J.W., Barr, S., & Alderson, D. (2014). *Spatial Risk Analysis of Interdependent Infrastructure Networks Subjected to Extreme Hazards. Vulnerability, Uncertainty and Risk*, pp. 677-686. DOI http://ascelibrary.org/doi/abs/10.1061/9780784413609.069.

Pant, R., Hall, J.W., Blainey, S.P. (2016). "Vulnerability assessment framework for interdependent critical infrastructures: case-study for Great Britain's railway network", *European Journal of Transport and Infrastructure Research*, 16(1), 174-194, ISSN:1567-7141.

Poudineh, R., and T. Jamasb. 2015. "Electricity Supply Interruptions : Sectoral Interdependencies and the Cost of Energy Not Served for the Scottish Economy." *Energy Journal*, October 2015. http://www.iaee.org/en/publications/ejindex.aspx.

Power Pwn. (n.d.). Retrieved July 22, 2015, from pwnieexpress: https://www.pwnieexpress.com/product/pwn-power/

Rid, T. (2013). *Cyber war will not take place*. London: Hurst & Company.

Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K., 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, 21(6), p.11–25. Available at: DOI:10.1109/37.969131.

Santos, J.R. and Haimes, Y.Y., 2004. Modeling the Demand Reduction Input-Output (I-O) Inoperability Due to Terrorism of Interconnected Infrastructures. *Risk Analysis: An International Journal*, 24(6), p.1437–1451. Available at: DOI:10.1111/j.0272-4332.2004.00540.x.

Santos, Joost R., Kash Barker, and Paul J. Zelinke Iv. 2008. "Sequential Decision-Making in Interdependent Sectors with Multiobjective Inoperability Decision Trees: Application to Biofuel Subsidy Analysis." *Economic Systems Research* 20 (1): 29–56. doi:10.1080/09535310801890672.

Shivaraj, G., Song, M., & Shetty, S. (2008). A Hidden Markov Model based approach to detect Rogue Access Points,. IEEE Military Communications Conference, (pp. 1-7).

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.

Srivastava, A., T. Morris, T. Ernster, C. Vellaithurai, S. Pan, U. Adhikari. "Modelling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information", IEEE Transaction on Smart Grid (2013) 4.1, pages pp 235-244.

Stamp, Jason; John Dillinger, and Willian Young (2003). *Common Vulnerabilities in Critical Infrastructure*. Albuquerque: Sandia National Laboratories .

Subcommittee on Economic and Subcommittee on Emergency (2005). SCADA Systems and the Terrorist Threat: Protecting the Nation's Critical Control Systems; Washington DC.

Symantec, "Dragonfly: Cyberespionage Attacks Against Energy Suppliers", 7 July 2014. Symantec Security Response, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf [Accessed: Dec 2015]

Thacker, S., Pant R., and Hall, J. W. (2016). System-of-Systems Formulation and Disruption Analysis for Multi-Scale Critical National Infrastructures. *Reliability Engineering and System Safety*. In Review.

van der Welle, A. and van der Zwaan, B., 2007. An overview of selected studies on the value of lost load (VOLL). *Energy Research Centre of the Netherlands (ECN)*. Available at: http://www.transust.org/workplan/papers/wp2_task_5_lost_load.pdf [Accessed July 21, 2015].

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

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

Appendix A: Catalogue of major ICS cyber events from 1999 through to 2014 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 on 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 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, SUBCOMMITTEE ON ECONOMIC, and SUBCOMMITTEE 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. An estimated $14 million in downtime costs.		Spyware Installation	Zotob Worm and MS05-039 Plug-n-Play	Infection
Aug 2006 (Wilshusen, 2007)	**Brown's Ferry**	Loss of recirculation flow on a US nuclear reactor down for maintenance caused a manual scram. A worm exploited a buffer overflow flaw in the widely used MSSQL server during the scram.		Unknown	Slammer Worm and Buffer Overflow	Non-ICS Targets

Date	Event Name	Detailed Description	Actors	Motivation	Methodology	Outcome
Oct 2006 (Wilshusen, 2007)	**Harrisburg**	Hackers gained access to a water treatment plant through an infected laptop.	Targeted Threat Agent	Mischief	Compromised Laptop	Setup a cheap server to run online games
Jan 2008 (Maras, 2012)	**Lodz**	Attacker built a remote control device to control trains and tracks through distributed field devices. Four trains were derailed with zero deaths. A disgruntled employee installed malicious code on a canal control system.	Targeted Threat Actor, Accident or Insider Attack	Mischief	Altered Universal Remote	Mayhem, Criminal Damage
Jan 2008 (Knapton, 2008)	**Kingsnorth**	Attacker broke into the EON Kingsnorth power station which caused a 500MW turbine to take 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 off shore 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. A recently fired employee disarmed safety alarms on three off-shore platforms.	Virus	Unknown, presumed nation state	Destroying centrifuges and thwarting uranium enrichment	Revenge & Sabotage
2010 to Aug 2014 (Symantec, 2014) (Kaspersky, 2014)	**Dragonfly/ Havex/ Energetic Bear campaign**	A campaign against defense, aviation, and energy companies	RAT	Espionage	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	RAT	Unknown, presumed hacking group	Wiping 30000 machines of their data	Unknown
April 2013	**California Power Station**	Snipers fired at a California substation, knocking out 17 transformers.	Physical	Unknown	Destruction of substation oil tanks	Unknown

