Securitisation and the Role of the State in Delivering UK Cyber Security in a New-Medieval Cyberspace

Richard David Hallows

Thesis submitted for the degree of Doctor of Philosophy (PhD) to the School of Humanities in the University of Buckingham

Original submission May 2019

Revision submitted July 2020

Declaration of Originality

I hereby declare that my thesis entitled ***The Role of the State in Delivering UK Cyber Security: Securitisation and State Authority in a New-Medieval Cyberspace*** *is the result of my own work and includes nothing which is the outcome of work done in collaboration except as declared in the Preface and specified in the text, and is not substantially the same as any that I have submitted, or, is concurrently submitted for a degree or diploma or other qualification at the University of Buckingham or any other University or similar institution except as declared in the Preface and specified in the text. I further state that no substantial part of my thesis has already been submitted, or is concurrently submitted for any such degree, diploma, or other qualification at the University of Buckingham or any other University or similar institution except as declared in the Preface and specified in the text.*

Signature: *Date: 30/05/2020*

Abstract

Both the 2010 and the 2015 UK National Security Strategies identified threats from cyberspace as being among the most significant 'Tier One' threats to UK national security. These threats have been constructed as a threat to the state, a threat to the country's Critical National Infrastructure (CNI), a threat to future economic success and a threat to businesses and individual citizens. As a result, the response to this threat has historically been seen as being a shared responsibility with most potential victims of cyber-attack responsible for their own security and the UK state agencies operating as a source of advice and guidance to promote best practice in the private sector. A range of government departments, including the Cabinet Office, MI5 and GCHQ among others, have been responsible for the government's own cyber security. However, despite a budget allocation of £860 million for the 2010 – 2015 period, progress on reducing the frequency and cost of cyber-attacks was limited and the 2010 strategy for dealing with cyber security was widely seen as having failed.

This led to a new National Cyber Security Strategy (NCSS) in 2016 which indicated a significant change in approach, in particular with a more proactive role for the state through the formation of the National Cyber Security Centre (NCSC) and a £1.6 billion budget for cyber security between 2016 and 2021. However, cyber-attacks remain a significant issue for many organisations in both the public and private sector, and attacks such as the Wannacry ransomware/wiper attack, UK specific data breaches such as those witnessed in 2017 at Debenhams, Three, Wonga and ABTA, and breaches outside the UK that impacted UK citizens such as Equifax show that the frequency and impact of cyber security issues remain significant.

The underlying cause of the insecurity of cyberspace is reflected in the metaphorical description of cyberspace as the wild-west or as an ungoverned space. This is a result of cyberspace features such as anonymity, problematic attribution and a transnational nature that can limit the effective reach of law enforcement agencies. When these features are combined with an increasing societal and economic dependence on information technology

and mediated data, this increases the potential economic impact of disruption to these systems and enhances the value of the data for both legitimate and illegitimate purposes.

This thesis argues that cyberspace is not ungoverned, and that it is more accurate to consider cyberspace to be a New Medieval environment with multiple overlapping authorities. In fact, cyberspace has always been far from ungoverned, it is just differently governed from a realspace Westphalian nation state system. The thesis also argues that cyberspace is currently experiencing a 'Westphalian transformation' with the UK state (among many others) engaged in a process designed to assert its authority and impose state primacy in cyberspace. This assertion of state authority is being driven by an identifiable process of securitisation in response to the constructed existential threat posed by unchecked cyber-attacks by nation states and criminal enterprises. The Copenhagen School's securitisation theory has been used to inform an original analysis of key speech acts by state securitising actors that has highlighted the key elements of the securitisation processes at work. This has clearly shown the development of the securitisation discourse, and the importance of referent objects and audience in asserting the state's authority through the securitisation process.

Original qualitative data collected through in-depth semi-structured interviews with elite members of the cyber security community has provided insights to the key issues in cyber security that support the view that cyberspace has New Medieval characteristics. The interview data has also allowed for the construction of a view of the complexities of the cyberspace environment, the overlapping authorities of state and private sector organisations and some of the key issues that arise.

These issues are identified as being characteristic of a particularly complex form of policy problem referred to as a 'wicked problem'. An understanding of cyber security as a wicked problem may aid in the identification of future possible policy approaches for cyber security policy in the UK.

Table of Contents

List of Figures

List of Tables

Acknowledgments

There are a number of people who have been a significant help and support throughout this process. Firstly, my thanks to the staff as Buckingham University Centre for Security and Intelligence Studies, in particular my supervisor, Dr Julian Richards, but also Dr Bill Kappis whose research sessions were more useful than I think even he believed, and of course Professor Anthony Glees whose encouragement has always been appreciated.

Also, at the University I would like to thank the library staff who were able to locate increasingly eclectic sources without ever once questioning the logic of a simultaneous request for works on cyber security and Medieval state structures.

Secondly, the numerous anonymous individuals at trade shows, conferences and on-line fora who have spent time patiently explaining things to me and have been an important part of the process of forming the basis of this thesis. Particular thanks are also due to a number of ex-colleagues from Cable & Wireless and IBM who were willing to assist by pointing me at people who would be able to help as well as being good natured test subjects for survey and interview questions. Their honest and invaluable critiques helped to prevent several long journeys down unproductive rabbit holes.

It is worth noting that I found there to be a generosity of spirit in the cyber security community that is of huge benefit to anyone studying the subject. This generosity of spirit was most evident in the interview subjects, all of whom were generous with both their time and their knowledge, and without whom this project would not have been possible.

And finally, but certainly not least, my family who have always supported this project and given encouragement when needed and whose patience and forbearance have been essential to its completion.

Acronyms and Abbreviations

ACD	Active Cyber Defence
APT	Advanced Persistent Threat
ATM	Asynchronous Transfer Mode
AWS	Amazon Web Services
BGP	Border Gateway Protocol
C2	Command and Control
CA	Competent Authority (defined within NIS directive)
CCDCOE	Cooperative Cyber Defence Centre of Excellence (NATO)
CCITT	Consultative Committee for International Telephone and Telegraph
CESG	Communications-Electronics Security Group (part of GCHQ)
CIA	Central Intelligence Agency
CIA	Confidentiality, Integrity, Availability (the 'CIA Triad')
CiSP	Cyber Information Sharing Partnership (UK part of GCHQ)
CNA	Computer Network Attack
CNE	Computer Network Exploitation
CNI	Critical National Infrastructure
CSP	Communication Service Provider
DDOS	Distributed Denial of Service
DIME	Diplomacy Information Military Economic
DMARC	Domain-based Message Authentication Reporting & Conformance
DNS	Domain Name System
DPA	Data Protection Act
EFF	Electronic Frontier Foundation
FBI	Federal Bureau of Investigation
GCHQ	Government Communications Head Quarters
GDPR	General Data Protection Regulation (EU)
GPS	Global Positioning System
HCSEC	Huawei Cyber Security Evaluation Centre
HTTP	Hyper Text Transfer Protocol
HULK	HTTP Unbearable Load King
IA	Information Assurance
IBM	International Business Machines (US)
ICANN	Internet Corporation for Assigned Names and Numbers
ICO	Information Commissioners Office
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force

IGF	Internet Governance Forum
IoD	Institute of Directors
IoT	Internet of Things
IP	Internet Protocol
IPA	Investigatory Powers Act
IPS	Intrusion Prevention System
ISC	Intelligence and Security Committee
ISO	International Standards Organisation
ISP	Internet Service Provider
ISPA	Internet Service Provider Association
ITU	International Telecommunications Union
JTRIG	Joint Threat Research Intelligence Group (part of GCHQ)
LOIC	Low Orbit Ion Cannon
NAO	National Audit Office (UK)
NATO	North Atlantic Treaty Organisation
NCA	National Crime Agency
NCCU	National Cyber Crime Unit
NCSC	National Cyber Security Centre (UK part of GCHQ)
NCSS	National Cyber Security Strategy (UK)
NHS	National Health Service
NIS	Network and Information Security Directive
NIST	National Institute of Standards and Technology (US)
NSA	National Security Agency (USA)
NTAC	National Technical Assistance Centre (UK part of GCHQ)
OCSIA	Office of Cyber Security and Information Assurance (Cabinet Office)
OFCOM	Office of Communications (UK)
PDF	Portable Document Format
PIME	Political Informational Military Economic
PMC	Private Military Contractor
PMF	Private Military Firm
RFC	Request for Comment
RFID	Radio Frequency IDentification
RIPE	Réseaux IP Européens
RIR	Regional Internet Registry
ROV	Route Origin Validation
RPKI	Resource Public Key Infrastructure
SDH	Synchronous Digital Hierarchy
SDSR	Strategic Defence and Security Review
SIEM	Security Information and Event Management

SONET	Synchronous Optical NETworking
SS7	Signalling System N^{o} 7
TCP	Transmission Control Protocol
TLS	Transport Layer Security (Replacement for SSL)
UTM	Unified Threat Management
VPN	Virtual Private Network
WDM	Wave Division Multiplexing
WGIG	Working Group on Internet Governance (UN)
WSIS	World Summit on Information Security

1 Introduction

In June 2013, documents leaked by Edward Snowden revealed that the UK's GCHQ had targeted civilian telecommunications engineers working in Belgium in order to implant malware on the private sector owned and operated Belgacom network, causing millions of euros worth of damage (R. Gallagher, 2014; Gallagher, 2018). In 2016, Apple Computers Inc. refused to assist the FBI in breaking into the iPhone of one of those involved in the San Bernadino terror attack (Zetter, 2016). In 2007, BT started to deploy Chinese telecommunications equipment in the core of the Critical National Infrastructure of the UK communications network despite UK national security concerns over alleged links between the manufacturer (Huawei) and the Chinese state (ISC, 2013). In 2016, the National Cyber Security Strategy stated that "*Only Government can draw on the intelligence and other assets required to defend the country from the most sophisticated threats.*" (HMG, 2016, p. 27). In 2018 in response to the Meltdown and Spectre Intel vulnerabilities, the National Cyber Security Centre tweeted a recommendation that "*users follow advice from their device vendors, and install new updates as they become available*" (NCSC, 2018f) indicating that the defence of the UK from sophisticated cyber threats was dependant on the delivery of capabilities from private sector organisations.

The above examples serve to illuminate some of the many complexities in the relationship between state agencies and the private sector in relation to cyberspace in general, and cyber security in particular. These examples reflect the research problem this project aims to address which is why, despite being a known and well documented problem for many years, security in cyberspace remains such an intractable issue in particular in relation to the relative roles of the state and the private sector.

The UK cyber environment has been adopted as a case study for analysis of these issues. However, cyberspace is a global environment, and there is inevitably reference to international considerations and developments from outside the UK. Developments in other states (and the United States in particular) are often relevant to cyber developments in the UK.

This thesis provides an analysis of the UK cyber security environment, through the use of secondary sources, the theoretical frameworks of New Medievalism (Bull, 1977) the Copenhagen School's securitisation (Buzan, Waever and de Wilde, 1998) and Wicked Problems (Rittel and Webber, 1973), original qualitative data obtained from semi-structured interviews with practitioners in the cyber security industry, and an analysis of securitising speech acts between 2012 and 2017 from representatives of the UK state that show the securitisation processes at work in relation to UK cyberspace. This has enabled the identification of the key rhetorical components of a securitisation process and trace the most recent securitising moves designed to enable the development of the UK state's security infrastructure in cyberspace. This use of securitisation theory has enabled the clear identification of the threat being articulated, the referent objects of these threats and the exceptional measures being requested by the state to address the threat.

A cyberspace that operates to its own laws can be seen as a threat to the state when these laws do not conform to state based realspace norms. This includes the ability of cyber-criminals to operate outside the law, the extra-jurisdictional issues of cyber-attacks from outside the state, and the lack of effective regulatory control over content, resulting in issues both of decency and intellectual property theft. These are a challenge to the state in both a Weberian sense of contesting the state's monopoly on violence, and in terms of the reach of state law.

1.1 Research Question

This research project was inspired by the desire to understand the UK state's behaviour with respect to cyber security in the UK, and in particular regarding the relationship between the state and the private sector in the delivery of cyber security and associated issues such as the dependency of the state on the private sector to deliver national security. As such, the fundamental research question can be most succinctly phrased as "*What is the role of the state in delivering cyber security in the UK?*" This is particularly interesting for the research period (January 2016 – January 2018), as it included significant changes in state behaviour leading up to the 2016 National Cyber Security Strategy which saw a more assertive approach by state institutions, including the introduction of the NCSC as a component of GCHQ.

This project has developed a framework for understanding UK state cyber security actions within the research period based on an understanding of the nature of cyberspace as a New Medieval environment and the process of securitisation which has been used to enable this more assertive state behaviour. This theoretical framework was then used to inform the collection of qualitative data through interviews with private sector practitioners. This data was then subjected to an inductive thematic analysis which highlighted some key cyber security issues, and a deductive thematic analysis on the basis of wicked problem theory which showed that cyber security may be a wicked problem.

Initial research into the issue of state behaviour regarding cyber security showed that there were potentially a number of factors that made the state's role in delivering cyber security both different and more complex than in delivering realspace security which warranted further investigation.

The sub-questions that have been used to guide this research project were formulated over a period of twelve months, and more recently re-structured as part of the assessment process for the thesis. The overall research question concerning the role of the state in delivering cyber security was based on the identification of areas where state authority was not as clearly applied in cyberspace as in realspace, for example in controlling the sale of illegal items in online dark marketplaces. It was this observation that was behind an initial analysis that underpins the project that examined the differences between cyberspace and realspace especially in relation to the role of the state. This is covered in this thesis in the analysis of the key concept of cyberspace later in this introduction page 16 and through the analysis of cyber-sovereignty, cyber-governance and cyber power in the literature review contained in Chapter 4 Literature Review on page 93.

Barakso, Sabet and Schaffner's five characteristics of a good research question (Barakso, Sabet and Schaffner, 2014, pp. 39–41) were used to formulate the research question. These characteristics are, first, a good research question should be non-normative and answerable; second, it should generate some implications for understanding real-world problems; third, it should address a debate or puzzle in the literature; fourth, it is not overly broad, and fifth, it is not overly narrow.

The question "*What is the role of the state in delivering cyber security in the UK?*" meets these criteria. It is non-normative in that it asks "what is" rather than "what should be"; it is answerable, in that state actions can be identified and analysed and it generates implications for understanding the real world problem of delivering cyber security in the UK and the role of the state in that endeavour which remains an ongoing debate. The characteristic that provides the most risk for this study is that the question may be too broad. To resolve this, limitations have been applied in the research period, the application of specific theory, and the UK focus, all of which aim to constrain the breadth of the subject area without making the question too narrow.

During the initial period of exploratory research the issues of state authority and sovereignty were regularly referenced in the literature as key differences between realspace and cyberspace (for example Herrera, 2008), especially with respect to the overlapping authorities in cyberspace. This was, on occasion, accompanied by reference to Medieval power structures and feudalism (Schneier, 2013; Brenner, 2014) and calls for a "Cyber Westphalia" (Demchak and Dombrowski, 2011, 2014). Initial research into the idea of Medievalism in a twentieth century context pointed to the work of Hedley Bull who initially termed the phrase "*New Medievalism*" (Bull, 1977) and then to a more detailed analysis from Philip Cerny (Cerny, 1998). A combination of these two works provided a set of eleven characteristics that could be found in a New Medieval environment. The analysis of cyberspace in relation to those characteristics was potentially a means to provide a conceptual understanding of the state's authority in cyberspace based on the characteristics of a Medieval precedent with a greater level of analysis than in the existing use of Medieval metaphors. This was the basis for the question of whether New Medievalism could usefully provide a conceptual model for cyberspace.

It was already clear at this point in the project that the authority of the state in cyberspace was not as clear cut as in realspace due to the overlapping authorities, the importance of transnational actors, and issues of anonymity and attribution, among others. Again, within this initial period of environment scanning there were some striking public statements reported from state representatives concerning the importance of cyber security in a national security context, including perhaps most importantly those leading up to the issuance of a

prospectus for the National Cyber Security Centre (NCSC) and the 2016 NCSS which emphasised the national security threat from cyberspace and the intention to introduce a more assertive state level approach (for example Lomas, 2016a).

The identification of a wider range of public statements appeared to indicate that an almost textbook Copenhagen School process of securitisation (Buzan, Waever and de Wilde, 1998) was being followed. In the context of the state's role in delivering cyber security, this use of the securitisation process with its emphasis on security threats and exceptional actions was a highly appropriate framework for analysis of the state discourse on cyber security. This was the basis on which the second sub-question was defined.

As the research topic became more closely defined in the initial period of the project, there was an increased focus on how the state worked in conjunction with private sector organisations and the perceived failure of the 2011 Cyber Security Strategy. This iteration of a state led cyber security strategy had attempted to encourage and persuade the private sector to provide cyber security that would adequately protect the Critical National Infrastructure and other organisations that were key to the economic stability of the United Kingdom. As this analysis progressed it suggested that national level cyber security was an extraordinarily complex problem with many different characteristics that were typical of wicked problems. This was supported by existing literature that provided an analysis of cyber security as a wicked problem based on a subset of the wicked problem characteristics (Clemente, 2011) and literature that addressed other public policy issues (such as climate change) as wicked problems (Australian Public Service Commission, 2007). These factors indicated that a more thorough examination of the cyber security environment using a wicked problem framework would be a productive approach to include within the research project as a means to conceptually frame the problem of cyber security and the solutions being adopted by the state.

At this stage of the research process, there had been a number of public statements made by state agencies that showed a lack of confidence in the private sector to resolve cyber security issues (Levy, 2016a; Lomas, 2016a; Martin, 2016a). This lack of confidence was expressed in relation to organisations that were the potential targets of a cyber-attack not taking the issue seriously enough, the cyber security vendor community providing target organisations with

inadequate and over-hyped solutions, and key infrastructure providers not working quickly enough to solve key problems in the infrastructure that were enabling cyber-attacks.

These statements further reinforced the initial findings in relation to sub-question two concerning how the state was seeking to assert authority within cyberspace. However, these statements also made clear that there was a significant dependency on the private sector in the delivery of any effective national level of cyber security.

The desire to understand this cyber security based relationship between the private sector and the state in more detail was the basis for sub-question four and the empirical component of the project with qualitative data gathered from interviews with senior individuals within private sector organisations involved in the delivery of cyber security. The analysis of this data (in conjunction with a theoretical analysis) showed that cyber security could be considered as a wicked problem (which has potential ramifications for any policy approaches) as well as a number of other key themes concerning the relationship between the state and private sector in this area.

The specific sub-questions for the project were.

1. Given the overlapping authorities in cyberspace, can the concept of New Medievalism (as articulated by Hedley Bull and Philip Cerny) provide a useful model for understanding cyberspace?

   This question is important because realist state-centric approaches may not necessarily provide the best model to understand cyberspace. The use of a Medieval metaphor for cyberspace in existing literature (in relation to overlapping authorities) indicated that this may be a useful avenue for investigation. Cyberspace governance models do not directly reflect those that operate in realspace, and being able to understand the governance model that does operate in cyberspace offers a mechanism for understanding the environment that will, in part, determine the state's role in delivering cyber security.

2. In the context of overlapping authorities in cyberspace and the well documented potential for cyberspace to challenge concepts of state sovereignty, are there identifiable

ways in which states are asserting their authority in cyberspace? What do the speech acts leading up the 2016 introduction of the National Cyber Security Centre tell us about the state's approach to the delivery of cyber security in the UK?

This question is important because in a New Medieval environment in which the state operates as one of multiple overlapping authorities, it can be hypothesised that the state will look to assert the same level of realspace authority within cyberspace. Again, during the development of the research questions it became clear that a process of securitisation was underway in relation to cyberspace that was developing a narrative to justify greater state level authority within cyberspace. This question provides the link between the New Medieval cyberspace environment and the development of the state's role in delivering cyber security.

3. Given the complexity of cyber security, can it be considered a wicked problem and what does this mean for the UK's response?

Having identified the way in which the state's role is being developed and some of the key components of the state led National Cyber Security Strategy, a picture of the state's developing role in cyber security can be developed. In line with the view that any good research question should aim to generate implications for real-world problems this question becomes important in providing a theoretical framework for the analysis of the state's response to the cyber security policy problem in the UK and enabling an analysis of the potential for the success of the approach to cyber security in the UK.

4. In the context of the securitisation of UK cyberspace what can the views of the private sector tell us, concerning the delivery of cyber security and the state's engagement in its delivery in the UK?

Given the state's actions to assert greater authority in cyberspace in which the majority of the infrastructure is within the control of the private sector, it is important to understand the view of the private sector in relation to the state engagement in cyber security as a cooperative and collaborative approach to the issue will be required.

These sub-questions help to develop the approach to the overall question of the state's role in delivering cyber security by identifying the issues of the cyber environment that have been instrumental in determining the state's role to date, understanding how the state is seeking to change its security role in that environment, providing a framework for understanding the issues that will occur in addressing cyber security as a public policy issue, and finally identifying the issues that arise from the relationship of the state with the private sector as a key partner in delivering a secure cyberspace.

1.2 Structure of the Thesis

This thesis consists of nine chapters.

Chapter One is this introduction which includes the research questions and an overview of the main components of the research project, including the original contribution. This chapter also includes a discussion of some of the key concepts used in the thesis including whether cyberspace represents a different 'space' to the physical world.

Chapter Two covers the research methodology, including sources, and details of the thematic analysis approach used for both securitisation speech acts, and the original qualitative data collected from practitioner interviews.

Chapter Three provides a background to cyber security issues focusing on threats and vulnerabilities.

Chapter Four is the Literature Review which focuses on discussions concerning cyberspace and sovereignty, governance, cyber power and cyberspace and international relations (including New Medievalism and Regime Theory).

Chapter 5 describes cyberspace in the context of new Medievalism, showing how cyberspace exhibits the characteristics of a New Medieval environment. This directly addresses sub-question one in the research questions.

Chapter Six discusses the securitisation of cyberspace in the UK, using the Copenhagen School framework to provide an analysis of securitisation speech acts. This Chapter is supported by Appendix A which includes a breakdown of the content of all the identified securitisation speech acts, and Appendix F which includes a detailed example of the

thematic analysis coding of a speech act. This addresses sub questions two and three in the research questions.

Chapter Seven provides a theoretical analysis of cyber security as a wicked problem, identifying some of the key features of cyber security that display the characteristics of a wicked problems. This, in conjunction with Chapter Eight provides the basis for further research in defining solutions for cyber security specifically as a wicked problem.

Chapter Eight provides a thematic analysis of the qualitative data collected through semi structured interviews with cyber security practitioners. This includes these developed from an inductive analysis based on the data alone and a deductive analysis based on a coding defined by the characteristics of a wicked problem. This chapter is supported by Appendices C, D, and E which include examples of interview notes and pre-interview information provided to participants, and Appendices G, H and I which include details of the thematic coding of the interviews. This chapter addresses the fourth of the sub-questions in the research questions.

Chapter 9 includes the conclusions of the thesis and recommended areas for further study.

1.3 Thesis Overview

The first part of the argument in this thesis is that cyberspace can be identified as a New Medieval environment based on the characteristics of New Medievalism identified by Hedley Bull (Bull, 1977; Hoffman, 1986; Carr, 2017) and Philip Cerny (Cerny, 1998). The initial impetus for using New Medievalism as the basis for an analysis of cyberspace was this common thread of overlapping authorities in the characteristics of New Medievalism and cyberspace. In addition, Hedley Bull's emphasis on international "*society rather than system*" and the "*common interest and values, common rules and institutions"* which suggest it is not only state power that could enable the emergence of a society, but that "*…anarchy is compatible with society, because the state is not the only reason for obeying rules in society.*" (Hoffman, 1986, pp. 185–186).[1]

[1] There is some debate concerning whether cyberspace can be treated as distinct environment in this way, in part because of the physical attributes of cyberspace infrastructure and users who are located in a State controlled territorial realspace environment (Grabosky, 2001; Brenner, 2006; Cohen, 2007;

These insights were the starting point for a more detailed analysis of cyberspace applying the documented characteristics of New Medieval environment.

The second part of the argument in this thesis is that the UK state is actively trying to assert its authority in UK cyberspace beyond its existing regulatory and realspace capabilities. It is argued that this is being driven by a process of securitisation based on the articulation of the need for greater security both in terms of security in cyberspace and the impact of cyberspace on realspace national security. A narrative has been developed by UK state agencies that there is a risk to national security from cyberspace that can only be addressed by the state which has then led to a process of state capacity building to allow the security issue to be addressed.

This assertion of state authority in cyberspace is complicated by the dominant role played in cyberspace by private sector organisation such as infrastructure providers, Communications Service Providers (CSPs), software and hardware manufacturers and owners and operators of key security referent objects in the Critical National Infrastructure (CNI).

Many of these private sector organisations act as an alternative source of authority in cyberspace. As a result, almost any cyber security implementation at a national level requires the support or at least acquiescence of the private sector. This has been most recently witnessed in debates around restricting content on social media platforms (Bienkov, 2018) but also in the context of the discourse around infrastructure deployment, vulnerability management, and support for law enforcement as previously referenced.

A thematic analysis of securitisation speech acts by key UK state actors is a key part of this thesis. These speeches show a clear securitisation process at work and this thesis argues that this process is playing an important role in equipping the state with the capacity to compete for power in cyberspace with private sector authorities, and take a more central and assertive role in relation to the private sector operation of cyberspace.

Herrera, 2008; Sheldon, 2014), however, this does not prevent cyberspace being evaluated as a distinct environment due to its significantly different characteristics of anonymity, removal of distance, speed and the man-made nature of the cyber-environment.

The final theoretical element provides an analysis of cyber security issues in the context of the characteristics of a wicked problem (Rittel and Webber, 1973). It identifies findings from alternative applications of wicked problem theory to unrelated complex issues (such as food safety and post conflict reconstruction) that may help to identify policy approaches for successfully addressing the wicked problem of cyber security.

The final key component of this thesis is based on qualitative data gathered from a small number of in-depth semi-structured interviews with senior cyber security practitioners from the private sector. This data has been subjected to inductive and deductive thematic analysis used to construct an understanding of some of the key issues in relation to the delivery of cyber security and the relationship between the UK state and the private sector as well as to support the construction of cyber security as a 'wicked problem'.

1.4 The Significance of this Research

The UK Government has described the cyber threat as a Tier One risk to national security (HMG, 2015b, p. 85). The NCSS of 2016 identified the risks as being driven by "*the scale and dynamic nature of cyber threats, and our vulnerability and dependency*" (HMG, 2016, p. 13). These threats, vulnerabilities and ultimately the risks to national security that derive from cyberspace are key components in understanding the background to the role of the state in UK cyberspace. Given these threats identified by the state there is a need to understand the role the state has in securing against these threats.

The questions of the role of the state in cyber security and how the state and the private sector can best work together to provide security in cyberspace have inspired a debate that has consistently failed to reach a conclusion. This is despite the need for a partnership approach having been a significant part of the discourse for many years. However, the parameters for this partnership are generally undefined, due to the complexity of the relationship between the state and the private sector in cyberspace.

It is difficult to define which areas of cyber security should be a state concern and which should be within the control of the private sector, with related actions determined by private sector motivations. This is, in particular, an issue with regard to the Critical National Infrastructure (CNI), involving often privatised companies on whom the normal

continuation of day-to-day life could be seen as being dependant. The idea that a cyber-attack could be allowed to compromise the financial system, disable the communications infrastructure, ground air traffic, or disrupt food or fuel supplies has regularly been constructed as state level security concern (Clarke and Knake, 2010; Brenner, 2011; Cornish *et al.*, 2011; Rudner, 2013).

This has resulted in a situation where the definition of what is considered part of the CNI can be used to determine the extent of state influence. In the UK the 2016 NCSS extended the definition of the CNI to include a wide range of commercial organisations and extended the cyber security role of the state to include the CNI supply chain as well as CNI organisations directly, further extending the state's scope of influence (HMG, 2016, p. 40). Regulatory initiatives such as GDPR (NCSC, 2018c) and NIS (NCSC, 2018d) have since served to consolidate and normalise state involvement in these areas.

The state has a multi-faceted role in cyber security where it has as much interest in being able to develop tools to undermine cyber security in the name of national security as it does in maintaining cyber security. The use of cyberspace as a domain in which power can be projected in international relations has driven a requirement for offensive as well as defensive cyber capabilities (Belk and Noyes, 2012; Blitz, 2013; Peterson, 2013), which have in turn created the threat of cyber-war (Stone, 2012; McGraw, 2013). Even if these capabilities are never used by the state, it can be argued that their effect has been to weaken cyber security for their own citizens:

a) By the non-disclosure of vulnerabilities (so called 'vulnerability hoarding') which has the effect of patches not being developed as the manufacturer is unaware of the vulnerability and so other user groups are left exposed (Schneier, 2015, p. 171; Smith, 2017).

b) By the proliferation of state developed exploits for vulnerabilities to non-state actors through accidental loss or theft. The Wannacry malware was a good example of a state exploit being 'released into the wild' and utilised by non-state actors after its theft from an NSA contractor (CERT-EU, 2017).) When these offensive capabilities are used by the state, they have the characteristic

of 'proliferation by use' in that as soon as the malware or exploit is publicly known it can be reverse engineered or adapted for reuse. Stuxnet is a good example of this where elements of Stuxnet code and design philosophy were discovered in other malware variants, Duqu and Flame, followed by components of Flame found in Gauss malware, showing how there can be multiple iterations of proliferation of adapted exploits (Bencsáth *et al.*, 2012)

c) By the perceived need for state agencies to be able to break encryption of electronic communication systems through so called 'back-doors' and to be able to access communications devices (Schneier, 2015, pp. 141–2; Landau, 2017, pp. 91–96). Government statements have reflected both the importance of encryption as a means of protecting information and as a tool that is valuable to terrorists and can prevent the state from accessing information necessary for security purposes. This has led to the idea that somehow encryption is something that is only required by those who mean to do harm, with Home Secretary Amber Rudd reported as stating that 'real people' don't need encryption (Collins, 2017).

d) Associated with the encryption issue is the demand for social media and other online platforms to disclose information to the state and act on behalf of the state in the control of online information. This is difficult for online service providers who do not wish to be considered as publishers of content that is delivered via their services, but rather as a platform that is used by individuals to publish their own information. However, with their growth as a major source of news, the power that can be exerted through social media platforms has become a significant concern for the state, most clearly in terms of radicalisation and state level influence operations such as those suspected as being a factor in the 2016 US Presidential election (Allcott and Gentzkow, 2017; New York Times, 2018), or the Brexit referendum of the same year (Kahn, 2017).

The distinction between state and private sector can also be seen in the ongoing debate regarding how far a private entity can go in defending itself in cyberspace. A range of

options are available that include defensive actions (such as firewalls, anti-virus software and the like) through a spectrum of 'active defence' approaches that could include deceptive capabilities such as 'honeypots' and 'tar pits', through to the right for a private corporation to be able to retaliate against cyber-attackers through what is referred to as 'hacking back'.

This understanding is also important in relation to a number of situations where, (for example in relation to the Law of International Armed Conflict (LOIAC)) the actions of the state may potentially have implications for private sector organisations. For example, if a cyber-attack is launched by the UK across the British Telecom network, this has implications for the consideration of BT staff as 'active combatants' and so their status as a legitimate target for a retaliatory attack (Brenner and Clarke, 2010, 2014; Schmitt, 2012b; Dunlap, 2013; Beard, 2016). If a cyber-attack is an act of war, then, as UK state representatives have made clear, a kinetic response may be justified (Townsend, 2018).

The state also has a key role to play in establishing norms of behaviour in cyberspace. The Snowden releases revealed state behaviour that did not respect privacy rights, (Kirk, 2018), interfered with the supply chain integrity of cyber infrastructure (Belk and Noyes, 2012; Greenwald, 2014a; S. Gallagher, 2014; Schneier, 2015, pp. 143–144) , and engaged in state cyber-attacks on civilians (S. Gallagher, 2014; Gallagher, 2018)) in order to covertly access private systems. Western state behaviour that defines cyberspace as a domain for military exploitation and a medium for covert operations is unlikely to encourage constraint by other state actors, yet alone non-state actors with malign intent and private corporations who may wish to protect their interests.

By identifying the securitisation processes at work in the New Medieval environment of cyberspace this project adds to an understanding of state behaviour in cyberspace, and in particular about how the state coexists with the private sector to deliver cyber security.

1.5 The Original Contribution of this Research

The Purpose of this research project was to explore the role of the state and the relationship between the state and the private sector in delivering cyber security with particular focus on the inherent tensions in relation to national security requirements in cyberspace.

As the project developed it became clear that despite the public/private relationship being a well-documented and discussed issue, there remain many aspects that are constraining the successful delivery of cyber security. By adopting a unique theoretical view of cyberspace as a distinct New Medieval environment, understanding state engagement through the Copenhagen School's securitisation framework and incorporating insights from practitioner interviews, it was possible to bring a different perspective to these issues, in particular in relation to governance and management of a national cyber security environment. Further analysis was able to conceptually position these issues within a 'wicked problem' framework, and therefore identify approaches that could inform future policy. The research offers an original contribution to the subject of cyber security in four areas.

First, the identification of cyberspace as a New Medieval environment offers a new way of understanding cyber governance issues. New Medievalism has previously been applied to the "Digital World Economy" (Kobrin, 1999) as well as globalisation more generally (Slaughter, 1997; Cerny, 1998), but the interpretation of cyberspace as a New Medieval environment represents a unique analysis.

Second, the analysis of the key securitisation speech acts in the UK is an original analysis, using the very specific inputs of the public speeches by state agents. While securitisation theory itself has been used in the context of cyber security (Hansen and Nissenbaum, 2009; Georgieva, 2015; Munk, 2015) it has not been used in a UK context or to inform an analysis of the process of public utterances by state agents with responsibility for cyber security.

Third, the original data gathered from the semi-structured interviews has provided a unique collective perspective from cyber security leaders in the private sector.

Fourth, the analysis of cyber security as a wicked problem based on the original characteristics and definition formulated by Horst and Rittel is a new and unique analysis. There are prior works based on a subset of the wicked problem characteristics, and US and Canadian cyber security has previously been placed in a wicked problem context (Malone and Malone, 2013), but I would argue that these have not fully connected the underlying difficulties of cyber security solutions with the characteristics of wicked problems, nor do

they reflect the UK environment and the current level of social complexity following the 2016 NCSS.

Taken as a whole, this thesis provides a narrative that connects the implications of the nature of cyberspace as a New Medieval environment to the process of state securitisation and cyber security as a wicked problem. This shows the complex nature of the cyber security policy problems faced today and the issues involved in delivering solutions that require state, private sector and citizen engagement.

It is also hoped that this project will add to the policy focused literature on cyberspace and provide at least some raw material that will help to bridge a gap between technical and policy elements of the subject.

1.6 Key Concepts

There are several key concepts that require a level of understanding in order to be able to address this subject effectively, including what we mean when talking about cyberspace, cyber security and related concepts such as conflict, threat and attribution.

Cyberspace and realspace: The study of cyberspace is beset with multiple contested definitions for even the most fundamental of concepts. However, how some of these basic concepts are defined has a huge effect on any further analysis. For example, if cyber issues are defined as being contained within the virtual representation of cyberspace, that has very different implications for discussions of governance and sovereignty to a definition that includes physical components of cyberspace. Physical components are rooted in the physical, territorially governed world.

Creating a firm definition for cyberspace is recognised as difficult (Betz and Stevens, 2011 loc. 154) and there are many different available definitions. Some of this difficulty is because the etymology of the word 'cyberspace' has its origins in science fiction to describe a "*consensual hallucination*" (Gibson, 1984). This is not a particularly accurate or useful description of what is generally referred to as cyberspace today.

The word has continued in common usage. Much of its normative value has been derived from John Perry Barlow's "*Declaration of the Independence of Cyberspace*" (Barlow, 1996) which

firmly defines cyberspace as spatially independent from 'realspace'. This is a definition that Barlow continues to stand by, in particular "*That the Internet is a separate, global place without the physical boundaries that define states and give them their power.*" (Greenberg, 2016).

It is the spatial nature of cyberspace that is particularly important in determining the capability of states to influence cyberspace. Most of the metaphoric constructions of cyberspace are as a separate space to 'realspace' (Cohen, 2007). This is, in part, a reflection of the different attributes of cyberspace in relation to distance, anonymity, human behaviour and transaction friction, and in part a product of the early utopian visions of cyberspace. These attributes have a significant influence on how people behave in cyberspace (Aiken, 2016; Suler, 2016) as well as offering new threats and opportunities for both control and empowerment, and changing power relationships.

However, despite the unique attributes of cyberspace, the people who inhabit cyberspace are real, embodied users who also inhabit realspace, and the underlying technologies (cables, routers, switches etc.) that enable cyberspace are rooted in the physical world. While cyberspace may be separate from realspace it is also connected, and can be seen as "*...subsumed within an emerging networked space that is inhabited by real, embodied users and that is apprehended by experience.*" (Cohen, 2007, p. 255)

This concept of a 'networked space' is a potentially useful way of envisaging the confluence of the virtual world of cyberspace and the embodied, physical world of realspace. It is the existence of this area where the embodied world and the virtual world meet and where cyber actions have a real world effect that is of particular concern for the relationship between cyberspace and the state.

Militarily, cyberspace has been defined as a domain (US Department of Defense, 2011), in the same way as land, sea, and air are described as domains. The key difference for cyberspace is that it is a completely manmade environment (Betz and Stevens, 2011 loc 622). This definition of cyberspace as a domain has been described as an '*article of faith*' for the US Air Intelligence Agency (Hayden, 2016, p. 128) and is now also recognised by NATO (Minarik, 2016).

The Tallinn Manual from NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) also incorporates the physical and virtual elements of cyberspace in the definition "*The environment formed by physical and non-physical components, characterised by the use of computers and the electro magnetic spectrum, to store modify and exchange data using computer networks.*" (Schmitt, 2012b, p. 211)

There are also many other technology-based definitions of cyberspace. The UK Cabinet Office definition was "*Cyber space encompasses all forms of networked, digital activities; this includes the content of and actions conducted through digital networks*" (Cabinet Office, 2009) while other offerings include "*the networked system of microprocessors, mainframes, and basic computers that interact at the digital level*" (Valeriano and Maness, 2015) while the 2016 NCSS defines it as "*the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internet connected devices and embedded processors and controllers. It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept.*" (HMG, 2016, p. 75)

These definitions, however, do not reflect the full complexity of cyberspace in terms of the different elements required for its construction. Martin Libicki, defines a three layered structure consisting of the physical layer (wires, routers switches etc.) "*the foundation of cyberspace in the tangible world*" (Libicki, 2007, p. 8), the syntactic layer of information format and the control and instruction of the systems, and the semantic layer which contains the information meaningful to humans and connected devices. Libicki also refers to a fourth layer "*were it one day to exist*" which he refers to as the 'pragmatic layer' that relates to the purpose of a communication (Libicki, 2007, p. 240).

Alexander Klimburg uses a four layer model to represent cyberspace of physical (cables, switching technology etc.), logic (the coding layer that provides instruction for the physical layer), data (the information that is used within cyberspace), and social ("*the sum of human actions and aspirations that make the Internet and cyberspace what they are…*" (Klimburg, 2017a, pp. 28–29)). This is effectively Libicki's three layer model with the social layer riding on top of it. This fourth layer was derived in part from US Cyber Command's inclusion of people in its definitions of cyberspace. (Klimburg, 2017a, pp. 50–51) and is seen by Klimburg as particularly important in the context of cyber security in that "*….all questions about cyber*

security are essentially ones about human beings and human decision making - for good or ill." (Klimburg, 2017a, p. 51)

This layering is an important concept for any analysis of governance, power or control within cyberspace as "*conquest works differently at different layers*" (Libicki, 2007) and much of the complexity of state engagement in cyberspace originates in the different models of ownership, control and regulation that are applicable to the different layers.

Another key delimitation of cyberspace to consider is where the edges are: at what point cyberspace ends and realspace begins? It has been argued that cyberspace is different because "*…all other domains possess some form of integument: the sea has the shore; the air has the land; land has the sky; space has the upper edges of the atmosphere.*" and that as the semantic level interactions begin and end outside cyberspace "*…then the edge – if indeed there is one – is to be found in the cerebral cortex of the human brain…*" (Betz and Stevens, 2011 loc 2095).

This is potentially useful as it suggests that the 'people' are a part of cyberspace when they interact with the data and systems of cyberspace and supports the inclusion of people and processes within a definition of cyber security. The edge of cyberspace discussion is fundamental to determining the point at which cyberspace and realspace intersect, especially when activity in cyberspace can produce realspace effects – be that influencing public opinion during an election or physically destroying centrifuges in Iran.

A potentially useful construct comes from the cybercrime literature where the concepts of cyber-dependent crime (also referred to as 'pure cybercrime') and cyber-enabled crime are used to differentiate between actions that can only take place in cyberspace and actions where cyberspace is used to enable actions in the physical world (McGuire and Dowling, 2013). This same idea can be applied across other cyber threats and actions.

Unfortunately the spatial relationships in cyberspace are too complex (Cohen, 2007) to be fully covered in this thesis, but, even given the many definitions of cyberspace we can see that the following attributes are important in later discussions:

- It is a man-made 'constructed' environment (Betz and Stevens, 2011 loc 629; Klimburg, 2017a, p. 28).
- It is treated as a strategic domain in its own right (Betz and Stevens, 2011 loc 629).

- People behave differently in a cyber environment (Suler, 2016)
- It can change power relationships, for example by acting as a force multiplier, especially for non-state actors (Denmark and Mulvenon, 2010, p. 13)
- It reduces the social proximity of actors to zero for some interactions (Betz and Stevens, 2011 loc 2082)
- It has intangible borders (Betz and Stevens, 2011 loc 2134)
- It offers great speed of operations which can be further enhanced by associated automation (Brenner, 2007a)
- It offers a level of anonymity with associated difficulty in attribution of actions (Betz and Stevens, 2011 loc 1721; Schmidt and Cohen, 2013, p. 105; Klimburg, 2017a, pp. 190–191)
- It is different to 'realspace' in some respects, but physically a part of realspace in others
- It is not a synonym for the Internet (although the terms are often used interchangeably), but the Internet forms part of cyberspace
- The development of the technology proceeds at a faster pace than the capability of realspace states to regulate its use (Klimburg, 2017a, p. 5)

Important to this project is an understanding that there is sufficient evidence for cyberspace to be treated as a distinct environment to 'realspace' – while acknowledging coexistence and overlap. This would mean that any analysis of the role of the state in cyberspace may not necessarily reflect the same definition that would be accepted in realspace. This is supported by much of the literature which suggests that state power relations in cyberspace are different to those in realspace, suggesting that states "*…will have to practice two versions of their domestic and foreign policies – one for the physical 'real' world, and one for the virtual world that exists online. These policies may appear contradictory at times – governments might crack-down in one realm while allowing certain behaviour in another; they may go to war in cyberspace but maintain the peace in the physical world…*" (Schmidt and Cohen, 2013, p. 7)

Behaviours are different in cyberspace, because cyberspace is different to realspace, despite the points of intersection.

The significance of the non-spatial attributes of cyberspace has been described by Susan Brenner in relation to cyber-attribution as "*Cyberspace nullifies the influence of the three spatial dimensions that constrain action in the real-world and, in so doing, erodes the significance of place in attacker-attribution*" and with reference to military capabilities she states that "*Cyberspace operations do not take place in a physical place; instead, they involve activity that occurs in and through computer technology*" and that "*'cyberspace' denotes an experiential, rather than spatial, phenomenon*" (Brenner, 2013).

For Brenner, the non-spatial characteristic of cyberspace has consequences in relation to the lack of constraints relating to behaviour in cyberspace in terms of criminal and state level activity. This lack of normative constraints mirrors the findings of John Suler in relation to the behaviour of individuals in cyberspace (Suler, 2016). The fact that cyberspace is not a spatial phenomenon can also be seen as preventing spatial characteristics such as physical separation. Brenner again described cyberspace as "*…not a spatial phenomenon; it is an interactive overlay that eradicates the constraints of geography. The notion of separating war-space and civilian-space becomes meaningless in a context that has no boundaries, and consequently no way to prevent the two "spaces" from coinciding and interacting.*" Again, the consequences of its non-spatial nature are significant, and serve to make it quite different to realspace. As James Comey said when Head of the FBI "*There are no safe neighborhoods. All of us are neighbors [online]*" (Ackerman, 2013) again showing the lack of spatial differentiation and constraint that is the norm in realspace, this time in relation to cyber-crime.

This is one reason why the use of existing theory has been so limited in cyberspace. The attempts to engage realspace realist state based theories to explain relationships in cyberspace have been generally unsuccessful, and the application of realspace assumptions frequently prevents any useful analysis. The issue of the application of IR theory to cyberspace is discussed in section 4.5 *Cyberspace, International Relations and New Medievalism* on page 113.

Conflict: Conflict is a key element of the discourse relating to cyberspace, ranging from the contested constructions of cyber-war (Schreier, 2012; Stone, 2012; Rid, 2013; Green, 2015; Valeriano and Maness, 2015) and more general discussions of conflict in cyberspace (Healey, 2011, 2013; Friis and Ringsmose, 2016) that in most cases focus almost exclusively

on state conflict with a typical definition of cyber conflict being "*…the use of computational technologies for malevolent and destructive purposes to impact, change, or modify diplomatic or military interactions*" (Valeriano and Maness, 2015, p. 21).

However, these discussions are based on a restrictive (albeit at times undefined) state dominated view of conflict, regardless of whether it involved cyberspace or not. This is surprising given that cyberspace is often credited with enabling non-state actors and enhancing capabilities in asymmetric warfare (Perritt Jr., 1998; O'Connor, 2011; Lindsay, 2013; Rowland, Rice and Shenoi, 2014) and I would argue that a much wider and more inclusive definition of conflict is appropriate in cyberspace especially given the number and variety of areas of contention that exist.

There are many definitions of conflict to choose from, which extend the concept well beyond the limits of what can sensibly called 'war' and involving actors other than states[2] and significant debate as to what should be included within any discussion on the definition or nature of conflict (Gurr, 1980, p. 2).

For the purposes of this thesis conflict is used to describe situations where two or more parties (that could be a state, a non-state actor, or individuals) hold incompatible subject positions (Diez, Albert and Stetter, 2006, p. 565 cited in Pia and Diez, 2007). As described by Pia and Diez (Pia and Diez, 2007) this definition *"emphasises the opposition or incompatibility at the heart of the conflict, and initially leaves open the exact nature of these incompatibilities, i.e. whether they are between individuals, groups or societal positions; whether they rest in different interests or beliefs; or whether they have a material existence or come into being only through discourse."*(Pia and Diez, 2007)

Under this definition, there is no requirement for conflict to inevitably incorporate violence (physical or virtual).

[2] Conflict resolution specialist Ryan O'Connell lists 30 academic definitions at www.viaconflict.com (O'Connell, 2013)

In addition to the definition above, cyber conflict has been defined as "*When nations and non-state groups use offensive or defensive cyber capabilities to attack and defend and spy on each other typically for political or other national security purposes*" (Healey, 2013)

It is almost inevitable that, in particular in the International Relations field of study that there is a focus on the conflict between nation states. However, given the overlapping authorities in cyberspace, these are not the only (or even the most important) conflicts that can be studied in cyberspace, especially when inter-state conflicts in cyberspace may only be an extension of real-space conflict.

There are many other conflicts in cyberspace. Tim Wu refers to the *"…clear conflict between the desire to reap the economic benefits of the Internet on the one hand and the desire to regulate it on the other.*" (Wu, 1998) and other commentators regularly adopt a wider usage such as "*…conflicts between the ITU, the US, the global private sector, and ICANN over Internet Governance*" (Denardis and Musiani, 2014) and the French Yahoo Nazi memorabilia case has been described as an example of where the "*Internet can give rise to conflicts as a result of the clash of differing cultural, political, or legal norms or values…*" (Solum and Chung, 2003), and problems relating to different legal interpretations relating to cybercrime are referred to as "*…gaps and conflicts in national law…*" (Brenner and Clarke, 2005). None of these instances suggest an inter-state, military, or violent conflict which seems to provide the default consideration for many when considering cyber conflict.

Choucri uses the word conflict to describe three different areas of contention in cyberspace (Choucri, 2012a, pp. 126–127) which are firstly, contentions over the architecture of the internet and the management of cyberspace, secondly, conflicts in the pursuit of political advantage and economic gain and thirdly cyber threats to national security, stating that "*Each is about he struggle over the authoritative allocation of value and control over who seeks to get what, when, and how across a range of issue areas.*" (Choucri, 2012a, p. 126)

In relation to the contention over architecture and management of cyberspace Choucri cites cases including network neutrality and Lessig's 'Code is Law'. In relation to cyber conflict for political advantage and profit she includes state power for political control, cyber challenges to the state, competitive politics via cyber venues, and cyber-crime and cyber

espionage. In relation to cyber threats to national security Choucri cites the militarisation of cyberspace, cyber-warfare, cyber threats to infrastructure and cyber terrorism (Choucri, 2012a, p. 127).

In the cyber domain, with these characteristics, Choucri makes the case that traditional state-centric conceptions of conflict are of limited utility and *"traditional theory is particularly disadvantaged"* (Choucri, 2012a, p. 126). It is important that any discussion of conflict in cyberspace is able to engage with these different aspects of the issue, although it does require a more nuanced discussion, both conceptually and semantically, than the more straightforward emphasis on state conflict.

This thesis has required this more nuanced use of the word conflict that is appropriate in cyber related discussions that encompass conflicts of ideas and policy approaches, as well as many different group and individual actors outside the state.

Threat: The term 'threat' is another that is used in several different ways within the study of cyber security. Julian Richards argues that semantically "*…all threats have a potentially cyber dimension to them"* leading to the conclusion that "*...cyber security means security against a range of threats including crime, espionage, vandalism, activism and terrorism, as well as actual war and warfare-related activities.*" (Richards, 2014). This directly correlates cyber-threats with threats in the physical world, which is also reflected in much of the discourse from the UK's NCSC who refer to the 'hardly new' concepts of money, power and propaganda as the main threat motivations in cyberspace (Martin, 2016b). This approach is also supported by the "*old wine in new bottles*" view of cybercrime (Grabosky, 2001).

At a more conceptual level, threat has been described as "*…representations of danger that imply an agent with intent and capabilities*". This definition is then specifically in opposition to the idea of risk which is described as leading to "*…security practices that are about probabilities, prevention, future scenarios and management, as opposed to deterring adversaries or defending against or defeating identifiable and calculable threats.*" (Friis and Reichborn-Kennerud, 2016) This distinction is interesting, but perhaps not that useful in the real world, where cyber security encompasses both threat and risk management (as shown below with reference to the standards promoted by NIST). The distinction is perhaps useful in terms of securitisation

theory with security being when "*….an issue is presented as posing an existential threat to a designated referent object.*" (Buzan, Waever and de Wilde, 1998, p. 21) It is the language of threat rather than risk that is most prevalent in the cyber security discourse at a state level.

Susan Brenner limits a discussion of threats to crime, terrorism, and war, but instead emphasises the 'morphing' of terrorism and crime into threats that are no longer internal to the state, but also externally originated due to their cyber dimension (Brenner, 2014, p. 15).

Focusing in on Information Systems Security, the United States National Institute of Standards and Technology defines threat as "*…any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.*"

They go on to say that

"*Threat events are caused by threat sources. A threat source is characterized as: (i) the intent and method targeted at the exploitation of a vulnerability; or (ii) a situation and method that may accidentally exploit a vulnerability. In general, types of threat sources include: (i) hostile cyber or physical attacks; (ii) human errors of omission or commission; (iii) structural failures of organization-controlled resources (e.g., hardware, software, environmental controls); and (iv) natural and man-made disasters, accidents, and failures beyond the control of the organization. Various taxonomies of threat sources have been developed. Some taxonomies of threat sources use the type of adverse impacts as an organizing principle. Multiple threat sources can initiate or cause the same threat event—for example, a provisioning server can be taken offline by a denial-of-service attack, a deliberate act by a malicious system administrator, an administrative error, a hardware fault, or a power failure.*" (National Institute of Standards and Technology, 2012)

This is all within the context of Risk as

"*…a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation),*

organizational assets, individuals, other organizations, and the Nation." (National Institute of Standards and Technology, 2012)

Risk management is a well-developed discipline in its own right and not suitable for analysis within this thesis, however, when understanding threats it is important to at least acknowledge that any model of risk would include "*…the risk factors to be assessed and the relationships among those factors…….typical risk factors include threat, vulnerability, impact, likelihood, and predisposing condition."* (National Institute of Standards and Technology, 2012) In this well accepted NIST model of information systems security threat is a one factor among multiple risk factors.

Vulnerability: Vulnerability is defined by NIST as

"*…a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Most information system vulnerabilities can be associated with security controls that either have not been applied (either intentionally or unintentionally), or have been applied, but retain some weakness. However, it is also important to allow for the possibility of emergent vulnerabilities that can arise naturally over time as organizational missions/business functions evolve, environments of operation change, new technologies proliferate, and new threats emerge.*" (National Institute of Standards and Technology, 2012)

This is a wide definition that quite deliberately includes process and organisational vulnerability as well as pure system related vulnerabilities. Vulnerabilities can be found in a wide range of business areas such as product development processes, supply chains, or within governance structures. They can be found in hardware, firmware, software, people and processes. Some authors have used much more restrictive definitions, for example that limit it to software defects (Herzog and Schmid, 2016). This is potentially both inaccurate and dangerous in that by excluding common sources of vulnerabilities, not all risks may be understood.

Attribution has been described as "*one of the biggest barriers to effective cyber deterrence*" (McKenzie, 2017, p. 7) and is the source of significant debate. Thomas Rid and Ben Buchanan

identify three key assumptions that they see as dominating the attribution debate (Rid and Buchanan, 2014).

The first assumption is that attribution is one of the most intractable problems of an emerging field, created by the underlying technical architecture and geography of the Internet, secondly there is a binary view on attribution: for any given case, the problem can either be solved or not be solved and thirdly that attributive evidence is readily comprehensible, that the main challenge is finding the evidence itself, not analysing, enriching, and presenting it. According to Rid and Buchanan these views are common; they are intuitive; and they are not wrong — but they are limited and insufficient. The reality of attribution has evolved significantly in the past decade, leading to a view of attribution as a more nuanced activity and inherently political in nature. (Rid and Buchanan, 2014). This leads to a situation where in order to try and attribute an attack, the analysis need not be purely technical, but can instead look at "*geopolitical factors, the apparent objectives of the intrusion, and the exhibited capabilities of other states*" (Buchanan, 2016, p. 143). They go on to claim that "*…attribution is not just possible; it has been happening successfully for a long time. Attackers cannot assume that they can cause serious harm and damage under the veil of anonymity and get away with it. Even if the attribution problem cannot be solved in principle, it can be managed in principle.*" (Rid and Buchanan, 2014)

At a technical level there is a significant emphasis on forensic elements of attribution such as malware analysis where code level indicators may provide clues to attribution, from coding similarities from code reuse through to stylistic aspects, language and the like although it is claimed that "*absent proper synthesis, a high density of technical forensic artefacts does not necessarily mean that operational or strategic questions can be answered with more certainty.*" (Rid and Buchanan, 2014).

There are competing claims regarding attribution of high-level adversaries. It has been said that "*…the higher the sophistication of the adversary, the longer attribution will take and the more difficult it will be…*" (Rid and Buchanan, 2014), but also claims that "*The greater the sophistication of a cyberattack…..the lesser the difficulty of authenticating its source.*" (Kello, 2018, p. 200). This is perhaps indicative of the relatively sterile level of academic debate concerning attribution that is a developing discipline in private sector and national security

organisations subject to levels of secrecy and commercial confidentiality that may hinder any clarity in the wider community.

There is also the potential for issues of misinformation to be prevalent in attribution debates. Firstly, there is clearly the potential for 'false flag' attacks to be perpetrated in cyberspace that lead to mis-attribution of an attack, but there is also a significant level of deliberate obfuscation of the level to which state agencies (and others) are able to perform attribution (Klimburg, 2017a, p. 191)

It is argued that attribution will decline as an issue as more capabilities and resources are dedicated to being able to attribute cyber-attacks, especially from the growing cyber security industry (Buchanan, 2016, p. 145) and that new and as yet secret SIGINT capabilities may provide greater attribution capabilities.