Appendix B: Table of wider societal impacts during scenario

Impact Summary

The overall impact of the scenario in terms of the UK Cabinet Office's National Risk Register 2015 is:

Levels of social disruption to people's daily lives			
	S1	**S2**	**X1**
	Widespread disruption to every aspect of people's daily lives.		
Energy			
	9 million customers affected	11 million customers affected	13 million customers affected
Food and Water			
	8 million customers suffer disruption to their fresh water supply	10 million customers suffer disruption to their fresh water supply	11 million customers suffer disruption to their fresh water supply
	Shortages in shops due to staff unable to get to work, no power to shops, supply chain failures including spoiling of chilled and frozen storage, closure of ports and transportation difficulties.		
Commuting Chaos			
	0.85 million passenger rail journeys disrupted per day	1 million passenger rail journeys disrupted per day	1 million passenger rail journeys disrupted per day
	London Underground shut down		
	Workforce unable to reach place of employment		
Airport Anarchy			
	150,289 passenger air journeys disrupted per day	150,289 passenger air journeys disrupted per day	330,242 passenger air journeys disrupted per day
	Passengers and airline companies reroute away from the UK.		
Community Disruption			
	Access to healthcare, social services and schools disrupted		
Petrol Panic			
	The British media induces a run on petrol stations over fear of shortages much like the 2012 fuel crisis.		
Container Crunch			
	76,200 tonnes of port freight disrupted per day	216,000 tonnes of port freight disrupted per day	287,000 tonnes of port freight disrupted per day
	Felixstowe Port shuts completely		
	British, European and global supply chain logistics disrupted.		
Digital Disarray			
	8.6 million customers disrupted	11.3 million customers disrupted	12.8 million customers disrupted
	Intermittent loss of mobile connectivity.		
	Intermittent loss of fixed broadband connections and commercial leased lines.		
	Mass movement to either fixed or mobile connectivity (depending on which is functional), leads to mass contention on the operable digital infrastructure.		
	Loss of some data centres, predominantly the smaller, less prepared facilities.		

Levels of social disruption to people's daily lives			
	S1	**S2**	**X1**
Economic harm			
Indirect and Direct Losses			
	£12 billion	£29 billion	£85 billion
5-Year GDP@Risk			
	£49 billion	£129 billion	£442 billion
	Depressed economic output, low consumption and damaged supply chains means the economy takes two years to recover to pre-disaster levels.		
	Britain drops over twenty places in the World Economic Forum's Global Competitiveness Report 2016, leaving it below China, Estonia and Puerto Rico.		
	Some firms have to implement large scale redundancies, in an attempt to bring their balance sheet losses under control.		
	Financial Services and the Retail and Wholesale sectors see the largest economic losses		
	Health and transportation are some of the critical infrastructure sectors which see the largest economic losses.		
	Components of the UK economy which have traditionally had competitive advantage lose out to other nations. Financial services firms move from the City of London to Frankfurt. Both air passengers and aviation companies' preference Paris Charles de Gaulle and Amsterdam Schiphol over Heathrow.		
The psychological impact			
	Widespread anxiety, particularly affecting the elderly and vulnerable.		
	Public confidence would be shaken in a similar way as after a major terrorism event, with the public becoming aware of the new possibilities of cyber as a means of attack on daily life.		
	The UK's ability to respond to other events is severely reduced: dealing with social unrest; protecting against Nation State recognisance and attack; Monitoring and preventing insider threats.		
Human cost attributed to emergency			
	This project did not quantify fatalities but they are likely to occur from: • Exposure to excess cold due to loss of power for gas & electric domestic heating. • Accidents of various sorts due to the loss of power.		
	This project did not quantify Illness or injury but these are likely to occur from: • Illness would increase due to lack of heating, hospitals would provide a reduced service despite having backup generators and priority access to fuel, and doctors surgeries would shut, or people unable to get to doctors due to lack of fuel.		

Research Project Team

Project Lead
Simon Ruffle, *Director of Technology Research and Innovation*

Project Contributors
Professor Daniel Ralph, *Academic Director*
Dr Michelle Tuveson, *Executive Director*
Dr Andrew Coburn, *Director of Advisory Board*
Dr Scott Kelly, *Senior Research Associate*
Dr Edward Oughton, *Senior Risk Researcher*
Eireann Leverett, *Senior Risk Researcher*
Dr Louise Pryor, *Senior Risk Researcher*
Ghita Kassara, *Risk Researcher*
Jennifer Copic, *Research Assistant*
Tamara Evan, *Research Assistant and Contributing Editor*

External Project Collaborators

Infrastructure Transitions Research Consortium, University of Oxford, http://www.itrc.org.uk/

Scott Thacker, *Infrastructure Systems Modeller*
Dr Raghav Pant, *Senior Postdoctoral Researcher - Infrastructure Risk Analyst*
Professor Jim W Hall, *Professor of Climate and Environmental Risks, Director of the Environmental Change Institute*

Cambridge Centre for Risk Studies
Website and Research Platform
http://risk.jbs.cam.ac.uk/

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.risk.jbs.cam.ac.uk

Join our LinkedIn group at
Cambridge Centre for Risk Studies

Follow us @Risk_Cambridge