Cyber security: This is also a nuanced term, with competing definitions such as Information Security (Infosec), Network Security and Computer Security. At times these terms are used synonymously, especially when the issue at hand is threats delivered through the internet. However, it is important to be able to delimit what is considered within the scope of cyber security, especially given the potential for mission creep in large organisations including those associated with national security in response to new threats (Schneier, 2015, p. 124).

The International Telecommunications Union (ITU) recommendation ITU X.1205 (International Telecommunications Union, 2008) provides a good working definition of cyber security focused on the means of providing cyber security:

> *Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general*

> *security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality.*

This ITU-T definition is very much based on the 'CIA Triad' (LM Security, 2016) (confidentiality, integrity, availability) that is a fundamental principle of Information Security practices.

The UK NCSS provides a more threat focused definition of cyber security as:

> "*…the protection of internet connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.*"

There are however some fundamentals that can be drawn from both that assist in establishing the basis for any discussion of cyber security.

1. Cyber security includes people and processes as well as technology
2. It is based on understanding and managing risk and has associated areas of risk mitigation and resilience
3. It incorporates all elements of the CIA triad of confidentiality, integrity, and availability
4. It includes the hardware and software of the systems and the network infrastructure
5. It includes 'data at rest' (stored data) and 'data in motion' (in transference from one electronic location to another)
6. It does not distinguish between levels of cyberspace

Common practice has been for 'Information Security' or 'InfoSec' and 'Cyber Security' to be used interchangeably at times, incorporating all risks to systems and information, including non-technology based risks from 'insiders' and non-network risks such as 'evil maid'[3]

[3] The term 'evil maid' is used to refer to any attack perpetrated by someone with unauthorised physical access to a machine, for example a maid in a hotel room where a laptop has been left unattended by a guest.

attacks that emphasise the need for physical and process security as well as electronic security. The term cyber security is used throughout this thesis.

2 Methodology

There are four main methodological techniques that have been adopted for this research project.

Firstly, the use of secondary sources to provide an analysis of the key characteristics of cyberspace; secondly, the use of Hedley Bull's concept of New Medievalism (Bull, 1977), extended by Philip Cerny's identification of the key characteristics of a neo-medieval environment (Cerny, 1998) to provide a theoretical construction of the governance environment in cyberspace; thirdly, the thematic analysis (Boyatzis, 1998; Braun and Clarke, 2006) using the elements of the Copenhagen School's Securitisation theory, of speeches by key securitising actors in the lead up to the introduction of the National Cyber Security Centre; fourthly, the thematic analysis of original qualitative data through semi-structured interviews with senior private sector individuals with responsibilities related cyber security who were able to take a strategic view of cyber security policy and initiatives. A deductive thematic analysis identified key themes articulated by the interviewees, while an inductive analysis using the characteristics of wicked problems was also undertaken to show the extent to which cyber security could be considered a wicked problem. This initiated a fifth methodological element which was a theoretical examination of cyber security against the wicked problem characteristics outline in the original articulation of wicked problem theory (Rittel and Webber, 1973) supported by secondary sources that considered the wicked problem nature of cyber security (Clemente, 2011; Malone and Malone, 2013; Denning and Denning, 2016).

The research period was between January 2016 and January 2018 and research using secondary sources was conducted throughout the research period. The theoretical framework using New Medievalism as a model for the environment of cyberspace was created during 2017, while the development of the Wicked Problem description was completed in 2018 following the analysis of qualitative interview data.

The analysis of speech acts included speeches between June 2012 and November 2017. This covers the major period of the development of state level interest in cyber security between the publication of the 2011 Cyber Security Strategy (Cabinet-Office, 2011) and the

introduction of the National Cyber Security Centre and the 2016 National Cyber Security Strategy (HMG, 2016).

The semi-structured interviews were conducted between May 2017 and October 2017. This was a long period of time in a fast moving environment, and some interviews were affected by different events, for example cancellations during the Wannacry attacks of May 2017 which then inevitably also influenced some of the discussion in subsequent interviews, although this is interpreted as more because the Wannacry attack become an easy example to quote rather than any change to fundamental views.

One area that may have changed over the research period was the attitude to the NCSC. It is impossible to say whether this reflects the views of the specific interviewees at the time or whether it was affected by timing. This was tested with later interviewees who suggested that attitudes to the NCSC had indeed changed over the research period. No other specific changes were detected.

2.1 Epistemology

This research project has taken a social constructivist approach to cyber security as a security issue which emphasises the importance of speech acts as performative utterances in constructing security (Huysmans, 2002). There are three key reasons for this approach.

Firstly, cyberspace is a man-made environment that "*would not exist were it not for the ability of human beings to innovate and manufacture technologies….*" (Schreier, 2012) It is people's perceptions of the possibilities of cyberspace that determine its capability. Cyberspace itself is a man-made construction and it is the construction of threats enabled by cyberspace that helps to determine security needs[4].

Secondly, the Copenhagen School's theory of securitisation used in this project views security as a social construction. The authors argue that "*Securitization is essentially an intersubjective process. The senses of threat, vulnerability, and (in) security are socially constructed*

[4] Note that although the issue of cyber security is being socially constructed, this is not a use of the theory of the Social Construction of Technology. The social construction of cyber-security here is not as a technology, but as described in terms of the senses of threat and vulnerability as referenced in the Copenhagen School's securitisation theory.

rather than objectively present or absent. Nevertheless, it is easier to achieve securitization under some conditions than under others" (Buzan, Waever and de Wilde, 1998, p. 57).

If we accept that cyberspace is a social construction and security is a social construction, then I would argue that it is appropriate for any study of security issues in cyberspace to be based on a constructivist approach.

Thirdly, a constructivist approach is appropriate as current approaches to governance and organisational boundaries in cyberspace are dependent on the development of norms of behaviour through a range of social structures, much in keeping with a constructivist ontology as "*Constructivists embrace an intersubjective ontology, emphasising norms, social agents, and structures….*" along with "*…central themes of change, sociality and processes of interaction…*" (Fierke, 2013). Again, this seems appropriate to any study of cyberspace as a fast changing environment in which context is fundamental to any understanding that is determined by the engagement of different actors in creating and defining the characteristics of the cyber domain.

2.2 Secondary Sources

A range of sources were used as input to the research. This included a wide range of academic and commercial secondary sources. Most cyber security incidents are dealt with by the commercial cyber security community in conjunction with state agencies. These sources often represent the most current thinking on many relevant areas and are the best sources for examples of developments in cyber security as well as current attacks and incidents.

There is a large practitioner literature that was used as a source in this project. Much of this is from the United States and is often the product of former government employees and advisors, for example works by former NSA Director Michael Hayden (Hayden, 2016) and former National Security Adviser Richard Clarke (Clarke and Knake, 2010).

The use of non-academic sources is a necessity in cyber security research and common in cyber related PhD theses. For example, a case study analysis of the Olympic Games cyber-campaign by the United States uses technical reports from "*Symantec and Kaspersky, as well as smaller companies*" (Herpig, 2014) as primary sources, and a PhD analysis of European cyber

security governance states that "*Cyber security is an emerging area, and traditional sources are not up to date with the constant technological changes, and this forces me to include other alternative sources for my data collection*" (Munk, 2015).

There is a recognised *"….growing gap between the emerging omnipresence of technology and the limited grasp most thinkers have of its impact on interstate dealings.*" (Kello, 2018, p. 10) which when combined with the rapid changes in technology makes this a fascinating, but difficult area to research from traditional academic sources and drives a dependency on state and private sector documentation.

With any commercial source there is the risk that the information may in some ways be influenced by self-interest, and certainly the threat analysis of the cyber security industry has been publicly criticised for allegedly inflating the threat (Lomas, 2016a). However, while there may be some unacceptable practices within the industry, I would argue that, in general, the larger players such as IBM, Symantec and the like, can be considered a trusted source, and there are a sufficient number of reports from different organisations to provide a high level of confidence in the analysis that is sufficient for the purposes of this project.

Again with the practitioner resources from former employees of state agencies, there are times when such sources have to be carefully considered as these works can contain a strong political viewpoint, or an element of justification of prior actions.

In any project associated with national security there will be areas that are secret and not easily accessible. There has been no attempt to acquire secret information as part of this project although information made available by Edward Snowden and Wikileaks that has since been reported in the press has been used as a source. In addition, two freedom of information requests were made as part of this project. One, related to software coding techniques and code obfuscation evident in the software of Huawei equipment, was rejected by the Cabinet Office on grounds that to answer would endanger national security. A second Freedom of Information request was made to the Information Commissioners Office regarding estimates of unreported data breaches to which they replied that there was no available data to show whether data breaches were being unreported, but that new GDPR requirements would ensure breach reporting and provide better data for the future.

However, since GDPR has been introduced, it has been claimed that there is now significant over-reporting of data breaches to the ICO (Afifi-Sabat, 2018).

Cyber security is a fast-moving environment with new developments, threats, or attacks emerging on an almost daily basis. While these sources are almost all from commercial organisations or new groups, they represented the most appropriate way to gather current information. It was essential to be able to track new developments and ensure currency of information, especially for use within interviews. In order to ensure the interview was based on current issues a combination of electronic feeds, conferences, and membership organisations were used to gather information.

This included membership of groups and organisations shown in Table 1 below.

Organisation Name	Description
Cyber Security Forum Initiative	LinkedIn online forum for discussion of corporate and government cyber security issues.
Cyber Security	LinkedIn group for cyber security professionals.
Cyber Exchange	UK Cyber Security Collaboration initiative from the Cyber Growth Partnership.
Alien Vault Open Threat Exchange	The world's largest open community based exchange of threat information operated by a manufacturer of security and incident management systems.
Electronic Frontier Foundation	Digital civil liberties pressure group.
SANS ICS Forum	An online forum for the discussion of issues relating to the security of Industrial Control Systems
The Internet Society	Internet Governance body that supports the work of the IETF. Provides occasional access to IETF meetings for members.

Table 1 Membership Organisations

In addition to this, there were many subscriptions to electronic information, mainly delivered by email. While these represented a significant volume of email (40 -50 per day, in part because subscription lists were frequently sold on to other providers) they provided an important daily update on key issues within the industry as well as links and connections to resources such as online education, virtual conferences and webinars, the availability of

which, would have been difficult to identify through other means. These include (in alphabetical order) the resources shown in Table 2 below.

Source	Description	Content
Bruce Schneier Blog	Respected US security commentator. Now employed by IBM Resilient.	Monthly pieces on implications of security issues.
Business Applications Digest	Newsletter from Tech Target dealing with wider application developments.	Big data, data centre operations, SAP and other business applications.
Cipher Brief	Washington DC based security platform aiming to engage private sector in security issues.	Cyber security news and analysis with a US and intelligence focus.
Cloud Digest	Newsletter from Tech Target on Cloud industry.	Cloud developments, including security.
Cloudera	Open Source Big Data software company.	Big Data developments and data management issues.
Computer Weekly	Computer industry magazine. (Also drives much of the Tech Target data).	General computing developments and issues, including security.
Computing	Daily newsletter from Computing magazine.	Links to in-depth articles on variety of computing subjects.
Cyber IQ	Subsidiary online magazine of Defence IQ	Defence oriented cyber.
Cyberx Labs	ICS/SCADA security solutions company	News and technical resources related to security of ICS/SCADA systems.
Cyware Labs	Threat sharing and awareness software manufacturer.	Good analysis of new threats and implications. Good technical information.
Darktrace	UK manufacturer of security software based on anomaly detection with strong links to GCHQ, NCSC and CNI providers.	Corporate information and threat analysis.
Dark Reading	Online security magazine	Good coverage of cyber issues and developments.

Source	Description	Content
Graham Cluley Blog	Respected UK Security Consultant	Daily reports on threats and analysis of industry issues.
Hacker News	Information Security newsletter	General information security and hacker news.
IBM Resilient	IBM Security Division	News and resources from IBM
IT Governance	Online magazine from education provider.	IT Governance issues. Particularly useful for certification, GDPR and NIS.
Info Security Magazine	Regular in-depth magazine on information security	Access to free virtual and physical conferences and other resources.
Information Security Buzz	Information Security Newsletter	Information Security industry news, including breaches, government initiatives etc.
Information Week	Weekly Newsletter	Information security issues and current landscape.
Ixia	Occasional newsletter from network security vendor	Occasional useful information on network level security, encryption etc.
Motherboard	Technology magazine	Wide ranging technology issues.
Network Computing	Network technology magazine.	Updates on network technology and networking issues.
Radware	DDOS protection provider	Technical information and threat analysis relating to DDOS attacks.
Recorded Future	Threat intelligence company	Detailed threat intelligence on specific cyber-attacks and industry issues.
Security Week	Cyber security newsletter from Wired Magazine	Access to articles, webinars and other cyber resources.
Symantec	Anti Virus Software provider	Industry updates, education and information.

Source	Description	Content
Tech Target	Daily Newsletter	Independent newsletter with cyber security and related news items and links.
Thales	Defence company working in cyber.	Links to research and resources from Thales.
Ultimate Windows Security	Independent newsletter	Windows security issues, patches, windows security management.
Wired	Electronic version of Wired magazine	General technology

Table 2 Electronic Subscription Sources

Desk based and electronic sources were supplemented by attendance at several conferences during the project. These are shown in Table 3 below.

Date	Conference Title	Description
June 2016	Infosec 2016	Annual conference and trade show for Information Security professionals.
Sept 2016	The Future of Cyber Security	Industry conference focused on the latest development in cyber security.
Oct 2016	Cyber security Ethics: The Common Good and the Digital Commons	Academic conference organised by Hull University as part of an ECRC funded programme.
March 2017	Security & Policing	UK Home Office sponsored show and conference aimed at security services.
March 2017	Infosecurity Global Spring Virtual Conference	Practitioner focused conference delivered online.
June 2017	Infosec 2017	Annual conference and trade show for Information Security professionals.
July 2017	Cyber security Summit	Public sector focused cyber security conference.
Sept 2017	Infosecurity 2017 Autumn Virtual Conference	Practitioner focused conference delivered online.
May 2018	Reinforcing Cyber Security Building Security, Confidence and Capability in the Cyber Domain	Public sector policy focused conference.

Table 3 Conferences Attended

While most of these sources are practitioner-based and often commercial in nature, they reflect the most appropriate cyber-security environment for this study and the environment in which the interview participants operate. As such, they provided an insight into the issues that were current in the cyber security industry that would be most likely to inform the interview content.

2.3 Securitisation Speech Act Analysis

A New Medieval cyberspace would require the state to take specific actions to assert its authority in cyberspace. One mechanism by which this is being achieved

is by constructing cyberspace as a national security issue that needs to be addressed by the state.

There are different critical security theories that could have been considered for adoption as a means to analyse the development of cyber security as a national security issue in the UK. Critical Security approaches in general are more appropriate for this study, as the security issues of cyberspace do not easily translate to a traditional military and realist view of security. This is particularly the case in relation to the number of non-state security actors such as the private cyber security industry, non-state threat actors such as criminal gangs and hacktivist groups, and key referent objects other than the state such as private critical infrastructure and companies. The broadening and deepening of security study represented by the Copenhagen School beyond the traditional state-centric and military oriented approach is particularly appropriate for cyber security study.

An alternative approach to the Copenhagen School that may have been interesting would be the development of a Welsh School emancipation-oriented view of cyber security. This is especially so, given the emancipatory potential of the Internet as an infrastructure that can provide tools to enable freedom from human constraints such as poverty, access to healthcare, and lack of educational opportunity. It is possible to argue that cyber threats limit the Internet's potential to deliver this promise and cyber security can be seen as the absence of cyber threats in the same way that Ken Booth describes security as the absence of threats (Booth, 1991 cited in Peoples and Vaughan-Williams, 2015).

However, within the Critical Security Studies discipline, the Copenhagen School was chosen as the security framework for analysis in this thesis. This was specifically because an initial review of statements made by security officials appeared to indicate conformity with the rhetorical structure of a securitising speech act as defined by the Copenhagen School. Based on this initial review it was decided that further study using securitisation as a tool for analysis would represent the most valuable avenue of study. There were four main reasons for

this. First, it is focused on security issues beyond the state military domain (although retains an interest in the state as a referent object); second, it allows for non-state referent objects which is particularly important for cyber security as the state is not the only referent object, with others such as private sector critical national infrastructure and economic issues relating to cyber-crime; third, securitisation allows for additional security actors as functional actors as well as securitising actors. Although this analysis has focused on the state (and its representatives) as securitising actors, there are any number of functional actors from within the private sector and civil society who are important contributors to cyber security. It is arguable that in some circumstances the state is not necessarily even be the prime actor in cyberspace. Fourth, securitisation provides an accessible and coherent tool for analysis through the emphasis on the speech act and the rhetorical structure of securitisation speech acts. This was particularly appropriate given the empirical identification of the formal speech acts using the rhetorical structure of securitisation.

The Copenhagen School theory of securitisation depends upon the use of a speech act as the means by which a securitising actor can make a securitising move and so this thesis includes an analysis of the speech acts that have been instrumental in the securitisation of UK cyberspace between 2012 and 2017. These start with a 2012 speech by the then Director of GCHQ, Sir Iain Lobban (Lobban, 2012) and end with a 2017 speech by the Chief Executive Officer of the NCSC, Ciaran Martin (Martin, 2017a), but include other key speeches within that time as shown in *Table 4 Cyber Security Speeches 2012 - 2017*.

Date	Speaker	Position	Audience
26 June 2012	Jonathan Evans	DG MI5	City of London
12 Oct 2012	Iain Lobban	Director GCHQ	IISS
4 Dec 2012	Francis Maude	Minister for Cabinet Office	IA12 Conference
27 March 2013	Francis Maude(Maude, 2013)	Minister for Cabinet Office	CiSP Launch Event
16 June 2014	Francis Maude(Maude, 2014b)	Minister for Cabinet Office	IA14 Conference
17 June 2014	Ciaran Martin	DG Cyber Security GCHQ	IA14 Conference
31 March 2014	Francis Maude	Minister for Cabinet Office	CERT-UK Launch Event
2 June 2015	Ciaran Martin	DG Cyber Security GCHQ	Infosec 2015
10 Nov 2015	Robert Hannigan	Director GCHQ	IA15 Conference
17 Nov 2015	George Osborne	Chancellor of the Exchequer	GCHQ
3 March 2016	Matt Hancock	Minister for Cabinet Office	Telegraph Conference
13 Sept 2016	Ciaran Martin	Head of NCSC	Billington Conference
24 Sept 2015	Michael Fallon	Defence Secretary	UK/FR Cyber Symposium
20 Oct 2016	Michael Fallon	Defence Secretary	RUSI Cyber Symposium
1 Nov 2016	Philip Hammond	Chancellor of the Exchequer	Microsoft Conference
14 Feb 2017	Philip Hammond	Chancellor of the Exchequer	NCSC
27 March 2017	Matt Hancock	Minister for Digital & Culture	IoD Conference
27 June 2017	Michael Fallon	Defence Secretary	Chatham House
13 Sept 2017	Ciaran Martin	CEO NCSC	CBI
14 Sept 2017	Ciaran Martin	CEO NCSC	EU Cyber Security Conf.
15 Nov 2017	Ciaran Martin	CEO NCSC	Times Tech Summit

Table 4 Cyber Security Speeches 2012 - 2017

These particular speeches were selected as they were directly addressing cyber security issues; they were documented on Government web sites and so publicly available for analysis; and they were given by individuals with relevant state political agency in cyber security.

The period 2012 – 2017 was selected based on it being contemporaneous with the acknowledgment that the 2010 Cyber Security Strategy was not delivering the expected results (National Audit Office, 2013) and the completion of the first year of

operation for the UK's National Cyber Security Centre (NCSC, 2017e). There is particular focus on the time between the two 2015 GCHQ speeches that publicly established GCHQ as a significant force in cyber security (Hannigan, 2015; Martin, 2015), through George Osborne's announcement of the creation of the NCSC (in advance of the 2016 Cyber Security Strategy) and the end of the first year of operation of the NCSC. This period has included the most explicit securitisation speech acts in relation to UK cyberspace.

In particular, formal 'set piece' speeches by UK politicians and security service chiefs were identified for analysis on the basis of the subject matter, and the extent to which the speeches were reported. For all the identified speeches, transcripts were available on one of uk.gov, mi5.gov.uk, gchq.gov.uk, or ncsc.gov.uk web sites. The set-piece nature of these securitising utterances also had the advantage of allowing an estimation of the type of audience on the basis of the context in which the speech was made, and to be able to allocate a specific securitising actor (both as an individual and as an organisational representative of the state) to the speech.

Each of the identified speeches were evaluated in terms of the key components that would be expected to be found in a securitising speech act according to the Copenhagen School's securitisation theory.

Initially, it was confirmed whether the speech conformed to the rhetorical structure of securitisation as defined by the Copenhagen school. More detail on the rhetorical structure of securitisation speech acts is included in section 6.1 UK Cyberspace Securitisation Speech Acts on page 172. Those that did not conform, and so did not represent a securitising move in their own right, were not subjected to further analysis in terms of their contribution to the securitisation of UK cyberspace. However, a number of them remain important within the process due to their position in developing context and understanding that supported the securitising moves.

The key securitising speech acts were further analysed to identify key components of securitisation including the securitising actor, the political agency of the

securitising actor, the referent objects of the securitisation, the audience for the securitising move, security predictions, and functional actors within the securitisation.

A number of speeches were excluded from full analysis as they either did not conform to the securitisation rhetorical structure, or they were speeches that were delivered in support of a very specific event (e.g. launch of CiSP) that did not effectively address securitisation. This includes those speeches shown in Table 5 below.

Date	Speaker	Position	Audience
4 Dec 2012	Francis Maude	Minister for Cabinet Office	IA12 Conference
27 March 2013	Francis Maude	Minister for Cabinet Office	CiSP Launch Event
16 June 2014	Francis Maude	Minister for Cabinet Office	IA14 Conference
31 March 2014	Francis Maude	Minister for Cabinet Office	CERT-UK Launch Event
3 March 2016	Matt Hancock	Minister for Cabinet Office	Telegraph Conference
24 Sept 2015	Michael Fallon	Defence Secretary	UK/FR Cyber Symposium
27 June 2017	Michael Fallon	Defence Secretary	Chatham House
14 Sept 2017	Ciaran Martin (Martin, 2017a)	CEO NCSC	EU Cyber Security Conference

Table 5 Speeches excluded as not addressing securitisation

However, although not securitisation speech acts, these speeches were still subject to analysis in relation to other discursive elements, in particular relating to partnership between government and the private sector, which represents a key point of discussion from the interview data gathered as part of this research project.

The analysis of the securitisation speeches was completed using a process of thematic analysis as described by Richard Boyatzis in *Transforming Qualitative Information: Thematic Analysis and Code Development* (Boyatzis, 1998).

Thematic analysis is described as "*…a process for encoding qualitative information. The encoding requires a specific 'code'. This may be a list of themes; a complex model with themes, indicators, and qualifications that are causally related; or something in between*

these two forms. A theme is a pattern found in the information that as the minimum describes and organised possible observations…." (Boyatzis, 1998, p. vii) These themes can be directly observable in the information or underlying the information. Themes can be "*...generated inductively from the raw information or generated deductively from theory and prior research.*" (Boyatzis, 1998, p. vii)

In thematic analysis terms the 'unit of analysis' for the securitisation of UK cyberspace are the cyber-related speeches between 2012 and 2017, while the 'units of coding' are the individual speeches that have been identified. Within the units of coding, the codeable events are the specific elements of the speech act identified by securitisation theory.

Thematic analysis was also used as the basis for the analysis of the interviews with cyber security practitioners where the unit of analysis is the private sector cyber security practitioner community, the units of coding are the individual interviews and codeable events are the inductively identified themes or the deductively derived events based in wicked problem characteristics.

So, in this thesis, both inductive and deductive thematic analysis approaches have been used. Securitisation speeches have been analysed deductively using the framework of securitisation theory, while the practitioner interviews have been analysed both inductively to extract key themes, and deductively based on the theory of wicked problems in public policy.

For the securitisation speeches, codes have been used that reflect the elements that are expected within a securitisation speech act allowing the speeches to be coded on the basis of their conformance to the requirements of the speech act.

This approach is based on that outlined by Richard Boyatzis where the elements of the code are derived from elements of the theory (Boyatzis, 1998, p. 33). The codes used are shown in Table 6 below, based on the five code elements of label, definition, description of indicators, description of exclusions and examples to aid in coding.

Table 6 Analysis Codes for Securitisation Speech Act Themes

Label	Definition	Flag Indicators	Qualifications	Examples
Threat	Articulation of cyber threat and threat actors	Threat, attack, hackers, hacktivists, terrorism, aggression, attack methodologies (SQL injection, malware, phishing etc.)	Exclude non-cyber threats but include use of cyber to support non-cyber threats	"high end threats and attacks" "state sponsored aggression" "cybercrime"
Scale of the Threat	Scale of the threat faced in terms of number of attacks or potential costs	Any statement of scale	Include references to speed and frequency as well as size and number	"repeated catastrophic breaches"
Exceptional Measures	Exceptional measures requested to respond to the threat	Invest, introduce, upgrade, create, new capability, legislation, regulation, strengthen, 'will'	Exclude anything that is a continuation of previous activity	"introduce a single national cyber centre", "more active cyber-defence approach"
Referent Object	The referent object of security i.e. the thing that is being secured	Infrastructure, integrity, systems, economy, confidence, reliability, companies	Ensure referent object is of sufficient importance to justify securitisation	"confidence in the digital economy"
Action Effects	The effect of taking action in response to the threat	Stable, resilient, success, positive consequences	Ensure they are future based results of action	"make Britain one of the best protected countries in the world"
Inaction Effects	The effect of taking no action in response to the threat	Loss, damage, negative consequences	Future based negative, or continuation of negative current position	"there will be no economic security for our country"
Partnership	State and private sector partnership calls	Partnership, together, private sector, share	Exclude partnerships of State agencies working together	"we will have to work together", "government and industry working hand in hand"

Once the codes have been defined, the speeches are reviewed for 'codeable events' based on the identification of key phrases and words that indicate the codeable event. In order to aid in analysis, speech was organised into numbered blocks of text. There was no semantic value to this blocking exercise but was intended purely to improve the ease of identification of where codeable events occurred. A 'blocked' version of George Osborne's 2016 speech and the resultant coding is included as an example in ***Appendix F: Speech Act Thematic*** Coding Example (Osborne) on page 401.

This coding allowed relevant sections of the speeches to be identified for use within the thesis narrative.[5]

The use of thematic analysis in a study of this kind, which (like most PhDs) has effectively been a 'one-man band' effort with no additional research resources does present some challenges.

Firstly, there is the issue of projection, where the researcher attributes their own feelings onto the raw information. This was not a problem in relation to the securitisation speeches as the use of the elements of securitisation as the basis for the coding gave a solid structure to work with. This was also the case with the analysis of interviews that showed themes relating to cyber security as a wicked problem. Where there was no pre-existing theoretical framework to guide the analysis, such as in the initial analysis of interview transcripts, there has been a focus on consistency in coding and only treating unambiguous statements as codeable events.

Secondly there is the issue of sampling. In the case of the securitisation speeches the majority of the total number of speeches related to cyber were used in the analysis. Some were discarded early on, as not conforming to the rhetorical

[5] Not all speeches were subjected to the detailed blocking and code allocation process as, given a limited number of codeable events, and relatively short speeches, the key securitisation elements could be identified directly from the text.

structure of securitisation, but any speech that adhered to the structure was included for analysis.[6] In the case of the interview participants the emphasis was on trying to achieve coverage of different industry sectors to provide a general overview of the views of cyber security practitioners. Detail on the interview participants is included in section 2.5 on page 52.

Boyatzis also cites the mood and style of the analyst as a potential issue (Boyatzis, 1998, pp. 15–16) but provides a number of techniques to mitigate this. In this specific exercise all appropriate mitigations were applied including not coding for too long, developing clear codes, stopping coding if preoccupied, and suspending judgement to just 'go with the data". There was no requirement to "*establish consistency of judgement between multiple perceivers*" as all analysis was undertaken by the same person.

Clearly the code definition and then the identification and selection of codeable events are highly subjective, but in order to try and ensure consistency one particular set of coding was completed at a time (rather than completing both the interview themes and wicked problem coding together for a single interview) as it was felt that consistency within the overall coding of the data was most important. Coding was completed over a period of several days in order to avoid 'coding fatigue' leading to inconsistent judgements being applied.

2.4 New Medievalism

The relationship of the state and private sector in cyberspace has been the subject of many studies and a significant literature has been developed over the past twenty years or more. Much of this literature is based on realist assumptions regarding the anarchy of the international system and the primacy of the state in international relations (for example Betz and Stevens, 2011). As a result, there is a preponderance of literature that emphasises conflict in cyberspace, either between states, or between states and non-state actors, with cyberspace itself seen as either a distinct

[6] Detail on the choice of speeches is included in Table 9 Securitisation Speeches

operational domain akin to land, sea, air and space in which state power can be exercised, or a route for exercising state power in other domains.

However, there are two reasons why New Medievalism as an alternative to realism is potentially useful as an IR lens through which to view cyberspace.

The first reason for adopting New Medievalism is that cyberspace as a distinct environment is not an ungoverned anarchy. There are multiple levels of authority that provide governance in cyberspace, and which can limit state actions in that domain. These include, the code itself that controls operations in cyberspace (Lessig, 1999, 2006) the infrastructure of cyberspace (DeNardis, 2012; Denardis and Musiani, 2014), existing state based international organisations such as the United Nations (UN) body of the International Telecommunications Union (ITU) and the Internet Governance Forum (IGF), emerging cyber-norms of behaviour (Osula and Rõigas, 2016) and Non-Governmental Organisations such as the Internet Engineering Task Force (IETF) and the Internet Society (ISoC). The multi-national corporations that dominate cyberspace including well-known consumer brands such as Facebook, Google, and Amazon along with the less obvious infrastructure providers such as Alcatel, Cisco, and Huawei also derive governance capabilities from their position.

The second reason for adopting New Medievalism is that states have not, to date, represented the most significant force in cyberspace. In its earliest incarnations, cyberspace was characterised as free from state interference (Barlow, 1996), and while it is no longer the case (if it ever was) that the state has no authority in cyberspace, the extent of that authority and the means by which it can be asserted remains contested. This has been characterised as a 'war' for the Internet as the most contested element of cyberspace (DeNardis, 2014; Powers and Jablonski, 2015). This should not be confused with discussions regarding traditional state conflicts taking place in the domain of cyberspace (Arquilla and Ronfeldt, 1993, 1997; Libicki, 2007; Clarke and Knake, 2010; Rid, 2013), or discussions concerning the projection of realspace state power through cyberspace (Morozov, 2011). All of these issues are inter-related in that they effect the balance of power in cyberspace,

but they are distinct areas of conflict. Current developments supporting the state assertion of authority are changing the balance of power in the complex environment of overlapping authorities in cyberspace.

These overlapping authorities and the historical relative weakness of state influence in cyberspace suggest that New Medievalism represents an appropriate theoretical lens for the analysis of power relationships in cyberspace. I would argue that this is the case even if a realist analysis is accepted as the most appropriate way to view state relationships in realspace, and these realspace power relationships then spread into cyberspace, especially when cyberspace can be used to project realspace power. There is a substantive difference between realspace power relationships projected through cyberspace and cyber based power relationships.

It is worth noting that much of the literature relating to New Medievalism is written from the standpoint of the Westphalian system breaking down into a New Medieval environment in particular in response to the pressures associated with globalisation (Matthews, 1997; Kaplan, 2000; Rapley, 2006; McFate, 2014). However, this thesis argues that for cyberspace the current question is one of a New Medieval environment potentially having state order imposed to more closely resemble a Westphalian state system. This is not necessarily the imposition of state order on an anarchic situation but is instead an attempt to impose current realspace governance norms on cyberspace, in particular in relation to the primacy of the state.

The laws that operate most effectively in cyberspace have not to date been based on a Westphalian state model but have instead been a collection of overlapping jurisdictions that have at times complemented one another and at times operated in opposition. It remains an open (and contested) question as to whether cyber governance will transition to a multi-lateral state based governance system, or whether it will remain within a loose multi-stakeholder system that incorporates many different governance authorities.

2.5 Interviews

The analysis of the securitisation process in the UK has shown that there are areas where there is a potentially significant disconnect between the private sector and the NCSC as the UK state agency responsible for cyber security. Press reports of objections to proposals for BGP and SS7 and pejorative commentary concerning the '*great British block off*' (Nichols, 2016) provide further indications of this disconnect.

In response, NCSC statements concerning "*magic amulets"* being sold by the cyber security industry and the "*winged ninja monkeys*" (Levy, 2016b) used to spread fear in the user population provide indications of an equal level of dissatisfaction with the private sector on the part of the state.

However, these are only indications, and none of these public statements, speeches and press reports seem to provide any depth of understanding of the relationship between the state agencies and the private sector in the delivery of cyber security in the UK.

To develop a better understanding of the perceptions of the relationship between state and private sector authorities a small number of in-depth semi-structured interviews were conducted with senior cyber security experts from within a range of private sector organisations. A sample of the interview participants shared with the NCSC (as part of a request for their engagement which was refused) were described by the NCSC as *"…some of the industry leaders in this area…"*[7].

[7] Private email from NCSC dated September 6th, 2017. The relevant section reads "*As I am sure you can imagine, the NCSC receives many requests for assistance from students like yourself and, unfortunately, we simply do not have the resources to meet them all. As a result, we have made the decision to limit our interactions, in the main, to those universities with which we have a strategic relationship (namely Academic Centres of Excellence in Cyber Security Research, Research Institutes and universities providing NCSC-Certified degrees). I am sorry that Buckingham does not yet fit any of these criteria and, therefore, regret that on this occasion we will not be able to assist you. However, we are pleased to see that you are already working with some of the industry leaders in this area and hope that they have given you excellent material to work with.*"

The researcher was able to call on a personal background as a senior manager with several technology companies to identify and recruit interview participants and produce an interview that was suitable for the intended participants. This was important as one of the key factors that can help to determine a successful interview process with an elite group is that a suitably qualified interviewer should be used (Kincaid and Bright, 1957).

The methodology identified in the initial research proposal planned to use both survey and interview data alongside key cyber security documentation and by analysis of the data from all three sources try and triangulate the inputs to deliver findings based on their intersection. However, a pilot of the survey was undertaken with a small group of five supportive individuals from within the private sector technology community. This survey pilot was undertaken to try and evaluate the survey prior to a more general release to a larger population.

The survey consisted of closed questions using Likert scales to enable survey respondents to indicate their level of agreement or disagreement with a statement. The available responses were, strongly agree, agree, neither agree nor disagree, disagree and strongly disagree. This was used as it provides a balanced set of response alternatives and includes a 'nonresponse' option of neither agreeing nor disagreeing with the statement which is accepted as an appropriate response to attitude questions (de Vaus, 2014, p. 105).

The Likert scales approach was chosen as firstly, it is a survey method regularly used in a corporate environment and respondents are expected to be familiar with its use; secondly, closed choice questions of this type are quick to answer, hopefully ensuring the survey is completed and not considered burdensome by respondents; and finally, they provide results that can be more easily coded for analysis (de Vaus, 2014, p. 99).

A seventeen point checklist (de Vaus, 2014, pp. 97–99) was used to refine the wording of the questions in order to ensure they were easy to understand and likely

to elicit a response that was honest and had not been biased by the question. Each question was defined with a specific documented purpose behind it.

In order to validate the questions in the survey, firstly, a "defect identification review" was conducted in which a senior manager with a multi-national Information Technology company was asked to complete the survey with the researcher present and were able to ask questions of anything that was not clear; secondly, a peer review by a small group of senior executives from the technology industry. The purpose of this review was to validate that the questions were reasonable to ask and that the scope of the survey was acceptable in a corporate environment, and thirdly a survey pilot was undertaken with a third small group of technology industry executives and managers from the UK and the United States. These individuals were typical of the intended survey participants.

Unfortunately, feedback from the survey pilot was universally negative and indicated that a survey approach was unlikely to deliver any usable data. Follow-up discussions with the pilot participants suggested that the subject matter was too complex, and the questions too far reaching for a survey approach to work. Every answer required a caveat or explanation which would be more effectively achieved through qualitative semi-structured interviews.

As a result of these issues, the survey approach was decided to be inappropriate, and the focus for gathering original data was through semi-structured interviews with a senior elite group of cyber security professionals in the private sector.

A set of five specific criteria were used to select interview participants. These were derived from the desire to use the interviews to gain a strategic level insight into private sector views of the state's role in delivering cyber security,

- That they should be working in a role that incorporated engagement with cyber security in the private sector. This could be in an organisation securing itself, assisting with national cyber security, or providing cyber security solutions for other private and public sector organisations.

- That they should be operating at a senior and/or strategic level in relation to cyber security in the private sector.
- That they should be in a position where they would have an awareness of state cyber security policy and national cyber security strategy.
- That the sample should not be dominated by one organisation or industry sector.
- That they would be prepared to discuss issues relating to state engagement in cyber security openly on the condition of organisational and individual anonymity.

Participants were approached either through recommendation, or by targeting an organisational role that included Information Security or Cyber Security and a job title that indicated an appropriate level of seniority or strategic viewpoint such as Head of or Director of.

These criteria were explained to prospective participants, alongside the interview briefing document (included as Appendix E: Documentation Sent to Research Participants in Advance of the Interview) which provided more detail on the questions that would be asked as part of the interview. Some prospective interview candidates withdrew from the process at this point as they considered themselves unable to contribute to the subject at the required level.

No interview data was excluded from analysis, even where the researcher felt the contribution had been limited.

Interview participants were senior managers or Board level executives within their organisations, senior technical staff or consultants operating at Board level, and as such can be seen to represent part of an elite group within the cyber security industry.

Participants from a range of organisations were selected. This was specifically to ensure that key industry sectors were included in the interviews, especially those that had the potential for engagement with national security aspects of cyber security, and so would have an extensive knowledge of and interest in state

activities and engagement related to the private sector. The interviewees included, for example, individuals from the Telecommunications and Internet Service Provider industry who were responsible for delivery of cyber security for their organisations and for their customers; individuals responsible for the security of highly personal data and critical equipment within the health care sector; individuals involved in delivering cyber security as a service; and those who form part of the Critical National Infrastructure including the Oil and Gas and Finance sectors.

One of the major problems with interviewing any elite group is that of access to participants (Welch *et al.*, 2002; Rice, 2010) and this was initially the case in this research project. Fortunately, due to prior work experience, the researcher was able to approach an initial five participants on the basis of a previous business or personal relationship and from there on present myself as 'an insider' (Rice, 2010) to facilitate further access. Some interviewees were willing to approach their own contacts with a view to involvement in the project and this 'snowballing' (Welch *et al.*, 2002) produced a further four of the participants and was the most successful strategy for engaging new participants.

Two participants were approached at industry conferences, although in general this was not a successful strategy as several others approached in the same way who initially agreed to participate, later withdrew their agreement either explicitly, or implicitly by not responding to voicemails or emails. Where stated, the reasons for not agreeing to an interview were either that they didn't feel they could contribute to the subject area, they felt that the confidentiality of the information precluded their involvement, or they were too busy.

Cold email approaches were generally unsuccessful, although initial approach through email once an introduction had been made was generally successful, and responsible for the engagement a number of participants.

Social media was also used as a mechanism to contact and research participants. In particular the business networking tool LinkedIn was successfully used in three

cases, as a contact mechanism, and in one case to identify the correct individual within an organisation.

LinkedIn was also used to 'connect' with participants prior to the interview, enabling me to review their background and experience, and gain a basic understanding of their organisation prior to the interview. This was essential in ensuring credibility through the interview process. In one case, the LinkedIn review proved particularly useful when unknown to either myself or the interviewee it transpired that we had both worked in the same division of Cable & Wireless but without ever crossing paths. This provided a common background that allowed me to establish my own credibility and develop immediate rapport during the interview.

In one case a participant could only be contacted by Twitter Direct Messages, which, while unlikely to be a successful strategy in most cases, suited this particular individual due to a requirement for confidentiality and anonymity.

The key element to the contact strategy was to use a range of tools that could meet the needs of the participant and would create an atmosphere of positive engagement on a peer basis.

Other contact strategies were considered, in particular a letter to the Chief Executive Officers of selected organisations asking for them to identify someone to be interviewed, but it was felt that this would not create the right environment as participants may not engage if they felt they were 'told' to do the interview, rather than choosing to do it and they may start the interview with a level of suspicion as to the motives behind it. It was also considered likely that at a business and executive management level there would be a level of concern about discussing security issues that might lead to unwillingness to be involved. This was confirmed by discussions with the UK country managers for two technology companies.

A blanket call via the Cyber Security Forum Initiative (CSFI) was also considered, but after investigation and an email to the forum moderator, was not felt likely to

produce participants of similar calibre to those that were being contacted through other means.

All interview participants were interviewed with a guarantee of anonymity.

Thirteen key individuals were interviewed as part of the research. They represented a cross section of the cyber security community, including representatives from Critical National Infrastructure organisations in telecommunications, and Oil and Gas sectors, cyber security provider organisations, defence contractor cyber security divisions, healthcare, information technology manufacturing, technology industry association, consultancy, and private think-tanks.

All participants were operating at a senior strategic level within their own organisations.

Participant A

Head of Information Security, Critical National Infrastructure organisation in the Oil and Gas sector. Responsible for both office-based, and field-based cyber security, including operational equipment on oil and gas extraction facilities.

Participant B

Chief Information Officer for a household name national health service provider, with responsibility for critical hospital systems, in addition to sensitive patient and business data.

Participant C

Customer Director for security solutions for major telecommunications equipment manufacturer providing security solution to private and public sector organisations, including underlying cyberspace infrastructure providers.

Participant D

Cyber Security Lead, Major Information Technology software and services organisation providing cyber security solutions and threat intelligence in both the private and public sector.

Participant E

Chief Technology Officer, Critical National Infrastructure organisation in the telecommunications sector. Responsible for provision of organisation level cyber security and national cyber security of the telecommunications industry with strong links to the National Cyber Security Centre.

Participant F

Public Sector customer director for major defence contractor providing cyber security solutions, including public sector Security Operations Centres.

Participant G

Independent cyber security consultant named as one of the top twenty women in cyber security by SC Magazine. A focus on human factors in cyber security.

Participant H

Cyber security lead for technology industry association. Strong engagement with both private sector and state initiatives, representing cyber security issues on behalf of the technology sector.

Participant I

Chief Information Security Officer financial services sector, and former Government cyber specialist.

Participant J

Former Head of Cyber Threat Intelligence for major defence contractor, former hacker, and founder of cyber security business working with the National Cyber Security Centre.

Participant K

Head of Customer Security Products, Critical National Infrastructure telecommunications sector.

Participant L

Project Director, international cyber think-tank and former Government cyber specialist.

Participant M

Distinguished Architect, Telecommunications Sector. Responsible for the provision of security architecture and design services for major customers of the telecommunications sector.

Most of the interviews were conducted by telephone, with the exceptions of participant L whose interview was conducted via Skype, and Participants E and F whose interviews were conducted face-to-face.

Telephone interviews were a pragmatic choice in terms of firstly limiting the cost of interviews. The travel costs for face to face interviews would have been prohibitive with interviewees located around the UK. Secondly, the telephone was preferred as a means of gaining access to the diary of senior people with many different calls on their time. In several instances this allowed interviews to be put back and quickly and easily rearranged due to time constraints on the part of the interviewee.

Skype was a very successful mechanism, despite the fact that the interviewee had to move rooms during the interview, but the location selected by the participants for the face to face interviews (a town centre café) meant that recording was not possible and only contemporaneous notes are available rather than a recording a transcript. A copy of these notes was sent to the participants to validate that they were correct. As an example, the notes sent to Participant F are included as ***Appendix C: Participant F Meeting*** Notes.

All interviews were recorded with the permission of the participant with the exception of Participant F and Participant E. Again, recording was a choice made, in order to ensure that the interviewer could be focused during the interview on

maintaining a comfortable conversation allowing follow up questions to be asked and potentially productive branches to be followed without concern for note taking which makes the interview process more difficult to manage when open-ended questions are being asked in an elite context (Dexter, 1970, p. 59; Berry, 2002). Nobody actively declined to be recorded. Three interviewees requested a copy of the interview transcript. An example interview transcript is included as ***Appendix D: Example Edited Transcript***.

Participants were asked to allow for 30 -40 minutes for the interview. The majority of the interviews extended beyond 40 minutes with the exception of Participant E who was constrained to 30 minutes by other commitments. In most cases, extension beyond 40 minutes was at the direct request of the interviewees even when the interviewer reminded them of the time constraint.

All but one of the telephone interviews were (based on perceived background noise and other distractions) conducted with the interviewee in a quiet office or home office environment. The interview with Participant E was completed while the participant was in a taxi to another appointment.

In order to record telephone interviews a high-quality Polycom Voice Station 300 hands-free conference phone was used. This was chosen on the basis of previous experience with the product and the features of hands-free operation, 360-degree microphones, resistance to interference from other devices, operation using a single analogue telephone line, and volume control and mute capability.

Recording was done on a Sony ICD-PX470. This option was chosen because of price and features, including a transcription playback mode which slows down the recording in order to aid the transcription process. A back-up recording device of a smartphone with Voice Recorder App was also present for all interviews but was not used.

The interviews were semi- structured, with open questions. These were preferred to a fully structured interview or survey in order to allow flexibility in the order of questions and latitude to ask further questions in response to significant replies

(Bryman, 2016) and to allow interviewees to answer within their own contextual framework and take account of the preference of a technical elite group to be able to fully articulate their views (Aberdach and Rockman, 2002). A semi-structured approach was preferred to an unstructured interview in order to ensure the interviewer retained control of the interview especially in relation to the available time (Hertz and Imbert, 1995, pp. 10–11).

The interview opened with the basic administration of confirming whether the interviewee had received the brief, whether they gave permission for recording and checking whether a transcript was required.

The ground rules (Hertz and Imbert, 1995, p. 10) for the interview were set, with emphasis on the fact that the interview was not intended to try and extract secrets from the participants; that they were speaking as experts in their own right and not on behalf of their organisation; that all answers would be anonymised and not attributable to them and that if they were uncomfortable answering any particular question they should just decline to answer.

The objectives behind these ground rules were to try and put the interviewee at ease with the process and generate a level of trust at the beginning of the conversation. It was also made clear that this was not an 'equal conversation' but that I would ask questions and most of the time would be for them to speak and not the interviewer. This again was to encourage participants to speak as freely and voluminously as they wished.

The interview opened with a request for them to provide their background and their role in cyber security. This served to provide an easy introduction to the interview (Aberdach and Rockman, 2002) as well as providing potential linkages to later questions. Interestingly, at this point, three participants self-identified as 'hackers' (although the exact meaning of this was not tested) and five self-identified as being formerly associated with the military or the intelligence agencies.

The content of the interview was based around the set of questions in the briefing document provided to the participants in advance of the interview along with a

one-page project summary. This allowed participants to self-select engagement on an informed basis, thus ensuring high quality interviews with participants who had already thought about some of the issues and considered themselves able to make a valid contribution. It is worth noting that at the end of the interview, several of the participants expressed their thanks for being able to take part and said how much they had enjoyed the process and how it had been useful for them to be able to discuss the issues covered by the interview. The briefing document sent to participants is included as ***Appendix E: Documentation Sent to*** Research Participants in Advance of the Interview.

Other organisations that were contacted but for various reasons were not interviewed included the UK NCSC, Uber, Vodafone and NTT. The main reason for non-engagement was not finding the right contact within the organisation, although one agreed participant was also called up as a reserve officer in the US Army and was therefore unavailable, and the NCSC declined as Buckingham is not a University with which they have a strategic relationship. Attempts to interview smaller businesses on the subject proved unproductive with either an unwillingness to participate or self-exclusion on the basis that they had no valid input to offer.

There were no significant ethical issues arising from the interviews. All interviews were conducted voluntarily, it was made clear that there was no compunction to answer any question they were not comfortable with, and that the interview could be ended at any time.

A similar thematic analysis approach to that used for the securitisation speech acts was adopted for the analysis of the interview data. Starting with a process of becoming immersed in the raw data through the interview and transcription process followed by a reading and re-reading of the transcripts, certain themes began to appear, both in terms of general view on cyber security and in terms of the themes associated with wicked problem theory. Each of the fully transcripted interviews was coded against the identified themes. The result of this coding is included in ***Appendix H: Interview Themes Codeable*** Events.

The codeable events for the themes of the interviews was based on an initial review of the interview data which identified seven key themes of

1. The complexity of the cyber security environment.
2. The failure of the market to address cyber security and the potential need for regulation as a result
3. The limitations on the role and capabilities of the private sector
4. The need for collaboration and the difficulties inherent in collaborative approaches
5. The difficulties in working with government and state agencies
6. The changing and adaptive nature of the cyber security environment
7. The need for better education and understanding

The coding table for these themes are shown in *Table 7 Analysis Codes for Interview Themes Codeable Events* below and the coding for all interviews is included in ***Appendix H: Interview Themes Codeable*** Events.

The initial review of the data also indicated that there was a potentially productive analysis that could be conducted in relation to the characteristics of wicked problems. The coding table that was used is shown in *Table 8 Analysis Codes for Wicked Problem Codeable Events* on page 66 and the complete wicked problem coding of all the interviews is included as ***Appendix I: Interview Wicked Problem*** Codeable Events.

Table 7 Analysis Codes for Interview Themes Codeable Events

Label	Definition	Flag Indicators	Qualifications	Examples
Complexity	The complexity of the cyber security environment and the issues faced	Complexity, balance of requirements, different, variety of issues	Complexity in systems, relationships and responsibilities	"even within organisations the concerns are different"
Regulation	The failure of the market to address cyber security and regulatory approaches	Rules, regulations, law	Include elements that suggest greater need for regulation or failure of existing regulation.	"come up with informed regulation"
Limitations	The limitations of private sector cyber security capability	Out of scope, beyond control, limit, not responsible, legal constraints	Ignore limitations relating to state capability	"most organisations do not try to break the law" "difficult to defend against state level capabilities"
Collaboration	The need for collaboration to address cyber security issues	Work together, collaborate, share, cooperate, assist, joint	Include criticisms of lack of collaboration as well as positive affirmation of the need for collaboration	"collaboration between industry and the regulators"
Difficulty	The difficulty of working with state institutions.	Lack of knowledge and understanding, secrecy, complexity, trust	Reference to Government, law enforcement and state institutions	"a long journey to go for organisations to trust the government" "scepticism about what the government can offer"
Change	The level and rate of change in cyber security.	Change, different	Include high levels or rates of change	"the threat is going to change"
Understanding	The need for greater levels of understanding of cyber security	Education, understanding, knowledge	Include lack of knowledge and need for greater knowledge	"understand their business better"

Table 8 Analysis Codes for Wicked Problem Codeable Events

Label	Definition	Flag Indicators	Qualifications	Examples
No definitive formulation	There is no definitive formulation of a wicked problem	Adaptive, change, new, unknown	Include indicators in relation to problems or security issues.	"difficult to identify all vulnerabilities"
Stopping Rule	Wicked Problems have no stopping rule	Never ending, continuous, repeating	Include repeating issues, or slight variations.	"seeing same attacks coming back"
No True or False	Solutions to wicked problems are not true or false but good or bad	Relative statements, insoluble problems, mitigation, risk management	Include solutions rather than problems	"managing risk – which is what cyber is"
No solution test	There is no immediate and no ultimate test of a solution to a wicked problem	Returning problems, guesswork	Include problem not going away, or not knowing if it has gone away, as well as returning	"IoT is an example of a returning old problem of unsecured devices"
One shot operation	Every solution to a wicked problem is a one shot operation	Work around, blowback, mutation	Look for solution by-pass and causing new problems	"once they have figures out what you are doing, they by-pass it"
Potential Solutions	Wicked problems do not have an enumerable set of potential solutions	Unlimited, continuing issue, never ending, constant search for resolution	Look for iteration of solutions and numerous answers	"data propagates and runs out of control"
Unique	Every wicked problem is essentially unique	Unique problem, specific, new problems.	Specificity in problem definition	"no one size fits all solution"

Table 8 Analysis Codes for Wicked Problem Codeable Events (continued)

Label	Definition	Flag Indicators	Qualifications	Examples
Symptom	Every wicked problem can be considered to be a symptom of another problem	Underlying problem, raising new issues	Include where problems iterate and need to be peeled back	"Negligence will allow criminal activity to be perpetrated form your machine in a bot net. Lack of anti-virus, unpatched anti-virus or illegal copies of windows"
Explanation	The existence of a discrepancy representing a wicked problem can be explained in numerous ways. The choice of explanation determines that nature of the problem's resolution	Several explanations, different reasons.	Include where different reasons for same problem.	"we do not understand today what we will need to do tomorrow"
No right to be wrong	The Planner has no right to be wrong	Criticism of security institutions.	Include areas where there is expectation that institutions could have done better, especially state related	"government has a huge responsibility"
Social Complexity	Social complexity adds a further level of difficulty to wicked problems	Groups, dependencies, relationships, collaborations, different objectives and expectations	Include differences and divergences of ethical standards as well as practical approaches	"difficult to distinguish between public and private actors" "not clear what the government wants from the private sector"

3 Background: Cyber Threats and Vulnerabilities

This chapter provides a background to understanding the changing role of the state in cyberspace and its engagement with cyber security. This includes the increase in risks that result from economic and societal dependencies on cyberspace, the increased threat of cyber-attacks and the vulnerabilities that exist due to the failure of the private sector to provide an adequate level of security without state engagement (HMG, 2016, p. 13).

One clear indication of the scale of the cyber threat is that the global cyber security market is anticipated to grow in value to more than $300 billion per annum in 2024 (Bhutani and Wadhwani, 2019) from a value of $137 billion in 2017 and an estimated $167 billion in 2019 (Statista, 2019). This growth is indicative of a continued need to address cyber security problems on a wider scale.

Cyber threats have been well-documented by government, academia and commercial organisations (Clarke and Knake, 2010; Richards, 2014; HMG, 2016; Symantec Corporation, 2017 among others). Rather than repeat this threat analysis, this section takes the approach of identifying the risks and vulnerabilities associated with these threats that are influencing the UK state's approach to cyberspace.

3.1 Dependency on Technological Infrastructure

Since its inception, and in particular since its commercialisation in the 1990s, cyberspace has grown in its importance to the normal functioning of society in the United Kingdom (alongside many other areas of the world). In the UK, as of 2017, 90% of households had internet access, with 82% of people using email, 64% reading online news, 63% using online banking, and 66% using social media (ONS, 2017b). As a global communications network it has helped to enable the processes of globalisation and the creation of businesses that have caused significant disruption to many industries such as publishing (Amazon), retail (the many online shopping sites), hotel accommodation (AirBnB), transportation (Uber), as well as enabling applications such as email, video conferencing and social media that have

changed the way in which people read the news, share information and communicate with one another.

The economic dependency of the UK on cyberspace is significant. While estimates vary, a 2014 report from Boston Consultancy Group was reported as showing that the Internet was the second biggest contributor to the UK economy after the property sector, worth 10% of GDP or £180 billion. In 2017 the UK Government quoted the digital economy as being worth £145 billion (HMG, 2017a, p. 14). The cyber-dependency of the economy can be seen in areas such as online shopping, which now accounts for more than 24% of all non-food sales (Financial Times, 2018), and the fact that 60% of employees who use a computer at work also use it to access the Internet (ONS, 2017a). Businesses such as retail banking, publishing and bookselling, transport and logistics, hotel and travel booking, and advertising (where Internet advertising is now a £10 billion business and the largest category of advertising spend in the UK, taking 46% of the overall spend (OFCOM, 2017)) have been changed beyond recognition by the growth of cyberspace.

It can be argued that some of the most dramatic indications of economic dependency are shown when cyberspace fails. Lloyds of London estimate that the costs of an extreme cyber event could reach more than $121 billion (Lloyds of London, 2017), the 2016 cost of malicious cyber activity to the US economy was estimated at between $57 billion and $109 billion.

Financial consequences for individual organisations are also potentially significant. The Talk Talk cyber-attack cost £60 million and led to them losing 100,000 customers (Farrell, 2016), while the Equifax data breach reportedly cost the company $439 million. In 2015, the CEO of IBM referred to cyber-crime as "*the greatest threat to every company in the world*" (Ginny Rometti quoted in Birch, 2015)

However, it should be noted that calculating the costs from malicious cyber activity is notoriously difficult (Home Office Science Advisory Council, 2018) and elements of self-interest, bias, and estimating error should be anticipated. Any estimate of the total cost to

the economy can be expected to have been impacted (downwards) by under-reporting of incidents (Fafinski, Dutton and Margetts, 2010).

In addition to the economic dependency there is also a societal dependency on cyberspace. Society has embraced the potential of cyberspace to the point where it is difficult to imagine life without the capabilities it provides. Estimates of nearly 48 million active Internet users (ONS, 2018) and an estimated 32.6 million regular Facebook users, 12.4 million UK Twitter users and 18.4 million Instagram users (Sweney, 2018) indicate the high level of societal digital use in the UK. The same ONS report shows that more than 82% of households have a fixed broadband connection to the Internet with 88% of adults able to access the internet from home. This has changed the way in which we communicate with one another and the way in which we access entertainment and information.

As logistics and other industries operate increasingly through online communication, and the development of the Internet of Things drives the creation of 'smart' cities and other smart infrastructure, the dependency on cyberspace for food, power, water, and other basics of life will increase. Cyberspace is also changing the way in which citizens interact with the state. The 2017 Government Transformation Strategy (HMG, 2017a) aims to use digital technology to transform the way in which the state relates to its citizens. It states that "*One of the most powerful enablers of transformation in the early 21st century is to adopt the tools, techniques, technology and approaches of the internet age. This is what we define as 'digital'.*"

The infrastructure of the state is becoming increasingly dependent on information technology. Since 2010 the UK government has been following a "digital by default" strategy for government services, with clear benefits from the cost savings of online government transactional activity displacing telephone or face to face contact (Cabinet Office, 2012).

This is neatly shown in the UK Transformation Strategy when it reports that:

> *"....from April 2015 to March 2016 over 33 million people taxed their vehicle online (and no longer need a paper record), 93% of vehicle tax and drivers transactions*

> *(about 200 million per year) were done online, over 4 million people applied for a driving licence online and over 5.7 million people used the voter registration digital service.*" (HMG, 2017a)

This is a significant change to how state functions are delivered, and when the Universal Credit benefits system is fully online, it will deliver some £63 billion of benefit payments annually, the successful processing of which will determine the wellbeing of millions of pensioners and other benefit recipients.

However, the Transformation Strategy also includes the warning that:

> "*Our commitment to digital transformation means that we must do this in a way that takes into account the risks of the digital age. As the National Cyber Security Strategy notes, cyber-attacks are growing more frequent, sophisticated and damaging when they succeed. We must therefore ensure that we move forward in a way that is secure, deters criminal behaviour and which maintains our commitment to individuals' privacy.*" (HMG, 2017a)

Transforming the infrastructure and operations of the state through a digital strategy, inevitably leaves that infrastructure susceptible to the risks associated with any digital infrastructure. Given the volumes of data collected by the state, the value of state transactions through tax collection, government procurement and benefits payments and the potential societal impacts of disruption to state services, it represents a significant target for criminals or hostile states.

3.2 Failure of the Market to Address Cyber Security

The 2010 - 2015 Cyber Security Strategy for the UK (Cabinet Office, 2009) emphasised the role of both the public and the private sector in securing UK cyberspace (National Audit Office, 2013, p. 11). The NAO identified key challenges faced by this strategy that included (among others) increasing the awareness of individual online risks and responsibilities and influencing industry to establish the required level of cyber security investment and correct the under-reporting of cyber-attacks (National Audit Office, 2013, pp. 25–26).

These challenges identified by the NAO are indicative of a failure in the 2010 - 2015 strategy with both individuals and industry seen as not having taken on the responsibilities that were anticipated in the strategy and which were required for it to be successful.

One particular example of this failure to take responsibility for security can be seen in the lack of 'security by design' evident in a huge range of insecure wireless enabled products (in particular related to the IoT) being released onto the marketplace with default or unchangeable passwords (Varmazis, 2018) that can then be misused as part of a botnet for DDOS attacks. Default passwords for devices are widely available online[8].

This includes high volume consumer devices such as security cameras and baby monitors that are internet enabled, but which may have no capability to patch security flaws, and on which consumers either do not change the default password or the device does not offer the capability to set or change a password. The Mirai botnet DDOS attack on a Domain Name Service Provider that made the Internet unavailable in many areas of the USA used 61 combinations of default username and password combinations to take control of more than 49,000 connected devices (mainly security cameras) in 164 different countries (Herzberg, Bekerman and Zeifman, 2016; Fruhlinger, 2018a). This shows the potential these devices have for causing significant impacts to the operation of the Internet infrastructure and Internet connected systems as well as the global nature of the problem.

A significant market failure across all sectors has been the lack of basic 'cyber hygiene' in particular in relation to software patching processes. This has led to the continued operation of systems containing unpatched known vulnerabilities. These vulnerabilities are relatively easy to scan for using free tools available on the Internet (Kimball, 2019) and as a result even some of the most significant cyber-attacks have exploited vulnerabilities that could have been previously patched. Examples of recent attacks that have utilised known vulnerabilities

[8] For example https://ipvm.com/reports/ip-cameras-default-passwords-directory offers details of security camera default passwords, http://routerpasswords.com/ offers lists of default router passwords and https://wifibaby.net/tech-support/default-router-usernamespasswords/ offers default credentials for baby monitors.

include the Wannacry exploit which took advantage of a known issue with Microsoft Simple Message Block for which a software patch already existed (Fruhlinger, 2018b) and the September 2017 Equifax data breach which used a Remote Code Execution vulnerability in Apache Struts software that had existed since 2012 and for which a patch had been available since March 2017 (Raywood, 2017).

Part of the problem with the patching process is that there is a clear issue with the current process of patching software vulnerabilities in that the release of patch, while informing users of a security solution, also informs bad actors of a security vulnerability. There are legitimate reasons why organisations may not install a patch immediately, such as the need to regression test against internal systems, or to schedule the installation for a maintenance window or a planned period of system down time. The delay between patch release and installation represents a window of opportunity for exploitation of what is at that point a publicly known vulnerability.

There are of course new vulnerabilities discovered within software for which no patch exists. These are the so called 'zero days', named as such due to the fact that there have been zero days in which to resolve them. The discovery of unknown vulnerabilities has become a rich business in its own right with 'vulnerability hunting' potentially delivering significant rewards with online marketplaces such as Zerodium offering up to $1.5 million for zero day exploits (Zerodium, 2018). It has also raised the issue of the state acquiring and stockpiling zero day vulnerabilities for its own use and failing to inform software manufacturers of vulnerabilities so as to be able to retain the vulnerability for their own offensive purposes. This has the effect of states leaving citizens at risk of these vulnerabilities potentially being exploited by malicious actors.

In the USA this is documented in the Vulnerabilities Equities Process (VEP) (USG, 2017). In the UK the process was documented in 2018, but remains such that disclosure is effectively decided by GCHQ with input from the NCSC (GCHQ, 2018b). GCHQ claim to release more than 90% of the vulnerabilities they find (Hannigan, 2017).

Another area of significant concern to the UK state agencies has been the perceived failure of the private sector to report cyber incidents, and in particular, successful breaches of their security. There is a strong financial and reputational motivation not to report a breach, for example, the Talk-Talk cyber-attack was reported as costing the company £60 million in direct costs and led to the loss of 100,000 customers (Farrell, 2016) and a 20% drop in share price (Guibourg and Ehrenberg, 2015). In addition, there was personal criticism (Pemberton, 2015), and although any direct connection was denied (Sweney, 2017) the eventual removal of Chief Executive Dido Harding.

A failure to report a cyber-attack leading to a data breach with the loss of personal data has the potential to impact the 'rights and freedoms' of individuals, especially given the increase in the amount of personal data collected and the potential for its use and misuse. This issue has been addressed by regulation in the introduction of the General Data Protection Regulation (GDPR) in May 2018. Although GDPR is focused on the protection of personal data and individual control through processes such as consent requirements and the right to be forgotten, there is also a clear economic rationale behind the regulation in that it specifically references "*the importance of creating the trust that will allow the digital economy to develop*" (European Union, 2016). This economic dependency on trust in the digital economy has been a key referent object in the securitisation of UK cyberspace (Maude, 2012; Hannigan, 2015; Martin, 2017e).

At a more tactical level, the failure to report breaches also prevents the timely raising of awareness across the cyber security community. This may be important in that it prevents organisations who could be attacked in the same way from taking mitigating actions in advance of the attack. It also prevents individuals whose data may be compromised from taking timely remedial action (Infosec Institute, 2018). However, it should also be noted that prior to GDPR being introduced there was no clear understanding of the scale of the

suspected under-reporting problem. In response to a Freedom of Information Request the Information Commissioner's Office[9] was unable to confirm any under-reporting.

Another area that is contributing to the definition of the state's role in cyberspace is the perception of a divergence in the interests of social media and technology companies and the interests of the state. One of the most public examples of this has been that of the terrorist use of the Internet for propaganda purposes and for operational command and control.

The use of the Internet for terrorist planning and operational communication has helped to fuel a debate about encryption capabilities that are available to bad actors and the resultant lack of capability of law enforcement and intelligence agencies to access encrypted data (Brown, 2015). This has resulted in calls for so called 'back doors' to enable access to encrypted communications which are strongly opposed by providers of encrypted communications and the Information Security industry more generally (Cheshire, 2017). Attempts by the state to control access to encryption appear to be destined for limited success, as users will potentially just migrate to services provided by organisations operating outside of territorial jurisdiction (Collins, 2017). State attempts to control encryption are nothing new and the 'Crypto Wars' and 'clipper chip' are a part of Internet legend (Electronic Frontier Foundation, 2014). Realspace threats such as terrorism are resulting in increasing pressure on technology organisations to support state efforts to break encrypted communications.

There has been direct criticism of online service providers, with then Home Secretary, Amber Rudd talking about terrorist propaganda quoted as stating that "*The tech giants need to step up and do more, take a moral responsibility for the fact their platforms are being used in this way.*" (Watts, 2017) and GCHQ Director Jeremy Fleming used his first public appearance in the role to connect criminals and paedophiles to encryption (Fleming, 2018b) and at the 2018 Billington conference called for warranted capabilities for intelligence agencies to break

[9] Email from Information Commissioner's Office Casework Reference IRQ0703940 sent to the author on 16th October 2017.

encryption (Fleming, 2018a). This debate is confused by the distinction made by the social media companies between their role as a 'platform' acting merely as a conduit to enable publication of material and the different function (with a much greater associated responsibility for content) of a 'publisher' of material. This has led to the UK government evaluating whether to change the legal status of some online service providers to be publishers (Ruddick, 2017).

However, there has been evidence of some online service providers taking action, such as Telegram's deletion of 78 ISIS channels on its service (Gibbs, 2015) and there is acknowledgment of attempts by service providers to remove terrorist content, but dissatisfaction with the speed at which this takes place with a call for a 'step change' in the way in which this is done (Prime Minister's Office, 2017).

This is all part of an ongoing discourse that links electronic communication and encryption to terrorism and criminality that is seen by some as merely an (invalid) justification for mass surveillance by the state with a corresponding impact on privacy and civil liberties (Schneier, 2015, pp. 160–164). The weakening of encryption may also carry risks that can impact the security of cyberspace (in particular around the authentication required for secure financial transactions) and may outweigh any benefits (Landau, 2017, pp. 91–96).

3.3 Increasing Attack Sophistication

There is a perception that cyber-attacks are becoming more sophisticated and more difficult for citizens to defend against. The proliferation of nation-state level exploits, increased use of machine learning techniques to avoid detection and prevent attribution, new malware distribution techniques such as file-less malware and the increased blurring of lines between bad actors, all add to this difficulty.

This 'sophistication' has been questioned as it may contain a level of both hype and justification for defensive failures, and it is certainly possible to find instances of attacks described as sophisticated that are later shown to be simple attacks by relatively unsophisticated actors (Buchanan, 2017). However, this perception of sophistication is one

that is promoted by state agencies such as the NSA in the United States (Gertz, 2017) and the UK's NCA and NCSC (National Crime Agency, 2017a) and as such may prove to be a factor in determining the role of the state in cyber security.

In addition to the increasing sophistication of cyber-attacks there are a number of issues associated with the detection of successful cyber-attacks.

Firstly, there can be significant delay before a successful attack is known to have taken place. The median 'dwell time' (or breach detection gap) between a compromise and detection has been calculated at 175 days in 2017 in European organisations (FireEye, 2018a). This means that for these types of stealth compromises, system intruders have that length of time to explore and understand the compromised systems, exfiltrate data, undertake obfuscation activity or develop further vulnerabilities for later exploit as required. Dwell time can be seen as less of an issue with loud transient attacks such as ransomware and web defacement, but is significant for more persistent stealth compromises that may be the basis of state or corporate espionage, ongoing credit card or personal data theft, and military posturing and pre-installations for future attack (Gerritz, 2016).

The 'lateral movement' of an intruder within a network or system is increasingly a key concern for cyber security operations and is an issue with defensive strategies that have depended on a perimeter defence to protect cyber assets, leading to the development of techniques in threat hunting within a network and 'defence in depth' approaches to cyber security[10].

Some criminal activities are based on undetected long term compromise. Traditionally this would include compromise of a device for use in a botnet, or ongoing data theft, but more recently also includes compromise for crypto-currency mining operations that use computing power on compromised machines and is seen as something of a victimless crime

[10] It should be noted however that the full adoption of defence in depth should not be considered a realistic strategy for corporate cyber defence as it would require the ability to counter-attack to destroy the enemy (Small, 2011). This is outside the scope of legitimate legal powers that can be claimed by private companies.

and a way for criminals to make money without users even realising that there is unwanted software running (Symantec Corporation, 2018).

Any attack that remains undetected has implications for the state and for national security. First, it represents a potential attack vector for future attacks, where an undetected previously compromised system can be exploited almost immediately. Second, it has the potential for significant lateral movement within the system and between interconnected systems. There are examples of compromise through partner networks, for example Home Depot (Kirk, 2014) or compromises from within the supply chain (NCSC, 2018a) meaning that undetected compromises within systems may provide access to multiple additional systems and organisations. Third, an undetected compromise is a mechanism for the kind of long term data exfiltration associated with state or economic espionage. Fourth, undetected compromises may provide the potential for further compromise through escalation of privileges of compromised accounts, potentially allowing more extensive harm to be caused in the future.

These four issues that arise from undetected compromise of privately owned systems all serve to create an increased level of risk within the UK cyber environment.

3.4 Increasing Scale of Cyber Attacks

As well as increasing in sophistication, cyber-attacks are also increasing in scale, in terms of the number of attacks, the number of records exposed by data breaches, the size of DDOS attacks and the financial implications of attacks.

The increasing scale of the effects of cyber-attacks is clearly seen in the statistics relating to data breaches, 2017 was recorded as having more than 5,000 data breaches, exposing more than 7.8 billion data records, compared with 2016 with 4,195 data breaches and 6.4 billion records exposed. Although most breaches are caused by external intrusion (hacking) the greater volume of records exposed is caused by accidental exposure for reasons such as misconfiguration or accidental publication (Risk Based Security, 2018).

The number of records is heavily skewed by a small number of highly significant breaches that expose billions of records. From 2017's 7.8 billion records, 4.5 billion were from 3 incidents and nearly half of the 2016 number of 6.4 billion was from one incident (Yahoo) in which 3 billion records were exposed. A total of 1.1 billion records were exposed in 2013 and 2014 and 823 million in 2015 (Risk Based Security, 2018)[11].

The two key issues here are first, that it harms personal privacy to have personal details available on the Internet; second that the data may be used to commit further crimes either through identity theft, fraud or through unauthorised access via stolen passwords. Stolen passwords are a particular issue when they have been reused across accounts, so that even systems where data has not been stolen may be easily compromised.

As is shown by the analysis of the securitisation speech acts there is much in the securitisation discourse in the UK that shows concern for public confidence in the digital economy. It is these issues that have the potential to cause both economic and societal disruption if confidence in the digital economy is destroyed by the theft of data, especially when the theft may not be noticed, or if noticed then not reported.

DDOS attacks have also become more dangerous in terms of the number and scale of the attacks that are possible (Alexander, Kupreev and Badovskaya, 2018; Fakhreddine, 2018).

For example, the release of Mirai botnet source code '*into the wild*', (i.e. making it freely available on the Internet through forums or code repositories) made similar attacks an option for an increased number of threat actors who could utilise the Mirai code for their own botnets. The development of new techniques to amplify DDOS traffic has made highly impactful DDOS attacks a simpler proposition, and the availability of 'DDOS as a service' (or DDOSaaS) now allows malicious actors to undertake a DDOS attack with no technical capability at all (Francis, 2016; Makrushin, 2017). All the above developments have added to the potential severity of the DDOS attack threat.

[11] These figures are included only to indicate the problem. Other industry figures support the general trend, although details and absolute number vary significantly especially given the lack of mandatory reporting until GDPR.

Possibly as a result of this, there has been a higher profile and more effective response from law enforcement with respect to DDOS attacks. This has included the arrest in the US of a man who hired a DDOS service (Vaas, 2017), the arrest of a man using 'plug and play' tools to launch DDOS attacks, (Vaas, 2018), the December 2017 arrest of the three men behind the Mirai botnet (Curtis, 2017), and the 2018 conviction of a man in the UK for DDOS attacks on Google and Skype (Crown Prosecution Service, 2018).

The founders of hacking groups Lizard Squad (who in 2015 had shut down the NCA's web site with a DDOS attack) and Poodle Corp were convicted in the USA in 2017 for operating the LizardStresser tool (Waqas, 2017), and a 19 year old in the UK was convicted for operating the vDOS subscription DDOS service and attacking Vodafone, Amazon and the NCA among others (Crown Prosecution Service, 2017),

However, the increases in the number and potential scale of DDOS attacks and the reduced technical skills required to initiate one, remain key issues for future security in cyberspace.

3.5 Increasing Exposure of Critical Infrastructure

Many of the systems that operate within the Critical National Infrastructure, in particular Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, represent a very different challenge to the more usual security challenges offered by systems operating on Linux or Microsoft software. Software on these ICS/SCADA systems has a much longer lifetime, a much slower patching cycle, and a significant test requirement before it can be installed on a production system (Pauna and Moulinos, 2013). All these characteristics make ICS/SCADA systems more vulnerable to attack.

In general, ICS/SCADA systems were not originally developed with the intention that they should be exposed to the Internet and were installed as proprietary and isolated systems. This provides an inherent level of security derived from the obscurity of the systems and air gapping i.e. physical separation of the systems from public networks. Over recent years however these systems have developed into more open architectures and have increasingly been connected to both corporate intranets and the Internet to allow remote monitoring and

operation and information sharing between systems. This connection to the Internet has exposed the critical infrastructure to Internet originated threats.

There are potentially catastrophic and life threatening scenarios involving the compromise of the CNI (Clarke and Knake, 2010; Brenner, 2011) and evidence of successful attacks on infrastructure targets such as the Natanz nuclear enrichment facility (Stuxnet), Saudi Aramco Oil Company (Shamoon), and Ukrainian Power Plants (Black Energy). There are reported attempts of attacks on Western infrastructure including the Rye Brook Dam (Kutner, 2016) and the Energy Sector infrastructure (Dragonfly attacks), (Symantec Security Response Attack Investigation Team, 2017) alongside the identification of sustained state level attacks on UK infrastructure. It is unsurprising that the exposure of CNI ICS/SCADA systems should be a concern, especially as recent research has shown that these societally vital systems remain vulnerable (Leydon, 2018) and are under sustained attack.

3.6 Espionage

Cyber-espionage and the use of cyber-tools as a mechanism for spying represents another area that can be seen to add legitimacy to the state's interest in cyber security.

State-on-state espionage is a long standing state activity, described as the second oldest profession (Michael Barrett quoted in Knightly, 1987) and although it is an infringement of state sovereignty there are accepted norms that govern its operation. Cyber-espionage however has a number of additional complications in relation to state engagement in cyber security.

There is organisational and functional blurring of the line between espionage and surveillance. The combined Computer Network Exploitation (CNE) and surveillance roles of the NSA is a concern in the United States (Schneier, 2015, pp. 215–216). In the UK, the situation is arguably more difficult with GCHQ effectively responsible for surveillance, espionage, offensive cyber, and cyber security of government systems, a key role to play in security of the CNI, including online service providers and CSPs, providing advice and guidance for private sector organisations, and engagement with key regulatory controls such as the Network and Information Security (NIS) Directive. The inherent conflicts of

interest that exist between these GCHQ functions and the national security constraints on oversight and transparency are areas of potential concern when considered in the context of privacy and civil liberties.

Cyber-espionage is further complicated by the difficulty involved in technically distinguishing between actions indicative of CNE and those that are indicative of Computer Network Attack (CNA). The covert installation of malware could be a tool for espionage or it could be 'preparing the battlefield' for an attack, with CNA and CNE both using similar or the same technical capabilities (Landau, 2017, pp. 52–53). This makes CNE and CNA difficult to distinguish, especially from a defender's point of view, creating a risky environment that has the potential for inadvertent escalation (Klimburg, 2017a, p. 153; Latiff, 2017, p. 52).

Further, there is a blurring of the distinction between cyber-espionage and cyber-crime. This blurring may be a result of state sponsored corporate espionage that is less covert than state-on-state espionage (Schmidt and Cohen, 2013, p. 114), or it could be a result of state hackers choosing to supplement their earnings by moonlighting in criminality (Klimburg, 2017a, p. 280) Alternatively, it may be a by-product of the same technical tools being utilised for both espionage or data theft (Deibert, 2013, p. 162) or even, as has been suggested regarding the Russian Business Network (RBN) crime infrastructure, as a result of criminal capabilities being nationalised by the government (Klimburg, 2017a, p. 235).

Cyber-espionage is a complex area that has emerged from traditional state and military disciplines of Electronic Warfare (EW), Information Warfare (IW), Influence Operations (IO) and Psychological Operations (PsyOps). This provenance again serves to blur organisational and operational boundaries between military and civilian intelligence operations and between information operations and CNA. For example, the UK military's 77th Brigade which was normally responsible for PsyOps is now reported as also including the UK offensive cyber capability "*sitting alongside that of GCHQ*" (Corfield, 2018). The disciplines of PsyOps and an offensive cyber-attack are arguably very different.

Arguably, cyber has significantly increased the reach and penetration of any information based operations, as has been shown by the reported Russian influence operations in the 2016 US elections (DHS and FBI, 2016) and the 2016 Brexit vote in the UK (Burgess, 2018; Wintour, 2018). The lack of serious response by private sector organisations such as Facebook can be interpreted as further reinforcing the need for a state level response to adversary information operations (BBC News, 2018).

However, state capabilities in cyberspace appear to be outstripping those of non-state malicious actors, and there is a risk that it is state capabilities that have the most potential for destroying confidence in the digital society either through the surveillance capabilities, supply chain interference with basic infrastructure, the proliferation of state tools, or the lack of oversight and transparency concerning their activities.

3.7 Proliferation of Cyber Capabilities

Also of concern is the proliferation of cyber capabilities, both in terms of exploits being made publicly available and their use becoming increasingly automated or offered 'as a service' and so bringing the capability within reach of those with no technical capability or skill. This is potentially providing a weapon that can increase capabilities in an asymmetric conflict.

Free software tools are available from repositories such as GitHub, and state level capabilities stolen by hackers have been made publicly available such as was the case with the NSA's Eternal Blue exploit stolen from the Equation Group by Shadow Brokers (Symantec Corporation, 2017) which was then used in the Wannacry attack. The availability of common tools has become such an issue that in 2018 the UK's NCSC issued a report that provided guidance on how to defend against five categories of tools including remote access tools (RATs), web shells, credential stealers, lateral movement frameworks, and C2 obfuscation tools (NCSC, 2018e).

Proliferation can be seen in the numerous free and easy to use tools available on the Internet that can be used for both legitimate and malicious purposes. Legitimate penetration and

stress testing of systems requires similar tools to those that are used to break into systems or attempt to take them offline through denial of service attacks.

Tools such as the Low Orbit Ion Cannon (LOIC) developed by Anonymous is widely available and is an example of a hacktivist tool becoming a generic hacking tool. Other Denial of Service tools are available such as the HTTP Unbearable Load King (HULK) that perform similar functions. These are cheap and simple to use, even with little or no technical expertise, but provide significant possibilities for malicious activity.

Common and once again free tools such as Wireshark, Metasploit and NMAP enable anyone to map network connections and gather details on connected devices including operating system and software levels, allowing vulnerabilities to be identified. With the easy availability of these tools it is unsurprising that the majority of attacks are untargeted and based on identification of a vulnerability rather than a specific objective for an attack.

There are also a range of password cracking tools such as Aircrack-NG for Wi-Fi passwords, or John the Ripper and THC Hydra for brute force and dictionary based password cracking. Again, this reduces the skill level and effort required to compromise credentials.

There is an increasing awareness of the potential for AI and machine learning in cyber security. Defensive systems have for some time used these kind of capabilities to learn about malware, or to identify anomalous activity on a network. Offensive capabilities are now also in use that allow malware to learn when it has been detected and create its own variant in such a way as to once again be undetectable, or to mutate with every single infection (Cobb, 2016; Panda Security, 2017).

As these tools and capabilities proliferate there are clear examples where the flexibility and adaptability of attack methodologies and exploits that make them difficult to secure against, in particular in terms of malicious capability reuse which reduces the cost and development time for new exploits, diminishes the skill levels required to produce sophisticated attacks, and as a result increases the number of potential attackers.

There are several examples of this kind of reuse of code:

a) The code behind the Mirai botnet has been reused in several variants (Arbour Security Engineering and Response Team, 2018) which has shown the potential for new capabilities to be quickly added on to an existing framework, with new exploits that enable additional IoT devices to be targeted.
b) Stuxnet code similarities were found in Duqu, Gauss and Flame malware (Bencsáth *et al.*, 2012) showing how even highly specific targeted attack code can be reused for a more generic attack methodology.
c) The NSA's Eternal Blue exploit was used in the Wannacry ransomware attack, the Petya wiper- attack (Burgess, 2017) and in the Eternal Rocks worm (Ashford, 2017)

These have all placed sophisticated techniques capable of significant harm in the hands of groups who as a result have been able to use highly advanced capabilities without needing to invest the resources required to develop such capabilities.

Proliferation in this way is one means by which terrorist groups may become more cyber capable. The potential for terrorist use of cyberspace represents another driver for the engagement of the state. Terrorist groups have not as yet made regular use of cyber-attacks, but have become cyber-capable in several ancillary ways (Ingram, 2014)

At this point, cyberspace is being used by terrorist groups as a distribution mechanism for propaganda, as a tool for recruitment and radicalisation and as a communication mechanism for command and control as well as the delivery of religious rulings and guidance (Weimann, 2011). There has been evidence of terrorist use of encrypted messaging applications such as Telegram and WhatsApp (Rawnsley, Woods and Triebert, 2018) which is of concern to state agencies responsible for preventing terror attacks.

However, any discussion of cyber-terrorism requires a distinction to be made between a terrorist cyber-attack and the information warfare and command and control use of cyberspace for terrorist purposes (Stohl, 2006; Heickerö, 2014).

Cyber terrorism in its most apocalyptic incarnation has yet to be realised[12], despite predictions that included

> "*The stock market closed, as did the commodities markets. Major hospitals cancelled all but emergency surgeries and procedures. Three major power grids experienced brownouts. Police and state militia units were ordered into the cities to maintain order and minimize looting. Millions of Americans, now staring at blank computer screens, were sent home from work.*" (Clarke, 2005)

There is evidence that the risk of this 'pure' cyber-terrorism is limited (Giacomello, 2004; Lachow and Richardson, 2007; Lachow, 2009) although research indicates that it is also considered a significant threat (Jarvis, Macdonald and Nouri, 2014). This threat is considered by the NCSC to be limited by a lack of terrorist cyber capability (Martin, 2016b).

However, the societal impact of online extra-jurisdictional propaganda and radicalisation is seen as potentially significant and the UK state has an interest as part of its counter-terrorism strategy to be able to limit the use of cyberspace 'safe spaces' for this and for terrorist communication and command and control (HMG, 2016, p. 52).

The state also has an interest in cyber due to the military implications of cyberspace. The use of cyber-capabilities as an extension of Electronic Warfare (EW) and as part of hybrid-warfare conflicts have been seen as a feature of Russian conflicts in Georgia and Ukraine (Segal, 2016, pp. 66–77) and were used as a justification for setting up 77th Brigade[13] in the UK with a mission to "*…counter hybrid warfare techniques*" included in their role (Fallon, 2016).

There is also an increasing military dependency on the use of satellite technology (and in particular GPS) in warfare to the point where it has been said that "*War today could not be*

[12] The one destructive terrorist cyber-attack on French television station TV5 that was originally publicly claimed and attributed to Islamic State was shown to be an attack by the Fancy Bears Russian hacking group (Corera, 2016).

[13] Note that 77th Brigade has since been incorporated into HQ 6 (UK) Div which "provides the British Army's Asymmetric edge. It orchestrates intelligence, counter-intelligence, cyber, electronic warfare, information operations and unconventional warfare." (MoD, 2020)

fought without satellites." (Latiff, 2017, p. 73) which has led to cyber-attacks to spoof GPS signals with potentially catastrophic effects of failure, including the mis-direction of GPS guided weapons.

The number, scale, and potential importance of cyber security across a whole range of state interests would suggest that there is a persuasive argument that can be made for the state to play an important role in the security of cyberspace. This is almost regardless of whether the assets being protected belong to the private sector, or whether the governance of cyberspace is based on existing territorial concepts of state sovereignty.

The range of threats from state and non-state actors, and the extent to which vulnerabilities across both public and private sector components of cyberspace can be exploited by these threat actors, provides a picture of risk that is the basis for much of the argument for the state's engagement in cyberspace.

3.8 Cyber Deterrence

Deterrence is a difficult concept in cyberspace with disagreement on whether it represents a useful concept, with criticism that discussing deterrence based on a domain (cyberspace) crates analytical challenges just as it would if talking about 'land deterrence' or 'sea deterrence' (Denning, 2015). However, it may be that these conceptual issues emerge from the presumption that cyberspace can be constructed as a warfighting domain in the first place (Libicki, 2012) or the presumption that a fundamentally realist construct born from the nuclear age has any meaningful application in cyberspace when it is more appropriate to acknowledge that "*Deterrence is also a weak tool in the increasingly important realm of cyberspace, where it can be extremely difficult to be absolutely sure of an attacker's identity.*" (Betts, 2013).

In its most basic form, deterrence can be defined as

> "*In international politics "deterrence" refers to efforts to avoid being deliberately attacked by using threats to inflict unacceptable harm on the attacker in response. The threatened harm can be inflicted by a stout defense, frustrating the attack or making it too costly to continue, or by turning its success into a pyrrhic victory. Or it can be*

> *inflicted through retaliation. (And through a combination of the two.) The emphasis in international politics is on providing that defense or retaliation militarily but non-military actions can also be used.*" (Morgan, 2010)

Deterrence is part of a coercive strategy in state relations with the threat of violence explicit within the deterrent. Any coercive strategy could also incorporate compellance and blackmail in addition to deterrence.

It is argued that a strategy of total deterrence fails in the cyber domain, in particular as deterrence by denial is difficult to achieve, and therefore forces deterrence strategy into one of retribution (Kello, 2018, p. 196) which is complicated by problematic attack attribution (Schmidt and Cohen, 2013, p. 105; Klimburg, 2017b, pp. 190–191; Kello, 2018, p. 199).

However, it is also argued that the fear of retaliation may be sufficient deterrent to prevent the use of offensive operations (Kugler, 2009; also cited in Valeriano and Maness, 2015, p. 47), despite the fact that anonymity and speed of effect be seen as preventing normal deterrence considerations from being effective.

Deterrence is also seen as an unrealistic approach to cyber operation as "*….credibility is lacking and actors cannot retaliate due to the uncontrollable nature of the weapon.*" (Valeriano and Maness, 2015, p. 47) This is offered as an argument for why there is restraint by cyber actors without effective cyber deterrence, also claiming that 'cyber manoeuvres' are limited by the possibility of any displayed capabilities being replicated onto the originator. By showing a capability as a means of deterrence, the capability can be copied and created by an adversary.

It is also argued that deterrence logic is weakened as the target of an attack bears some responsibility for the attack due to security failings in its cyber infrastructure. By failing to have a strong defence the logic of the deterrence processes are made inoperable (Valeriano and Maness, 2015, p. 47). Deterrence logic is also undermined by the potential for

preparatory requirements for a cyber-attack with probes or even pre-installation of software required for an attack to be effective.

Cyber deterrence logic is also weakened by a norm of non-action in response to cyber-attacks, with even many suspected state-sponsored attacks being treated as criminal acts rather than as a state-on-state cyber-attack (Valeriano and Maness, 2015, p. 47). This is of course not helped by the difficulties inherent in a system where the same groups and individuals may be acting on both a criminal and a state level and the same techniques could be present in both state-on-state and criminal attacks.

These perceived deficiencies in cyber deterrence have led to the use of an effects based measurement of a cyber-attack and an equivalence approach to retribution actions, on a kinetic basis if required (Kello, 2018, p. 196) requiring 'cross domain' deterrence with the perceived negative potential for 'spillovers' of effects from cyber to other domains which may be considered escalatory (Glaser, 2011).

The other main issue for deterrence in cyber operations is that it is effectively only applicable in a state-on-state situation which may not necessarily be the main source of conflict in cyberspace. The effectiveness of cyber deterrence against terrorist groups or criminals is likely to be limited, especially where there is little or no infrastructure that can be used as a target for retaliation.

The UK Government defined its cyber deterrence posture in the 2016 NCSS where it states that:

> "*The principles of deterrence are as applicable in cyberspace as they are in the physical sphere. The UK makes clear that the full spectrum of our capabilities will be used to deter adversaries and to deny them opportunities to attack us. However, we recognise that cyber security and resilience are in themselves a means of deterring attacks that rely on the exploitation of vulnerabilities.*
>
> *We will pursue a comprehensive national approach to cyber security and deterrence that will make the UK a harder target, reducing the benefits and raising the costs to an*

> *adversary – be they political, diplomatic, economic or strategic. We must ensure our capability and intent to respond are understood by potential adversaries in order to influence their decision-making. We shall have the tools and capabilities we need: to deny our adversaries easy opportunities to compromise our networks and systems; to understand their intent and capabilities; to defeat commodity malware threats at scale; and to respond and protect the nation in cyberspace.*" (HMG, 2016, p. 47)

This makes clear that within the bounds of proportionality, any retaliatory attack need not be limited to a cyber based attack, again raising concerns of spillover and escalation from cyber based conflict to a kinetic attack, although there is no empirical evidence to support this hypothesis in cyber-conflicts to date (Valeriano and Maness, 2015, pp. 102–103)

In 2019, then Foreign Secretary Jeremy Hunt outlined four principles for cyber deterrence (Hunt, 2019), which were; first, the identification of any actor responsible for malicious cyber activity; second, responding to any attack by publicly 'naming and shaming' the actor responsible and also exposing the tools, techniques, and practices behind the attack; third, prosecuting anyone responsible for cyber-crime; and, fourth, with allies "*…consider further steps, consistent with international law to make sure we don't just manage current cyber-attacks, but deter future ones as well.*" (Hunt, 2019) He also identified additional coercive measures including travel bans, asset freezes and economic sanctions, while highlighting GCHQ's offensive cyber capabilities and the diplomatic efforts to build a broad international coalition.

Any effective deterrent capability requires credibility in terms of both the existence of the deterrence capability and the willingness to use that capability to punish an attack. To deter, a state must provide demonstrable evidence that it is able to carry out its threat and to deny, it must have the capabilities to do so (Brantly, 2018)

In cyberspace it could be argued that deterrence by denial is not credible because of the high number of vulnerabilities in computer systems that have the potential to be exploited.

Although having the potential benefit of being a threat of a 'response in kind' as opposed to an escalatory kinetic response, a cyber based deterrent based on the threat of using a cyber-attack as punishment also presents a number of difficulties.

1. Using cyber as a deterrent capability may not be in the best interests of those who could utilise it as they may also have the most advanced and potentially vulnerable IT infrastructure. A cyber based deterrent may provide legitimacy to state cyber-attacks, and this may not be in their interest.
2. Deterrence requires credibility in the ability to apply the deterrent capability. Cyber does not necessarily allow this with the potential for both false positives and false negatives in attribution of attacks (Libicki, 2009, p. 29).
3. It is difficult to predict the effects of a retribution cyber-attack, and so "*…both the retaliator and the attacker[would] be unable to predict the effect of retaliation, neither may be entirely certain of what effect retaliation did have. If the potential retaliator doubts whether its planned retaliation will have the desired effect, it may be better off pretending that no attack occurred (quite possible in some cases) than making a big deal of the attack, revving up the retaliation machine, and having little or nothing to show for it.*" (Libicki, 2009, p. 30)
4. It relies on the accurate attribution of an adversary's actions, which remains difficult and time consuming in a cyber environment (Glaser, 2011).
5. 'Hands-tying' (i.e. no choice but to respond) and other credibility enhancing measures may be lacking in a cyber environment (Glaser, 2011).

Again, as Martin Libicki has explained, deterrence in cyberspace presents a much more ambiguous environment than that of nuclear deterrence, in that

> "*….attribution of attack was not a problem; the prospect of battle damage was clear; the 1,000th bomb could be as powerful as the first; counterforce was possible; there were no third parties to worry about; private firms were not expected to defend themselves; any hostile nuclear use crossed an acknowledged threshold; no higher levels of war existed; and both sides always had a lot to lose.*" (Libicki, 2009, p. xvi)

He cites cite a range of key questions for cyber deterrence that do not occur with respect to nuclear or conventional deterrence discussions including attribution, the effectiveness of retaliatory attacks in terms of being able to create effects sufficient to deter and to disarm the original attacker in particular where the attacker does not present a 'target rich' environment, whether third parties will stay out of the way and whether escalation can be avoided.

In a cyber context there are problems with the concept of extended deterrence, again emerging from attribution issues in that any state offering extended deterrence would want to understand the identity of the attacker, which would likely require a significant level of access to the attacked systems. It would be problematic for a state offering extended deterrence to trust the attribution claimed by the state benefiting from extended deterrence as they may have their own motives for attributing an attack to an adversary (Libicki, 2009, p. 20). Despite this, Libicki cites the re-hosting of Georgian servers in the USA in order to mitigate a DDOS stack as an example where 'extended defence' may be beneficial (Libicki, 2009, p. 130).

Given the difficulties with deterrence, the potential for the use of other coercive strategies such as cyber compellence is also problematic. Compellence is seen as the ability of one state to coerce another state into action, usually by threatening punishment. However, analysis of known cyber conflicts has shown that "*the utility of cyber operations for compellence is limited and occurs at a level consistent with other coercive instruments.*" (Jensen, Valeriano and Maness, 2017).

This confirms the limited utility of deterrence and other coercive strategies in cyberspace. The different nature of the cyber environment does not appear to support the direct application of realspace realist concepts such as deterrence, and seems to support the hypothesis that new tools and conceptual models are required to more accurately understand power relationships in the cyber domain.

4 Literature Review

This literature review identifies some of the key debates in relation to the UK state and cyber security. There are many different approaches that have been taken in other cyber security related theses, for example Herpig, 2014; Munk, 2015; Jolley, 2017, but this specific approach was selected as one that would allow a conceptually coherent review that informs the remainder of this particular thesis.

There are several issues in any cyber related literature review that are regularly encountered by researchers in this area.

Firstly, there is the sheer scale of the task in reviewing literature relating to cyberspace especially given the lack of resolution of many key debates that originated in the mid-1990s (in particular in relation to sovereignty, governance and the state in cyberspace); secondly, there is a lack of consistent terminology or even an agreed understanding as to what is meant by 'cyberspace'; third the number of different 'works in progress' related to institutional development and international agreements concerning cyberspace creates a very confusing picture of the issue area; and finally the speed at which change takes place, especially in terms of technical developments such as the Internet of Things (IoT).

This thesis has required reference to a large and eclectic literature covering a wide range of subject areas outside the cyber realm, from New Medievalism, Security Studies the nature of the state, sovereignty and authority and the theory of Wicked Problems. Reference to literature related to these elements of the thesis is not included in this review and is contained in the specific relevant chapters where necessary.

In addition, there has been a wide range and depth of cyber specific literature covering both theoretical and practical aspects of cyberspace itself and the security issues in cyberspace. This has ranged from the nature of the cyber threat, through offensive and defensive cyber capabilities, teenage hackers, hacktivists and cyber-terrorists. A large part of this literature is not relevant to this thesis except as the source of key examples that enable the main arguments to be made. The cyber-threat and the security response is one of the more difficult sections of the literature due to the rapid development of security issues in

cyberspace alongside the relevance of what could almost be considered historical documents in cyberspace terms regarding the underlying principles such as anonymity, censorship, deterrence, attack attribution, and the like. It is not unusual to see literature from 2016 and 2017 continue to reference works from 1996 and 1997 as many of the underlying concepts and analysis of the issues remain valid and many debates remain unresolved. For example, Alexander Klimburg opens his 2017 *The Darkening Web* with reference to a 1995 magazine article which he says that "*despite being written in the Stone Age of the Internet , much of what was said then, holds true today.*" (Klimburg, 2017b, p. 3) This adds significantly to the volume of literature that is available for review, but also requires careful analysis as for every statement from 1995 that holds true today there are many that clearly don't – it was the same year that Bob Metcalfe (the inventor of Ethernet and the founder of 3Com) predicted the collapse of the Internet in 1996 (Goble, 2012).

Over the past thirty years there have been many key contributions made by a large number of academics and practitioners from various backgrounds in academia, the military, private enterprise, and civil society. Cyberspace has brought many different disciplines together to produce a rich literature that informs this thesis.

The literature that represents the most complex review challenge - and potentially least valuable in the context of this thesis – is the fast-flowing technical literature regarding cyber security issues and analysis of specific attacks. The majority of this is produced by the private sector and can be highly technical in nature. This project has not been a technical cyber security project – there are more than enough of those being completed by PhD candidates in computer science departments - and while some of these technical analysis documents are referenced within the text when they can be utilised to provide evidence of an underlying principle, they are not included in detail in this thesis.

Clearly, with any state related information there are associated issues of secrecy and information availability. This has been an issue on a small number of occasions relating to a Freedom of Information request for information concerning the Huawei Cyber Security Centre which was denied for reasons of national security; access to the Cyber Information

Sharing Partnership platform (CiSP)[14] which was not possible without a corporate sponsor; and access to Government sponsored conferences and trade shows, although this final issue was eventually overcome allowing attendance at some government cyber security conferences in 2017 and 2018.

The most significant source of help with access to information that would normally be secret has been the information leaked by Edward Snowden starting in June 2013. This has provided a significant insight to state activity in cyberspace and as well as providing information that is now well analysed and commentated upon, continues to bring new secrets to light.

However, it has to be emphasised that the secrecy surrounding state cyber operations will mean that (to paraphrase Secretary Rumsfeld) there are also likely to be "*….unknown unknowns – the ones we don't know we don't know*". (DoD Press Operations, 2002). This does not negate the value of investigation into cyber issues, but it does emphasise the value of direct engagement from individuals involved in the day to day provision of cyber security in providing data for analysis.

This literature review is structured around the three connected areas of cyber sovereignty, cyber power, and cyber-governance alongside New Medievalism in the context of cyberspace and international relation.

4.1 Sources

The literature informing this project has been used from a range of sources, each of which have presented some challenges and issues.

Academic literature on the subject of cyberspace and the interconnected issues relating to cyber security and the state is spread through a wide range of academic journals from *International Studies*, and *Strategic Studies*, through *Information Security*, to *Air and Space Power* and *Military Ethics* – one of the major challenges with studying cyber related issues is that

[14] Note however that access to a commercial threat sharing platform (AlienVault's Online Threat Exchange) was obtained and used throughout the project to access detailed information on specific cyber threats. Details of the Alien Vault OTX is available at otx.alienvault.com/dashboard/new, last accessed on 15/2/2018

they extend to all aspects of modern life and are an integral part of security considerations in the twenty first century. This has produced an unmanageable volume of academic literature that claims to engage with 'cyber'.

It is only since 2016 that some cyber specific journals have started to appear, for example The Journal of Cyber Security Technology launched in 2017[15], the Oxford Journal of Cyber Security launched in late 2015[16], the Journal of Cyber Security Research, first published in 2016[17], and the Cyber Security Journal first published in 2017[18] although, almost inevitably, much of what is published in these journals to date has been technical in nature, which may be another indication of the technical bias in this subject area although there is some relief in the 2016 launch of the *Journal of Cyber Policy* which promises a more policy oriented view of cyber issues[19].

The project has also required reference to a range of government sources regarding cyberspace and particularly cyber security. These have included strategy documents such as the National Cyber Security Strategy (HMG, 2016), along with Government reviews relating to the subject (National Audit Office, 2014, 2016; HCSEC, 2017; NCSC, 2017e). Given the basis of the Copenhagen School's Securitisation theory in the speech act, a number of published speeches on cyber security from government ministers and senior individuals in state agencies have been used to identify securitising moves by the UK Government.

Cyberspace is a phenomenon that states around the world are coming to terms with, often in different ways dependant on their own culture and political systems, but it is apparent, that certainly in the more open liberal western democracies there are similarities in conceptual thinking and common approaches (especially those driven by transnational organisations such as NATO and the EU, along with the 'Five Eyes' SIGINT grouping, which means that UK policy implementation is at times informed by thinking from outside the UK. This is

[15] Details available at www.tandfonline.com/toc/tsec20/current# accessed on 14/2/2018
[16] Details available at academic.oup.com/cybersecurity accessed on 14/2/2018
[17] Details available at www.cluteinstitute.com/ojs/index.php/JCR/index accessed on 14/2/2018
[18] Details available at www.henrystewartpublications.com/csj accessed on 14/2/2018
[19] Details available at www.tandfonline.com/loi/rcyb20 accessed on 14/2/2018

particularly the case with conceptual level thinking such as that on deterrence, active defence, jurisdictional issues, and surveillance and interception.

In particular, as the founding nation of the Internet, the legislative authority behind some of the governance infrastructure (in particular ICANN), home to many of the main infrastructure providers and cyber security companies, as well as a key partner for UK state agencies, the United States would seem to have a potentially disproportionate role to play in both the global and the UK cyber security environment. This is reflected in some of the sources used in this project, for example where commentary on cyber vulnerabilities and attacks in the United States also seem relevant to a UK environment. For example, alleged issues of supply chain interference with Cisco Routers and Juniper Networks equipment by the NSA in the United States represent an example of supply chain interference by a liberal state security agency that may have effects in the UK (National Crime Agency, 2017a) but may also reflect actions that could be taken by UK agencies despite no direct example of similar interference by GCHQ.

Think Tanks have also produced some useful literature both as their own reports, for example from RUSI (Rosemont, 2016) and Chatham House (Cornish *et al.*, 2011; Hurley, 2012) in the UK and the RAND organisation in the US (Libicki, 2009; Ablon and Bogart, 2017). Frequently these reports are also turned into useful public literature, for example, the Council on Foreign Relations' Adam Segal's Hacked World Order (Segal, 2016).

Cyberspace and cyber security issues have become the subject of wide public debate. Cyber-war (in its widest context) even has its own documentary television series (Neudorf *et al.*, 2016). This public debate has served to widen the opportunity for cyber literature from both practitioners and academics to include full length works with a wide appeal. Much of this work is focused on the threat and threat response and offers a wide view of the cyber security debate to encompass privacy and surveillance alongside 'the hacker threat' and the lack of preparedness of society for the inevitable catastrophic cyber attack.

While necessarily populist, many of these works also present a specific insight from practitioners, such as former Presidential Special Advisor on Cyber Security, Richard Clarke's Cyber-war (Clarke and Knake, 2010), former Director of the NSA and Director of

the CIA General Michael Hayden's Playing to the Edge (Hayden, 2016), or Senior Counsel to the NSA and Head of US Counter Intelligence Joel Brenner's America the Vulnerable (Brenner, 2011) or also from journalists with exceptional access, for example Gordon Corera who covers security issues for the BBC and appears to have had exceptional access to HCSEC (Corera, 2015) and Glenn Greenwald who has delivered significant insights based on the Snowden documents in his work both in book form (Greenwald, 2014b) and in *The Intercept*.

Cyber security is now a large industry, estimated to be worth some $90 billion in 2017 (Muresan, 2017) with many highly respected industry organisation such as IBM, Symantec, Cisco, British Telecom and many others having a stake in this industry. The main players all have a strong output of commissioned and internal research, regular news output, weblogs, educational webinars, and detailed threat and vulnerability analysis materials, in most cases freely available. While there can be little doubt that these materials are designed to serve a commercial purpose, and they are the subject of criticism at times (Lomas, 2016a) they can also be a reliable source of information especially in terms of malware analysis and attack attribution, and the same criticism of sowing fear, uncertainty and doubt has also been laid at the door of governments (Lee and Rid, 2014).

Cyber security (at times as 'Computer Security', 'Network Security' and 'Information Security') has long been of interest to the technology community and comprehensively covered by the technical media such as *Computing*, *Computer Weekly*, *Wired*, *SC Magazine*, and *The Register*. The majority of the specialist magazines no longer produce printed copy, but are instead pure digital media outlets with only a web site as reference.

Cyber has also become a matter of more general interest, especially where it intersects with national security matters and there is regular coverage in respected general media such as the UK quality Press – in particular *The Guardian* who first reported the Snowden material, and from the United States, *Forbes*, the *Wall Street Journal* and *New York Times*.

There are also a number of reliable internet based sources used within this project. This includes 'blogs' such as *Schneier on Security,*[20] *The CipherBrief*[21]*s, (*an online information feed run under the auspices of former NSA Director General Michael Hayden*),* the NCSC Blog, and other industry weblogs such as Microsoft, Kaspersky, Symantec, among others.

There are also a number of online magazines associated with the subject that have proved valuable 'pointers' to trends in cyber security, perhaps most importantly *Dark Reading*[22] and *The Hacker News*[23] and *Recorded Future*[24].

Finally, there are a number of collaborative practitioner-based groups that have proved useful both for connecting with people in the cyber security industry, and again as pointers to specific information. This has included (to varying degrees) *Intelligence Based Cyber Security*[25], *Cyber Intelligence Network*[26], *Cyber Security*[27], and the *Cyber Security Forum Initiative (CSFI)*[28].

4.2 Cyberspace and Sovereignty

There is an extensive literature on the relationship between cyber space and national sovereignty that has been developed throughout the history of the Internet, although the effects of electronic communication on the structure of the relationships between states has been recognised since the first proposals for a transatlantic telegraph cable in the 1840's (Standage, 1998, p. 136).

The Internet that emerged in the 1990's exhibited a very different approach to the relationship between electronic communication and the state as shown by Barlow's libertarian Declaration of the Independence of Cyberspace (Barlow, 1996) which presented the communications environment as a 'space' in its own right which was independent of

[20] Available at www.schneier.com accessed on 14/2/2018
[21] Available at www.thecipherbrief.com accessed on 15/2/2018
[22] Available at www.darkreading.com/Default.asp accessed on15/2/2018
[23] Available at www.thehackernews.com accessed on 15/2/2018
[24] Available at www.recordedfuture.com accessed on 15/2/2018
[25] Available at www.linkedin.com/groups/2302719 last accessed on 15/2/2018
[26] Available at www.linkedin.com/groups/1765567 last accessed on 15/2/2018
[27] Available at www.linkedin.com/groups/3821801 last accessed on 15/2/2018
[28] Available at www.linkedin.com/groups/1836487 last accessed on 15/2/2018

state influence and sovereignty. Developments since that time have shown firstly that the sovereignty of the nation state cannot be so easily dismissed, but it has also shown the complexity of applying a physical territorially based concept to a virtual environment. In its basic form debates about sovereignty remain not that different from those in the 1990's although it is now far more nuanced, with an acknowledgment that although cyberspace may be a force that might negatively affect the integrity of territorial sovereignty it may also be an instrument of control through which states can strengthen their territorial sovereignty, so the effects of cyberspace on state sovereignty have not proved as one dimensional as might have been envisaged and the nation-state itself is proving far more resilient in the face of cyber effects than originally predicted (Betz and Stevens, 2011 loc 1079).

These effect of cyberspace on sovereignty has been analysed by Betz and Stevens with reference to four understandings of sovereignty argued by Stephen Krasner (Krasner, 1999 cited in Betz and Stevens (2011) loc 1107; and in Franzese, 2009) of domestic sovereignty, interdependence sovereignty, international legal sovereignty and Westphalian sovereignty.

They argue that cyberspace does not erode all forms of sovereignty, with almost no effect on international legal sovereignty, some implications for Westphalian sovereignty and its most significant impact on interdependence sovereignty due to transnational information flows with a resulting impact on domestic sovereignty.

States have reacted to any perceived impact on sovereignty in a way that has been described as a "*double move*" of "*…the territorialisation of cyberspace and the de-territorialisation of state security…..*" (Herrera, 2008) meaning that the elements of cyberspace that enable its 'statelessness' are increasingly being territorialised in that "*the very nature of cyberspace has been shaped by geopolitics.*" (Herrera, 2008, p. 74) and that increasing controls are being placed in cyberspace to allow for its control on a territorial basis. This includes 'trusted computing' initiatives that remove anonymity, digital rights management as an example of how realspace controls are implemented in cyberspace for intellectual property, and the use of firewalls and filtering at a national level to control the movement of information across territorial borders.

The de-territorialisation of state security can be seen in the use of technologies such as Radio Frequency Identification (RFID) chips and Global Positioning System (GPS) systems that are enabling technologies for growth in mass state surveillance. The use of RFID in banknotes as a way to control the cash economy is described as "*a perfect illustration of the double edged nature of digital information technologies: they give unprecedented power to private citizens but they also empower states.*" (Herrera, 2008, p. 82).

Other discussions regarding the (re-)establishment of state sovereignty in cyberspace have included analysis of data protection regulation (Bendrath, 2007), data localisation (Nugraha, Kautsarina and Sastrosubroto, 2015) access control (Deibert *et al.*, 2010a; Internet Society, 2012a; Deibert, 2013), so called 'Balkanisation' or 'Splinternet' initiatives (Healey, 2011; Malcolmson, 2017), filtering of content (Betz and Stevens, 2011; Pariser, 2011; Internet Society, 2012a; Nichols, 2016) and the territorialisation of cyberspace (Lambach, 2016). All these innovations suggest that the state is establishing a more significant future role in cyberspace regulation. The re-assertion of state level sovereignty has been described as having been accelerated by the Snowden revelations and a desire for states to protect their cyber borders from surveillance by the United States (Liaropoulos, 2017).

The assumption that the Internet was a significant threat to sovereignty is also challenged on that basis that the Internet has the potential to enhance sovereignty through strengthening international law, strengthening economic interdependence empowering non-governmental organisations and supporting international security mechanisms. This was supported by the assertion that the Internet did not threaten all states equally and that such an argument depends on a specific conception of sovereignty, while the difference between liberal and non-liberal states is also a difference in the threat of the internet to their conception of sovereignty with liberal states less likely to be threatened, and with the potential for sovereignty to be enhanced (Perritt Jr., 1998).

However, there are good examples where cyberspace has challenged territorial sovereignty in law. The sale of Nazi memorabilia in France through Yahoo was prohibited by a French court and then protected by a US court on First Amendment grounds, thus effectively preventing French law from applying in France for a system provided from the United

States (Adams and Albakajai, 2016). There is, however, a strong case argued that this type of 'regulatory leakage' at borders is not specific to cyberspace and is analogous to air pollution being blown across borders by the wind. "*…territorial regulation of the internet is no less feasible and no less legitimate than territorial regulation of non-Internet transactions." Regulating these trans-border situations may require a different approach, but it does not mean the end of territorial sovereignty*" (Goldsmith, 1998).

This is indicative of one of the great difficulties inherent to many debates concerning cyberspace, which is whether the issues are specific to cyberspace or whether they are merely a cyber example of factors that apply equally in a physical 'realspace' and a cyber environment. This has been an element of debates on cyber-law with Easterbrook's example of the law of the horse (Easterbrook, 1996); cyber-crime which was described as "*old wine in new bottles*" (Grabosky, 2001) as well as long debates on cyber-war and when a cyber-attack is equivalent to the use of kinetic force and when a kinetic response is justified (Schmitt, 2012a; Hackett, 2015 are examples among many others.).

The influence of territorial sovereignty in cyberspace is also argued from the perspective that targets for cyber-attacks are located in physical space, creating additional complexity in terms of the physical points of attack origin and the point of attack occurrence (Brenner, 2007a), and the fact that the infrastructure of cyberspace in terms of cables, server farms, satellite earth stations and the like, as well as the users of cyberspace, are located in physical space which means they are subject to the usual realspace sovereignty and territorial considerations (Cohen, 2007; Sheldon, 2014). The importance of the physical location of cyberspace infrastructure was clearly shown when the Egyptian government succeeded in shutting down Internet services in 2011 (DeNardis, 2014, pp. 212–3).

However, territorial sovereignty also breaks down in cyberspace due to the complexity of territorial regulation being applied to systems that operate on a non-territorial basis. This creates a patchwork of overlapping authorities that is Medieval in nature. As Bruce Schneier explains "*You're going to be affected by the rules of the country your hardware manufacturer lives in, the rules of the country your software vendor lives in, and the rules of the country your online cloud application provide lives in. You're going to be affected by the rules of the country where your*

data resides, and the rules of whatever countries your data passes through as it moves around the Internet." (Schneier, 2015, p. 259)

As a result, at any point in time and place cyberspace is subject to multiple regulatory authorities from many other times and places.

There is an alternative view that is part of the sovereignty debate that cyberspace can be seen as a 'global commons' equivalent (or at least analogous) to sea and space which supports the idea that state sovereignty should have a limited role in cyberspace (Liaropoulos, 2017). This view seems to have been initiated by the United States government, with particular reference in a 2010 speech by Hillary Clinton in which she referred to the Internet as a 'global networked commons' (Schonfeld, 2010). This view of cyberspace as a global commons was also in line with cyberspace being defined as a military domain of operations, making military cyber power analogous to sea power and air power. It may be suggested that the historical Western dominance of these traditional commons environments has influenced the view of cyberspace as a global commons (Betz and Stevens, 2011 loc 2040) and it has been a theme in some US cyber policy inputs such as a State Department report on Frameworks for International Cyber Stability (International Security Advisory Board, 2014).

Cyberspace as a global commons is a contested concept (Cornish, 2015) as it does not meet the legal criteria of a global commons and has the significant issue of consisting almost completely of privately owned infrastructure, and is "*…not a place in the sense geographers conceived of the global commons as specific tangible 'resource domains outside the jurisdiction of any one state'….*" (Betz and Stevens, 2011 loc 2120). It has also been argued that cyberspace does not possess the defining characteristics of a global commons (a governing international treaty, permissible uses and prohibitions, definable with boundaries, states forgoing claims of sovereignty, and no state capable of controlling the global commons) and that states' competing interest in security will "*cause them to want to assert control in cyberspace*" (Franzese, 2009).

Cornish however, goes on to suggest that even if cyberspace does not meet the criteria of a global commons "*….the users of cyberspace act increasingly as if it were held in common ownership*

and as if they have inalienable rights to use it." (Cornish, 2015) This potentially further complicates sovereignty debates when the population acts as if cyberspace is a commons, but state authorities act as if it is subject to territorially based control.

One issue with many of the discussions about the effects of cyberspace is that they are predicated on a specific understanding of cyberspace in terms of both its capabilities and technical underpinnings; neither of which are necessarily consistent over time as they change in line with technological developments. This has the effect of ensuring that cyberspace is a 'moving target' for analysis.

This is already clear in terms of the new technical capabilities that have been applied in cyberspace that have an impact on sovereignty, for example, the development of DNS filtering that has enabled the Balkanisation of the Internet using traditional territorial nation state based divisions or allowed for location dependant access to content. Slightly more complex will be the issues arising from the development and implementation of optical satellite to satellite communication to provide a backbone transmission network that is subject to space treaties rather than any terrestrial constraints. Given the argument that sovereignty can be derived from the physical location of routers and switches within territorial authorities, the removal of that constraint could be expected to have an (as yet undefined) impact.

It is also difficult to talk about cyberspace sovereignty in any cohesive way due to the different underpinnings of different elements of cyberspace, most clearly shown by the difference between the telephone network (and related infrastructure) and the Internet (which utilises the same cable and satellite infrastructure of the telephone network), with the physical infrastructure seen as a significant factor in enabling territorial sovereignty over communications networks for example due to the ability of states to regulate territorially based infrastructure (Herrera, 2008).

4.3 Cyberspace Governance

The cyberspace governance debate has been characterised as a choice between a state-based multi-lateral governance system, with support for such an approach characterised as non-

Western and authoritarian, and a multi-stakeholder governance system advocated by the United States and other western nations.

This debate about the governance of cyber space is strongly connected to discussions concerning sovereignty, in that state sovereignty is implicit in state-based governance models of cyberspace and any multi-stakeholder approach can be seen as impinging on state sovereignty. The debate generally suffers from a focus on Internet governance which, at times, ignores the complexities inherent in cyberspace in that it also engages various transmission infrastructures (satellite, microwave, mobile communications) as well as established governance models around the telecommunications networks and infrastructure on a national and international basis.

There is little discussion about changing the way in which the telecommunications infrastructure is managed. This may reflect a view that the governance systems of the UN and ITU that control the telecommunications environment are established to a point beyond useful debate, however, the lack of consideration of the inter-relationship between the two may be a weakness in the discussion given that there is already competition between the existing Internet governance institutions and the ITU in addressing future networking issues, for example through the ITU's Network 2030 initiative (ITU FG-Net-2030, 2020).

Lawrence Solum identifies five models of Internet governance including the Internet as a self-governing realm of individual liberty, beyond the reach of government control; governance through transnational institutions and international organisations; governance by code and Internet architecture that determine how the Internet operates; governance by national governments and law and finally governance by market regulation and economics which assumes that market forces drive the fundamental decisions about the nature of the Internet (Solum, 2009).

Solum's analysis of the five models leads to a conclusion that "*…the optimal system of governance is a combination of regulation by transnational institutions, respect for the architecture that creates transparency, national regulation, and markets.*" (Solum, 2009)

This hybrid model of collective governance is supported by Denardis and Musiani, with the notable absence of the Internet as a self-governing entity when they describe Internet governance as something that "*…..transcends traditional government-centric mechanisms like national statutes or intergovernmental treaties…..*" and is "*….collectively enacted by the design of technology, the policies of private companies, and the administrative functions of new global institutions like ICANN and the Internet Engineering Task Force (IETF), as well as national laws and international agreements.*" (Denardis and Musiani, 2014)

This 'hybrid model' of overlapping multiple authorities is one that again points to cyberspace as an environment that has the governance characteristics of New Medievalism.

The idea that code regulates the Internet is one most often associated with Lawrence Lessig and the subject of a number of articles and books (Lessig, 1999, 2000, 2006). The underlying idea being that the software that determines the operation of the Internet can be considered to be governing the Internet through the rules that are enforced through what is coded. In many ways it is undeniable that the software and protocols that determine the operation of the Internet are providing a level of governance, but the code is increasingly needing to operate within the context of state regulation that constrains the operation of code, creating a set of overlapping and at times contradictory governance systems (Penney, 2015) and all software and hardware is built within the constraints of a territorially regulated environment (Schneier, 2015)

Describing the relationship between 'code' and the state, Solum states that "*No national government has made a serious attempt to change the fundamental architecture of the Internet's code*" (Solum, 2009, p. 69) although in more recent times the UK NCSC has embarked upon a process of instituting changes to both the Internet's Border Gateway Protocol (BGP) and the telecommunications network's Signalling System N°7 (SS7) (Levy, 2016b) despite reports of significant objections from the private sector (McGoogan, 2016). Although there is no public information available concerning this implementation it was referred to by the Head of the NCSC when he listed one of the achievments of the

NCSC's Active Cyber Defence Program as *"…getting our telecoms industry to agree to update a key protocol to make it much harder to use UK infrastructure in DDOS attacks."*(Martin, 2017a).

This initiative was despite the IETF also working on multiple approaches to resolving the BGP security flaws (NIST, 2017), although research in 2017 concluded "*insurmountable obstacles*" to 'BGPsec' deployment and very slow progress on other initiatives (Gilad *et al.*, 2017).

This change to the code of cyberspace is a fundamentally different state intervention in cyber-governance from the more common mechanisms of control, such as firewalls, IP address blacklists and DNS filters or other territorially enforceable actions such as enforcing software to be installed on publicly accessible computers, shutting down internet cafés and the like, and shows how the governance debate along with sovereignty is subject to technical change.

However, there has, since the early days of the Internet been a view that there was a need for 'law' to govern cyberspace, with important contributions from David Post and David Johnson (Post, 1995; Johnson and Post, 1996) but, applied with a contextual understanding of cyber space as a distinct space with laws that applied to that space and "*…will not, could not, and should not be the same law as that applicable to physical, geographically defined territories.*" (Johnson and Post, 1996, p. 1402).

However, this is subject to the argument that whatever the laws governing the virtual world of cyberspace, eventually actions in cyberspace interact with the physical world either through the physical infrastructure of cyberspace that is subject to the laws of the territories in which it is located, or the people who are initiating the actions – who again are also subject to the laws of the territory in which they are located (Cohen, 2007; Sheldon, 2014). This is the basis of the argument for state based governance of cyberspace.

The main propositions for state based governance of the Internet have been based around United Nations (UN) organisations such as the International Telecommunications Union (ITU), which would potentially see governance of the Internet and the telecommunications network unified under the ITU's jurisdiction. However, there remains no agreement on the

future of Internet governance. The UN sponsored 2003 World Summit on the Information Society (WSIS) tried (and failed) to reach an agreement on Internet Governance, but agreed that states, the private sector, civil society, inter-governmental organisations and international organisations all had important roles to play in governance (International Telecommunications Union, 2003).

WSIS also saw the formation of the Internet Governance Forum to continue the discussion on governance, (Mueller, Mathiason and Klein, 2007) but that has since become highly politicised with complaints that the constituent group representatives are being replaced with individuals identified through an opaque UN internal process (McCarthy, 2016). However, the UN formed Working Group on Internet Governance (WGIG) did at least produce a usable Internet governance definition of:

> *"Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet"* (WGIG, 2005).

However, cyberspace governance remains an open and contested situation, with even supposedly successful collective agreements such as the Budapest Cybercrime Convention ratified by only 61 states as of August 2018 (Council of Europe, 2018) and lacking support from Russia and China on the basis that it violates state sovereignty, even though the treaty allows states to opt out of any cooperation "*…if a request infringes on sovereignty, security, or other critical interests.*" (Segal, 2016, p. 96). In general the states based model is treated with apprehension by the Internet community and by the United States as the key proponents of the alternative multi-stakeholder model (DeNardis, 2014, pp. 32–34).

However, research has indicated that multi-stakeholder governance is ill defined as a governance system, and that different types of governance, and even different types of multi-stakeholder governance may be required for Internet governance along with different participants in the governance process as cyberspace is integrated into new areas of activity. It concluded that there may be different modes of governance required for different functional areas of Internet governance (Raymond and DeNardis, 2016). This echoes the

conclusions of Chang and Grabosky in relation to cyber security (Chang and Grabosky, 2017) that there can be no single solution that can be applied. These conclusions add weight to the view that cyber-governance (and in particular cyber security governance) can be understood as a 'wicked problem' (Clemente, 2011; Malone and Malone, 2013).

DeNardis also describes Internet governance as enacted via various routes including the technical design decisions, private corporate policies, global institutions, national law and policies and international treaties (DeNardis, 2014, p. 23). This list again shows the overlapping and at times conflicting authorities engaged in the governance of cyberspace as well as different approaches to governance within cyberspace, for example, the idea that governance of content on the Internet (propaganda, radicalisation material, child pornography and the like) can be outsourced to private corporations as a form of privatised governance is inevitably difficult in that it asks private profit motivated organisations to mediate speech on behalf of the State (DeNardis, 2014, pp. 171–2).

Cyber security also faces similar governance issues, in particular in relation to the engagement of the private sector in delivering the cyber security necessary for national security. This has been extensively written about in relation to the private sector ownership of critical national infrastructure and the inevitable engagement of the private sector in delivering cyber security at a level that is essential to national security (Brenner, 2007b, 2011, 2013; Libicki, 2007; Clarke and Knake, 2010; Brenner and Clarke, 2014; Richards, 2014; Segal, 2016).

In the UK, the state, and in particular Government Communications Headquarters (GCHQ), has taken an increasingly proactive role in delivering cyber security, expanding from the original Computer Emergency Response (CERT) and the Information Assurance mission for the UK Government and associated responsibilities such as the Computer Security Incident Response Team (CSIRT) organisations. This has been achieved through an identifiable process of securitisation of cyberspace with the inclusion of cyber within the National Security Strategy (NSS), the development of a National Cyber Security Strategy (NCSS), and the introduction of the National Cyber Security Centre (NCSC) as part of GCHQ.

However, the cyber security regulatory space remains contested and as Chang and Grabosky argue, "*the appropriate institutional configuration for cyber security will vary over time and space depending on the security setting in question and the prevailing capacities of individual participants.*" This leads to a the conclusion that there is no "*one size fits all*" solution for the governance of cyber security (Chang and Grabosky, 2017)

There is also a change in power structures brought about by cyberspace, with a loss of historic power over information flows with states and corporations both seen as losing control of their information, whether through copyright infringement or leaking of sensitive state information (DeNardis, 2014, p. 10).

4.4 Cyber Power

Power itself is a contested concept (Nye, 2011, p. 5) and it is perhaps even more so when it comes to power in cyberspace, and as a result, there are a number of interconnected but fundamentally different debates concerning cyber power.

An initial distinction needs to be made between power that can be exercised *IN* cyberspace and power that can be exercised *THROUGH* cyberspace. Nye refers to this as producing "*….preferred outcomes within cyberspace…*" or using "*….cyber instruments to produce preferred outcomes in other domains outside cyberspace.*" (Nye, 2011, p. 123) Nye also identifies targets of cyber power as intra-cyberspace and extra-cyberspace, while dividing instruments of power into 'physical' and 'information' showing that physical power resources can be brought to bear in the cyber domain.

Alexander Klimburg defines cyber power as having three dimensions "*….coordination of operational and policy aspects across governmental structures, coherency of policy through international alliances and legal frameworks, and cooperation of non-state cyber actors.*" (Klimburg, 2011)

This provides a focus on cyber capacity building as an indication of cyber power, rather than any behavioural outcomes achieved through cyber power. It does have the advantage of acknowledging the key issue that non-state actors are fundamental to state cyber power through the ownership and operation of much of a state's cyber capacity.

Other definitions see cyber power solely in terms of the effects it can produce in other domains (Kuehl, 2009), for example, "….*the ability to use cyberspace to create advantages and influence events in all the other operational environments and across the instruments of power.*" (Kramer, Starr and Wentz, 2009) This is further emphasised by Starr's model that focuses on use of cyber infrastructure to enable the PIME/DIME existing levers of power. (Starr, 2009a, p. 47)

An investigation into the relationship between cyber power and national power (van Vuuren *et al.*, 2016) concluded that cyber power is "*…best understood more as a way of achieving national power, than simply a means or attribute of national power…*" and that cyber power "*…is not an isolated element of national power, but rather a set of characteristics that are embedded in all elements of national power.*" This definition encapsulates the multi-faceted nature of cyber power as a means by which national power can be asserted and as a tool that enhances other elements of national power, suggesting that cyber power can be used to achieve effects in cyberspace and in realspace and described as "*the sum of strategic effects generated by cyber operations in and from cyberspace.*" This also recognises cyberspace as one of the five domains (alongside air, land, sea, and space) in which power can be projected (Rowland, Rice and Shenoi, 2014).

There is an ongoing debate concerning whether cyberspace enhances or diminishes state power, and whether it provides an asymmetric advantage to smaller states, and non-state actors or whether it enhances the power of larger states. This drives a strong connection between cyberspace governance arguments and cyber power, in particular in that the multi-stakeholder approach is seen as enhancing US and Western cyber power, in particular through the use of the Internet to spread ideas that might be considered subversive by authoritarian states and to enable citizens of all states to connect and share information.

Added to this, the ability of virtual (non-territorial) capabilities to create physical (territorial) effects (i.e. the extra territorial projection of power through cyberspace) is one of the most significant issues for cyberspace and fundamental to the debate concerning cyber power in relation to the use of force and cyber-attack in terms of the resulting attribution difficulties and the separation of the origin of attack and the point of attack occurrence (Brenner, 2013).

In this context there is a significant debate about the effect that cyberspace has on the relative power of the state in relation to non-state actors. Joseph Nye Jr sees cyberspace as having a strong element of power diffusion away from the state and enhancing the capabilities of non-state actors (Nye, 2010).

There are a number of elements to this, including cyber as a force-multiplier for non-state actors, the offensive bias of cyber, the relative vulnerability of a strong power society that is heavily dependent on Information Technology and the low cost of entry for non-state actors wanted to use cyber power to exert influence, for example through the rental of DDOS attacks or the hiring of black-hat hackers for attacks on cyber infrastructure. This dichotomy of cyber power has been emphasised in the context of military power (Starr, 2009b, p. 59) and the vulnerability inherent in cyberspace was incorporated into Booz Allen Hamilton's Cyber Power Index, which evaluated cyber power on the basis of a range of cyber capacity elements and where cyber power was defined as "*….the ability to withstand cyber-attacks and to deploy the digital infrastructure necessary for a productive and secure economy.*" (Booz Allen Hamilton, 2011)

Alternative views suggest that the increasing complexity of engaging in any coercive cyber activity (as evidenced by the Stuxnet malware) may indicate a higher than imagined cost to develop the tools of cyber power and that, certainly as far as military power goes, cyber power does not fundamentally change its nature and in fact "*….shored up the existing distribution of military power rather than undermining it*" (Betz, 2012)

This diffusion of power has also been a key element of debates about the role that cyberspace plays in civil society, its engagement in the 'colour revolutions' and the spread of ideas that are considered subversive in certain states. In these areas, cyberspace has been seen as a direct challenge to state power and control.

The other side of this debate has been based on a view that cyberspace has enabled the development of more powerful instruments of state control, in particular surveillance to such an extent that cyberspace is a force that enhances state power rather than diffuses it to the extent that Julian Assange (who is not one for understatement) declared that "*The Internet, our greatest tool of emancipation, has been transformed into the most dangerous facilitator*

of totalitarianism we have ever seen. The Internet is a threat to human civilisation." (Assange, 2012, p. 1)

A less apocalyptic working of the same underlying theme is found in Evgeny Morozov's *The Net Delusion* which details many of the state controls that have been used to limit freedom of expression in cyberspace and the effectiveness of totalitarian state activity in cyberspace to limit dissent with the active assistance of western corporations (Morozov, 2011).

Measuring state cyber-power is extremely complex, in part because the complexities inherent in the fact that the more cyber capability that exists the more vulnerabilities may also exist (Brenner, 2011; Goldsmith and Russell, 2018) and little analysis of how cyber-power can be maintained given the proliferation of cyber capabilities through use or theft, the weaknesses inherent in the shared responsibilities for cyber security and the underlying security failings of the technical architectures on which the internet (and the telecommunications networks) are based.

However, it is clear that the power instruments available to state and non-state actors have become increasingly important in cyberspace, as a means for states to influence one another, for non-state actors to influence states, and for states to influence the behaviour of non-state actors, including its own citizens as well as citizens of other states. With the ability to project power non-territorially, issues of sovereignty and the complexity of the overlapping authorities involved in cyberspace governance, the literature suggests a multi-pronged challenge to the state in cyberspace.

4.5 Cyberspace, International Relations and New Medievalism

There is, by comparison to the morass of realspace IR literature, little that specifically addresses International Relations and cyberspace. There is even less that addresses understanding state and non-state relationships within cyberspace. It should be noted that the use of New Medievalism in this thesis is solely concerned with using theory to help understand relationships ***within*** cyberspace. It is important to note that there is no implication that cyberspace somehow makes realspace resemble a New Medieval environment.

Although "*…there is an evident need for scholars of international relations and security to contribute to the theoretical evaluation of the cyber revolution.*" (Kello, 2013) the literature points to the lack of contributions that try to provide any IR analysis of cyber security. In '*The Anarchical Society at 40'*, Madeline Carr states that

> "*…there have been surprisingly few attempts to employ International relations theory, concepts, and ideas for understanding the landscape of cyber (in) security. Most of the existing work on this emerges from scholars working on military doctrine or strategic studies with a particular (and somewhat repetitive) emphasis on the writings of Clausewitz.*" (Carr, 2017)

In the same essay on attribution on cyberspace she goes on to suggest that returning to enduring IR thinkers may help attempts to understand some of the issues involved. This is very much the approach taken in the use of New Medievalism in this project.

Lucas Kello has also argued that there is a scholarship gap in the international relations discipline's consideration of cyberspace (Kello, 2013, 2018), citing issues of data reliability (for example due to secrecy and threat inflation), technical complexity of the issues, and the rapid pace of technological change as key to inhibiting study of this area, and repeats the concerns regarding the continued academic emphasis on Clausewitzian concepts of conflict when "*…the traditionalist lens of interstate violence reveal merely what the cyber issue is* ***not****: it is dissimilar to armed attack, military conquest, physical coercion.*" (Kello, 2018, p. 56)

The traditional and tired Clausewitzian analysis is of little help in understanding conflict in cyberspace.

When talking about the use of International Relations to study cyberspace Nazli Choucri states that "*…Cyberspace has created new conditions for which there are no clear precedents.*" (Choucri, 2012a, p. 14) She goes on to make the point that cyberspace enables new actors, but also provides new capabilities for existing state actors.

Part of the issue with literature in this area is that much of the theory concerning cyberspace engages with the impact that cyberspace has on realspace relations, in particular with cyberspace as an instrument of globalisation (for eample, Nye, 2004) and as Nazli Choucri

stated, "*…interactions in this virtual domain have catapulted to the realm of high politics and are at the forefront of almost all major issues in international relations…*" (Choucri, 2012b).

While it is acknowledged that the impact of cyber interactions on the realspace international order is clearly important (perhaps even more important) than that in cyberspace, it is not the subject of this thesis which looks to restrict any analysis to relationships within cyberspace. The fact that the two are different is widely acknowledged, with Choucri again stating that "*…cyberpolitics in this domain cannot be reduced to a mirror image of interactions in world politics as conventionally understood.*" (Choucri, 2012b). Different approaches are required in the cyber domain.

There is general agreement on why cyberspace is different in its effect on realspace international relations, which, as articulated by Choucri, includes issues of temporality, and physicality, (meaning that activities undertaken or decisions made are not constrained by geography, spatial consideration, or sovereign boundaries), permeation, (activities which penetrate state boundaries); fluidity, "*…the ease with which shifts in patterns of interactions take place…*"; participation (reduction in barriers to activism and political expression); attribution; and accountability (or the lack of accountability due to the lack of reliable attribution) (Choucri, 2012b).

Lucas Kello (Kello, 2018) argues that cyber-politics exists in "*two states of nature*", with one being a traditional realist view of states competing for security but with the complication of a weapon of unknown effects, the second being a "*chaotic global milieu comprising non-traditional players whose aims and motives may be subversive of national or international order and who may not accept or even understand…..the anarchic states system*" (Kello, 2018, p. 12)

This seems indicative of the different ways in which cyberspace is treated, in particular as an extension of realspace. Although it is arguable that cyberspace and realspace relations are becoming more closely aligned, but this does not mean that they are the same. As Choucri states, "*…increasingly "close coupling" between the traditional and cyber politics in international relations, reflecting the growing interconnections between two initially distinct and separate arenas of interactions. By definition, "close coupling" does not necessarily imply mirror-image dynamics.*" (Choucri, 2012b)

The use of New Medievalism as a mechanism through which to describe cyberspace is not aimed at explaining traditional inter-state relations at the virtual level. It is specifically trying to show how the authority of the state in cyberspace is diminished by the attributes of cyberspace. In order to show that New Medievalism represents an accurate description of cyberspace, key attributes of New Medievalism (as described by Hedley Bull (Bull, 1977) and Philip Cerny (Cerny, 1998) have been analysed to show how they are reflected in a cyber environment.

There are of course other theories that could be applied to cyberspace. Joseph Nye has written about cyber governance as a regime complex in the context of regime theory (Nye, 2014). This mapping of cyber governance institutions as a regime complex is interesting and takes account of the dependence on norms and non-state institutions in cyberspace.

International regimes in general are described as "*...the sets of governing arrangements that affect relationships of interdependence…*" This would include "*…networks of rules, norms, and procedures that regularise behaviour and control its effects.*" Keohane and Nye describe these rules as not as well defined or well enforced in an international environment as in domestic environments and argue that institutions are not as powerful or so autonomous. The overall environment includes international rules, national rules, private rules, and the absence of rules which could be to the extent that where "*…there are no agreed norms and procedures or when the exceptions to the rules are more important than the instances of adherence, there is a non-regime situation.*" (Keohane and Nye, 1989, pp. 19–20).

While governance in cyberspace is developing rapidly I would argue that if (on the basis of these definitions) regime theory is applicable, it remains arguable that it represents a non-regime situation due to the absence of norms of behaviour for states and the asymmetric and anonymous attributes that allow non-state actors behaving outside the rules to have a disproportionate and significant effect on the effectiveness of cyber governance.

I would argue that New Medievalism (as determined by the attributes adopted in this thesis) represents at best a weak governance regime, but with so many exceptions that it is best viewed as a non-regime situation and so, is appropriate for consideration as a model for analysis of the cyberspace governance environment.

Within their introduction of regime theory, Nye and Keohane also make a compelling case for why the "*assumptions of political realists are often an inadequate basis for analysing the politics of interdependence.*"(Keohane and Nye, 1989, p. 23). This is on the basis that realist assumptions include that states are dominant actors in world politics; that states are coherent units; that force is a usable and effective instrument of policy; and that there is a hierarchy of issues headed by military security, above issues of economic and social affairs. (Keohane and Nye, 1989, pp. 23–24). They go on to define "*characteristics of complex interdependence*" which include actors other than states participating directly in world politics, no clear hierarchy of issues, and force as an ineffective policy instrument (Keohane and Nye, 1989, p. 24).

If we accept that governance of cyberspace is strengthening at this time, it may best be viewed as being in a state of transition between a non-regime situation and an international regime of complex interdependence.

However, there is no reason why a New Medieval lens through which to view cyberspace should be considered contradictory to a regime complex view. It is a very similar analysis that leads to both conclusions, and it could be argued that New Medievalism is a description of the weak regime complex that currently exists in cyberspace.

There is an argument to be made that realist assumptions are becoming more appropriate for cyberspace as states start to take a more significant role in cyber governance and accelerate their adoption of cyberspace as a tool through which they can enact realspace policies. This is a result of cyberspace becoming more fundamental to state policies, both in terms of economic success, delivery of state services, and national security. This change to state engagement in cyberspace is supported by Keohane and Nye's view that issues may usefully be analysed on the basis of complex interdependence until they become a matter of life and death. It is at that point that "*realist assumptions would then be more relevant*" (Keohane and Nye, 1989, p. 29). The increasing importance of cyberspace in economic, political, and security spheres would suggest that development in line with realist theory is likely in the future. Certainly, the growth of state activity, in particular in terms of their use of offensive cyber capabilities in state-on-state conflicts, suggests this may be the case.

The analysis that leads to the regime complex understanding is not dissimilar from the analysis undertaken for this thesis, and the weakness of the overall governance is reflected in the prediction that "*…cyberspace is likely to remain a regime complex rather than a single, strong regime for some time.*" (Nye, 2014) One element missing from Nye's analysis however is the regulatory influence of code in cyberspace. In the context of the regulation of actions in cyberspace, Lessig argues that "*This regulator is code--the software and hardware that make cyberspace as it is.*" (Lessig, 2000) He goes on to refer to the code that implements TCP/IP and say that "*These architectural features of the Internet mean that governments are relatively disabled in their ability to regulate behavior on the Net.*" (Lessig, 2000) This assigns a huge governance capability to code and the creators of the code that is not necessarily considered in Nye's regime complex.

There are a number of salient criticisms of regime theory including firstly that it is too state centric (Strange, 1983, p. 349), although in this instance Nye's analysis does emphasise the influence of non-state actors within the regime complex, and in fact rejects the hegemonic transition theory that would suggest that the regime is developing as a result of the decline of the previously hegemonic US influence in cyberspace; secondly that it is too imprecise a concept and that the concept of a regime can be constructed to mean almost anything (Strange, 1983, p. 342); third that the concept is too static a view (Strange, 1983, p. 346), and this is certainly a problem in cyberspace where technology changes at a rapid pace and new regulations, new code, new RFCs from the IETF and many other elements all have the potential to change the nature of the regime complex, especially when there are such fundamental disagreements between the multi-lateralist and the multi-stakeholder point of view. This pace of change leads Nye to identify the issues of technology and other changes that "*are affecting how state and non-state actors understand and define their interests*" (Nye, 2014).

Susan Strange also contests the suitability of the word 'regime' as it implies an "*…exaggerated measure of predictability and order in the system as it is…*" and that it is "*…value loaded in that it takes for granted that what everyone wants is more and better regimes, that greater order and managed interdependence should be the collective goal.*" (Strange, 1983, p. 345)

This may be a valid criticism with respect to the application of regime theory to cyberspace and Nye certainly seems to suggest a desire for Susan Strange's "*more and better regimes*" with reference to the evolution of the current regime complex in different sub-issues through a series of regime developments from interstate agreements, use of trade agreements, through to coordinated action by *'like-minded states'*. (Nye, 2014)

One of the difficulties with an analysis of cyberspace as a distinct environment is that states have developed a view of cyberspace as a domain of military operations akin to air, land, and sea (and latterly space). This has the result that state action in cyberspace merely tries to replicate state realspace actions, so arguments concerning the theory that best applies to state relationships in realspace can be seen by extension as also applying to cyberspace. In a discussion about security and state-on-state conflict, this tends to favour realist state centric interpretations of the international environment.

The supposed anarchic nature of cyberspace also plays to a realist interpretation with some going as far as to state that "*…anarchy and its effects describe cyberspace well.*" And that "*…cyberspace lacks effective global institutional governance*" (Valeriano and Craig, 2018) despite the fact that this interpretation of cyberspace as anarchic may be considered simplistic and not reflecting the reality of a complex governance structure that exists throughout even the supposed most anarchic and ungoverned 'dark web' elements of cyberspace. (Bartlett, 2014)

It is argued by Valeriano and Craig that the increasing militarisation of cyberspace evidenced by new military units such as Cyber Command in the United States, and a 'cyber-arms race' can be explained as a "*response to threat in an anarchic world*" shaped by Robert Jervis's realist concept of the security dilemma (Jervis, 1978; cited in Valeriano and Craig, 2018) although they conclude that realist theories "*… often fall substantially short in explaining the unique dynamics of cyber conflict*" (Valeriano and Craig, 2018)

A realist interpretation of cyberspace also fails to take account of the fact that states are not necessarily the primary force in cyberspace. However, it can be argued that this is changing, and that as states have become more aware of the potential of cyberspace as a factor that can influence their realspace ambitions, they have become more important actors within cyberspace. It can also be argued that as state influence has increased it has led to a more

anarchic cyber environment with increased proliferation of attack tools, and greater disruptive activity such as espionage. This thesis includes the argument that states are asserting their authority in cyberspace, especially through security considerations, including hostile state-on-state interactions and as a result it is becoming a more realist environment. This, again, is analogous to Medieval Europe which in realspace terms was effectively ended by the Peace of Westphalia and the introduction of the modern states system. This Medieval analogy has been a factor in calls for a Cyber Westphalia (Demchak and Dombrowski, 2014) and the development of distributed networked security models with cyber security provided on behalf of citizens by corporate entities acting like states (Brenner, 2014, pp. 141–168)

There are some realist analyses that do not distinguish between realspace and cyberspace state actions, but view cyberspace as another domain that reflects the realspace interactions of states. This is supported by studies of state-on-state conflict that show *"….that much cyber conflict takes place between historically rival states…"* (Valeriano and Maness, 2015) This would seem to show that states with historical rivalries allow that rivalry to bleed into cyberspace, rather than indicating the nature of cyber-interactions more generally.

Choucri, hoever, makes the important distinction between states using the cyber-domain to support realspace objectives, and using the realspace domain to support cyberspace objectives (Choucri, 2012a, pp. 11–12) and Susan Brenner has pointed out the importance of this distinction between the physical and virtual when she wrote that *"…because cyberspace is a non-spatial perceived environment, threat control systems that are predicated on spatial threat-dynamics are ill suited to the task of maintaining order 'in' cyberspace."* (Brenner, 2014, p. 243)

Realist physical assumptions are ill suited to an analysis of cyberspace and even when claiming that *"…realism appears to be the natural go-to theory for elucidating pressing cyber security issues"* Valeriano and Craig admit, citing Martin Libicki's work on cyber-deterrence (Libicki, 2009), that deterrence is not a viable approach within cyberspace, instead relying on a kinetic responses and cross domain general deterrence (Valeriano and Craig, 2018) so immediately showing how a key realist theory cannot be simply transferred to a cyber analysis.

Realism does not appear to be a straightforward explanation for cyberspace, and there are suggestions (which support the basis for new analysis such as that presented in this thesis) that there is a need for "…*the development of new theories based on empirical observation or the deductive logics of the cyber domain rather than automatically falling back on realist theories that were developed to explain kinetic forms of warfare.*" (Valeriano and Craig, 2018)

There is little literature that specifically addresses cyberspace and New Medievalism. The key characteristics of New Medievalism were defined by Hedley Bull in *The Anarchical Society*. Written in 1977, this was a time before the internet, although one could argue that designating the technological unification of the world as one of those characteristics seems highly prescient in hindsight given the global nature of the communications capabilities of today.

Madeline Carr's analysis in *The Anarchical Society at 40* (Carr, 2017) showed how attribution issues could affect international relations and, although acknowledging that technology is causing states to make compromises in relation to their sovereignty in cyberspace decides, with reference to her 2016 work on public and private partnerships in cyber security (Carr, 2016) that the state remains "*the key mechanism for governing cyberspace*" and does not make the leap required to place cyberspace in a New Medieval governance environment.

Susan Brenner has used a Medieval analogy to describe the need for a new approach to cyber security that does not depend on the power of the state alone, but used corporations as a mechanism to organise cyber security with corporations described as analogous to Medieval noblemen in that corporations own and control elements of cyberspace, with a 'private army' of employees (Brenner, 2014). These 'nobles' would be coordinated by the state to provide the resources and capabilities necessary for cyber security.

Alternatively, Anne-Marie Slaughter has talked about proponents of New Medievalism missing the two points that first private power is no substitute for state power, and second that a power shift is not a zero sum game, so "*a gain in power by non-state actors does not result in a loss of power for the state.*" Instead of a New Medieval new world order this may lead to a trans-governmental system of disaggregated state functions networked internationally. (Slaughter, 1997)

Philip Cerny has written about New Medievalism in the context of realspace globalisation and the "New Security Dilemma" created as a result of changes in inter-state relations and the growth of new non-state actors and in which "*attempts to provide international and domestic security through the state and the states system actually become increasingly dysfunctional.*" (Cerny, 1998, p. 40)

This situation where states can no longer provide security within a globalised transnational environment interacts "*….with economic and social processes of complex globalisation to create overlapping and competing cross-border networks of power, shifting loyalties, and identifies and new sources of endemic low level conflict – a 'durable disorder' analogous to some of the key characteristics of the Medieval world.*" (Cerny, 1998, p. 40)

Cerny identifies six characteristics that sustained the Medieval world order which he then applies to the New Medievalism of the 'global era'. These six characteristics are: multiple competing institutions; the lack of exogenous territorialising pressures; the uneven consolidation of new spaces, cleavages, conflicts and inequalities; fragmented identities; mixed, contested and overlapping property rights; and finally, the spread of 'zones grises'.

These characteristics provide a useful context for the analysis of cyberspace as a new Medieval environment that will be used in this thesis. Cerny's 'durable disorder' also offers a useful concept for the undercurrent of hostile and disruptive activity in cyberspace.

Charles Tilly offers an analysis that describes the possibility that the realspace state system was created and extended through conflict, leading to the assertion that "*States make war and vice versa*" in that the practical requirements of a state armed force "*generated durable state structure*" with the requirement for financial and logistical support structures which in turn gave the state the capacity to wage war. As the link between war-making and state structure strengthened, the nation state as a unit with a monopoly of physical force within a territory was confirmed (Tilly, 1992, pp. 69–70). An equivalent process of 'state building' as a by-product of state-on-state conflict may be underway in cyberspace

Stephen Kobrin identifies many of the issues that "*the digitalisation of commerce and the emergence of global electronic networks*" creates for the Westphalian order, especially in terms

of property rights, the blurring of public and private domains, and the creation of transnational elites. The changes enabled by this are such that it is a "*systemic transformation from a modern to a postmodern political economy*" i.e. from the modern post-Westphalian era of territorial sovereignty to a post-modern "*new, yet undefined, mode of political organisation not rooted in geography.*" (Kobrin, 1999). Although this looks at the effect of cyberspace on realspace structures, rather than looking at how cyberspace is constructed as a distinct environment, it provides an additional conceptual gateway to the analysis of cyberspace as a New Medieval environment.

New Medievalism also appears as a theme in the Private Military Contractor (PMC) and Private Military and Security Contractor (PMSC) literature. This is seen as particularly relevant as the use of mercenaries and the privatisation of force was a feature of Medieval warfare, which disappeared with the advent of the nation state and standing armies. The re-emergence of organisations that fight for profit is one indication of the emergence of New Medievalism (Singer, 2008; McFate, 2014)

The Medieval characteristics of cyberspace are also implied (although never explicitly stated) by literature suggesting that we are witnessing the development of the 'Westphalian Web' (Maher, 2013) or the a Cyber Westphalia (Demchak and Dombrowski, 2011, 2014). These works suggest that the move to a more state based system in cyberspace is underway through regulation, the implementation of cyber borders, as well as the development of cyber-warfare capabilities, with a transitional period that will involve significant cyber conflict, including those designed to test "*the limits of what can, and cannot, be accomplished using cyber operations without escalating into the kinetic exchanges typical of the industrial era war.*" (Demchak and Dombrowski, 2014, p. 34). A long, difficult, and violent transition to a state based structure would be supported by analysis such as Joseph Strayer's (Strayer, 1970) of the realspace emergence of the modern state from Medieval Europe.

Miryam Dunn and Victor Mauer suggest the same New Medieval power structures in cyberspace when she asserts that *"… states are collectively enforcing their authority in cyberspace. Consequently, we have not witnessed the end of the nation-state, but a return to*

overlapping authorities, including various forms of governance structures." (Dunn-Cavelty and Mauer, 2007, p. 159)

In addition to the literature on cyberspace and New Medievalism there is the regular use of medieval analogy in writings about cyberspace. The potential for self-regulation in cyberspace is described as analogous to the Lex Mercatoria of Medieval merchants (Perritt Jr., 1998) and Florian Egloff has used the analogy of sixteenth century privateering for twenty first century cyber security (Egloff, 2015) to illuminate the role of non-state actors, the increasing militarisation of cyberspace and the unintended consequences of state sponsored force exercised by non-state actors and what this means for cyber policy.

The relationship between large information technology corporations and their users has been described as a 'feudal' relationship in which users "…*pledge their allegiance to more powerful companies who, in turn, promise to protect them from both sysadmin duties and security threats*" (Schneier, 2013).

Moving on from the New Medieval metaphor in cyberspace, and the transition to a Westphalian system, there is also a well-developed literature on the assertion of state authority in cyberspace. This literature covers both the role of the state within cyberspace and mechanisms by which states can define their authority. This has, in particular, involved turning cyberspace (and cyber security) into a national security issue that has to be addressed by the state.

Much of this literature concerning state roles in cyberspace overlaps with that related to governance issues, especially when state-centric governance models are discussed (Mueller, 2013; DeNardis, 2014; Liaropoulos, 2017; Glen, 2018 and others). There is also a growing literature concerning techniques for state control of cyberspace and activities of its citizens in cyberspace, initially focusing on denial of civil liberties and filtering and access control (Deibert *et al.*, 2010b, 2010a) but more recently including analysis of the way in which regulatory developments enhance state capabilities for example through state enforced data protection law and concepts such as data sovereignty (Nugraha, Kautsarina and Sastrosubroto, 2015; Kohl and Rowland, 2017).

Underpinning many of these analyses is the construction of cyberspace as a national security issue that requires a state response, which is the basis for the analysis of the UK state's securitising moves incorporated in this thesis.

5 Cyberspace as a New Medieval Environment

This chapter describes how cyberspace reflects the key characteristics of New Medievalism as articulated by Hedley Bull (Bull, 1977) and Philip Cerny (Cerny, 1998) and identifies how these characteristics are found within cyberspace to an extent sufficient to be able to consider cyberspace as a New Medieval environment.

Cyberspace is often metaphorically described as the "*wild west*" (Denmark and Mulvenon, 2010; Limbago, 2017; National Crime Agency, 2017a), or more literally an "*ungoverned*" or "*lawless*" space (Schmidt and Cohen, 2013, p. 82; Baylon, Brunt and Livingstone, 2015; Egloff, 2015 and many others). It has also been described as a "*Hobbesian*" world (Ilves, 2014) or even simply "*Mogadishu*" (Hayden, 2016, p. 132) to reflect an understanding that cyberspace lacks institutions with state-like authority and allows criminality to flourish unchecked by law enforcement or other mechanisms of state control.

There is an alternative discourse which suggests that this view of cyberspace is incorrect as there are well developed governance mechanisms in place, structured to meet the needs of the different layers of cyberspace and providing different sources of authority (Lessig, 1999; Nye, 2010; Denardis and Musiani, 2014; Klimburg, 2017b, p. 241). What is clear from this discussion however, is that cyberspace is not governed in the same way that realspace is governed and that realspace governance structures – and in particular those incorporated within the Westphalian state – have not to date been easily transposed to cyberspace.

This chapter will argue that as an international system, cyberspace and realspace are based on significantly different governance models, with the Westphalian nation state as the dominant form of governance in realspace, and cyberspace potentially exhibiting the attributes of a New Medieval system of international order.

New Medievalism has been described as *"…important because it offers a conceptual lens for understanding the seemingly dissonant and chaotic world order emerging from the ashes of the Cold War that cannot be easily grasped past the blinders of state-centrism."* (McFate, 2014, p. 74) Given the chaotic non-state centric nature of cyberspace governance I would argue it may be an

even more appropriate lens through which to view world order in cyberspace where the 'blinders of state-centrism' have been just as prominent in preventing meaningful analysis.

The New Medieval metaphor has been used in relation to cyberspace's impact on realspace to explain the characteristic of the "*technological unification of the world*" (Bull, 1977, pp. 263–266) but it has not previously been used as a means to explain specific governance issues in cyberspace.

There is a long history of discussion about cyberspace's impact on the development of 'flattened hierarchies and 'network organisations' in realspace as part of a globalisation discourse. For example, Manuel Castells describes "*the Network Enterprise*" (Castells, 2001) and developed the theory of the Network Society (Stalder, 2006) and Nye and Welch cite Esther Dyson as arguing that "*as decentralised and virtual communities develop on the Internet, they will cut across territorial jurisdictions and develop their own patterns of governance*" with the result that states will become less important in that environment (Nye and Welch, 2014, p. 333). It is this development in cyberspace as opposed to in realspace that is of particular interest here.

Using New Medievalism as a conceptual lens for cyberspace enables some of the key differences between cyberspace and realspace to be described without depending on the historical and heavily contested views of cyberspace as either a utopian environment, or as the "*wild west*" as neither of these constructions are an accurate reflection of social order in cyberspace today.

Bull suggests that a New Medieval international order would *"…contain more ubiquitous and continuous violence and insecurity"*(Bull, 1977, p. 255 cited in Friedrichs,2001) than a system in which the hegemonic claims of nation states are recognised. A Medieval analogy is often used to describe environments in which extreme violence and chaos are defining elements, and Medieval is often invoked as a "*byword for backwardness or cruelty or some combination of both*" (Bain, 2017, p. 6). Writing in *The Atlantic* in 1994, Robert Kaplan provided a New Medieval image of the conflict in Sierra Leone which said that "*A pre-modern formlessness governs the battlefield, evoking the wars in Medieval Europe prior to the 1648 Peace of Westphalia, which ushered in the era of organized nation-states.*" (Kaplan, 2000, p. 8) and more recently there

has been a consistent pejorative discourse regarding the behaviours and beliefs of Islamist terrorists and the Taliban in Afghanistan as being Medieval in nature (Bain, 2017, p. 6).

However, it is argued that the idea that Medieval society was a more brutal equivalent to a Hobbesian state of nature is an inaccurate depiction (Friedrichs, 2001, p. 485). In addition to the 'centrifugal forces' of conflicting and overlapping authorities "*the societal system was held together by Christian universalism*" with both the Catholic clergy and feudal nobility forming "*trans territorial classes that preserved a considerable degree of uniformity within the system*" (Friedrichs, 2001, pp. 485–486).

This transnational Medieval class of clergy and nobility is mirrored in cyberspace by a transnational class of corporate managers, entrepreneurs and cyber specialists. These individuals work for global corporations such as Facebook, Google, Amazon, IBM, Apple, Twitter, and the like. It is from this resource pool that individuals are also assigned to cyberspace's global governance organisations such as the Internet Engineering Task Force (IETF). These groups often have objectives (in both realspace and cyberspace) that do not coincide with those of nation states, and as per the nation state system and the transnational market economy "*…implicitly raise antagonistic claims to how the organising principles of world politics should look like. Since neither of the two is in a position to prevail against its rival, they will be permanently forced to compete and cooperate*" (Friedrichs, 2001, p. 491).

This combination of competition and cooperation can be seen as a key element in cyberspace governance debates involving the state and private sector at the most fundamental level with the differences between a US favoured (The White House, 2018, p. 25) multi-stakeholder governance regime and an alternate state based governance regime delivered through the United Nations and the International Telecommunications Union (ITU).

This competition and co-operation is especially evident within the arena of cyber security where the state agencies are dependent on the engagement and support of the private sector to try and deliver a secure national cyberspace environment (should that indeed be possible in a globally interconnected system) while at the same time competing with the private sector over the integrity of private sector systems. The previously referenced examples of the conflict between Apple and the FBI concerning iPhone encryption (Zetter, 2016) and the

arrangement introduced on grounds of national security for the pre-inspection of Huawei equipment before its deployment in UK networks (ISC, 2013) in addition to issues relating to 'back-doors' being pre-installed in encryption software to enable lawful intercept (Klimburg, 2017b, p. 46) and the relationship with social media companies with regard to the removal of hate speech from social media platforms (HMG, 2017b), show a commercial or jurisdictional conflict between the state and the private sector that interferes with any potential for cooperation.

5.1 The Characteristics of New Medievalism in Cyberspace

The definitive attribute of New Medievalism from Hedley Bull is that it is a *"…system of overlapping or segmented authority…"* (Bull, 1977, p. 254) and whether "*…the inroads being made by these 'other associations' to use the mediaevalists' expression) on the sovereignty or supremacy of the state over its territory and citizens is such as to make that supremacy unreal and to deprive the concept of sovereignty of its utility and viability.*" (Bull, 1977, pp. 254–255).

Bull went on to identify five features of world politics which provided evidence of a trend towards New Medievalism. These are; the regional integration of states; the disintegration of states; the restoration of private international violence; transnational organisations; and the technological unification of the world (Bull, 1977, pp. 254–256).

In addition to the five characteristics defined by Bull, Philip Cerny has identified six key characteristics of a New Medieval world (Cerny, 1998). Along with Bull, Cerny refers to multiple competing institutions but in addition he includes; the lack of exogenous territorialising pressures; the uneven consolidation of new spaces, cleavages, conflicts and inequalities; fragmented identities; contested property rights; and the spread of 'zones grises'. Cerny also identifies the New Medieval world as not being one of chaos, but of 'durable disorder', a description that seems highly appropriate for cyberspace with the constant low-level cyber conflicts that take place every second of the day.

Most analysis of cyberspace in relation to the potential for a New Medieval world order has focused on how cyberspace (and in particular the Internet) has acted as an enabler for these developments in realspace rather than cyberspace itself. However, this thesis argues that

New Medievalism may provide a model that is more valuable as a means to understand how international order is constructed in cyberspace as a distinct environment from realspace as shown through an analysis of the individual New Medieval characteristics.

The first characteristic of New Medievalism in cyberspace is the existence of multiple authorities. Any analysis of authority in cyberspace shows significant levels of authority resting with different entities. These authorities are not the same for different elements (or layers) of cyberspace. For example, authority in relation to the deployment of physical infrastructure for cyberspace is different to the authority governing electronic mail applications, or virtual network connections, and the governance of the telecommunications networks through the ITU is very different to the governance of the Internet. This serves to confuse the discussion somewhat, as there are multiple different instances of overlapping authority depending on which of the constituent elements of cyberspace is being considered.

Lawrence Lessig argues that cyberspace is governed by the code that determines the operation of the electronic systems that constitute the environment and this code is what both makes cyber space what it is and regulates it, and so "*…we can build, or architect or code cyberspace to protect values that we believe are fundamental.*" (Lessig, 2006, loc 283).

In this context of the ability of code to regulate what happens in cyberspace Lessig states "*This regulator is code--the software and hardware that make cyberspace as it is.*"(Lessig, 2000) He goes on to refer to the code that implements TCP/IP and say that "*These architectural features of the Internet mean that governments are relatively disabled in their ability to regulate behavior on the Net.*" (Lessig, 2000)

However, if it is the code of cyberspace that provides its governance, the source of that code is clearly important. In the context of the Internet, the specifications of what that code has to deliver are the product of the Internet Engineering Task Force (IETF) Request for Comment (RFC) process, which in itself is governed by a credo of "rough consensus and running code" as outlined at the 1992 IETF plenary session (Clark, 1992).

If this view is correct and it is the 'code' that regulates cyberspace then this suggests a significant segmentation of authority in this environment with authority divided between

different protocols and standards as well as between different equipment manufacturers, software developers and service providers. Cisco, Microsoft, Google and Facebook for example, all have authority within cyberspace through the code that they provide to deliver the environment. The relationship of this code-based authority with the state is interesting, as it can be used to enable state authority in cyberspace or to diminish it.

There are examples where the code of cyberspace allows the authority of the state to be ignored, such as the use of the Internet to by-pass state regulations on gambling by providing access to gambling services outside the state's territorial boundary (Manter, 2003). There are instances where code ignores state regulations, for example delivering content regardless of copyright (Bohannon, 2016), or undermines state authority, for example by providing encrypted communications capabilities that cannot be accessed by state agencies (Castro and Mcquinn, 2016). There are also instances where the code in cyberspace can be used to enable state authority, for example by controlling access to content (Zuckerman, 2010).

These examples show that the authority of code in cyberspace significantly overlaps the realspace authorities of the nation state if they are applied to cyberspace. In some areas, such as encryption, where software development companies refuse to enable state security activities by providing 'back doors' it seems that the concept of sovereignty of the state is deprived of its utility.

However, code can equally be capable of enforcing state sovereignty and leading to a "*consolidation of institutional control*" (Schneier, 2015, pp. 92–103), for example through geo-location capabilities such as the Global Unique Identifier (GUID) that uniquely identifies every device, or the metadata that is created by any communication and collected by both state agencies and private corporations to support data mining and other data exploitation activities which gives rise to serious concerns that this will enable a public-private partnership in surveillance (Keen, 2015, pp. 179–183).

The second characteristic of cyberspace that reflects New Medievalism is the privatisation of violence within the cyber environment. The restoration of private international violence

(although Bull also uses 'force') is identified by Bull as a feature of world politics that is indicative of a trend towards New Medievalism.

There are three main ways in which the privatisation of force is exhibited in cyberspace. First, there is the use of force by private individuals and corporations for accepted defensive purposes; second, the use of private force in conjunction with, or on behalf of, the state for offensive purposes; and third, the illegitimate or unsanctioned use of private force by non-state actors.

Cyberspace provides two major areas of complexity in understanding private force. Firstly, there is a grey area between offence and defence so that at times it is difficult to judge when force is being used for defensive or offensive purposes. Secondly it can be difficult to identify who is exercising force because of the potential for obfuscation and deception enabled by anonymity and the attribution problems inherent to cyberspace. This has led to the growth of cyber proxies operating on behalf of the state (Maurer, 2018) and regular confusion concerning attack motivation and attribution, with what appear to be criminal attacks from groups such as The Guardians of Peace and The Lazarus Group in fact originating with a nation state (Bartholomew and Guerrero-Saade, 2016).

Defensive force is used by corporations and individuals to protect networks and systems from cyber-attacks such as malware, unauthorised access, and Distributed Denial of Service attacks. These capabilities are incorporated in a wide range of security systems including anti-virus software, firewalls, anomaly detection systems, intrusion detection systems (IDS), intrusion prevention systems (IPS), access control systems and security incident and event management (SIEM) systems. This aspect of private force in cyberspace has become an accepted way of minimising the risk of basic cyber-attacks and is the most common example of force used in cyberspace. Although it is, in general, a non-aggressive approach to cyber security, I would argue that force used in the pursuit of cyber-defence can still be considered force in so much as it unilaterally imposes effects on others' behaviour.

In the current security environment in cyberspace most private corporations and private citizens have been required to take responsibility for deploying their own defensive capabilities, supported by a global cyber security industry estimated to have been worth

between 90 and 120 billion dollars in 2017 (Morgan, 2017; Muresan, 2017). Within this environment, the UK state agencies have to date offered mainly advice and guidance to the majority of private organisations, while providing more in-depth security services for government networks and systems.

However, the distinction between defensive and offensive cyber activity is becoming increasingly blurred. Approaches to cyber-defence at a state level that may involve the pre-installation of malware on an adversary network, and concepts such as 'Active Defence' at a non-state level that can involve deception (honeypots), interference with the attacker for the purposes of analysis (tar pits), and potentially even the use of retaliatory force ('hacking back') eventually form a continuation of capabilities may make attack and defence almost indistinguishable and certainly creates a 'Grey Zone' of approaches to cyber security (CCHS, 2016).

There are commentators who suggest that companies are considering a more proactive approach to cyber defence (Ashford, 2016a), and so turning to traditional military suppliers for support. There have also been suggestions that government (in the US at least) may turn a blind eye to any criminality involved and would be "*more likely to consider assisting frustrated companies than threaten prosecution when they talk about going on the offensive*" (Timberg, Nakashima and Douglas-Gabriel, 2014). This suggests that there is the potential for a move from passive cyber-defence to a more pro-active approach to the use of private violence in cyberspace. This has led to the grey area of active defence.

The term 'Active Defence' has been used in several different ways. The UK NCSC refers to an approach of 'Active Cyber Defence' (Levy, 2016b) and the U.S. Congress bill that would legalise 'hacking back' by corporations is named the Active Cyber Defence Certainty Bill (Robinson, 2018). Both these uses can be seen as representing a stretching of the term beyond its normal use that could cause confusion on the part of policymakers. The NCSC's Active Cyber Defence refers to a very specific programme undertaken by the NCSC for UK public services (Levy, 2016b, 2018) while the Active Cyber Defence Certainty Bill described retaliatory actions to be undertaken by private enterprises.

George Washington University Centre for Cyber and Homeland Security provides a useful definition of active defence as:

> "*Active defense is a term that captures a spectrum of proactive cyber security measures that fall between traditional passive defense and offense. These activities fall into two general categories, the first covering technical interactions between a defender and an attacker. The second category of active defense includes those operations that enable defenders to collect intelligence on threat actors and indicators on the Internet, as well as other policy tools (e.g. sanctions, indictments, trade remedies) that can modify the behaviour of malicious actors. The term active defense is not synonymous with "hacking back" and the two should not be used interchangeably.*" (CCHS, 2016)

Even within this definition there is a range of activities (as shown in Figure 1) from information sharing, through techniques such as 'honeypots' and 'tar pits' that enable analysis of attacker behaviours and divert an attack away from critical systems, to 'beaconing' or 'dye bags' and threat intelligence gathering including collecting forensic or attribution data that could later be used to identify the attacker or could be shared with other organisations. This 'Grey Zone' shows the extent to which the use of private force has been legitimised in cyberspace, with aggressive actions such as bot-net takedowns and the use of 'white hat' ransomware seen as potentially legitimate actions.

These approaches can be taken further into areas of dubious legality, such as patching the attacking machine, installing malware on to the attackers' command and control server or even launching a DDOS attack against the attacking machines. All of these actions would be likely to fall foul of the Computer Misuse Act in the UK if undertaken by non-state actors, and have only recently been legalised for use by GCHQ by the 2016 Investigatory Powers Act (Vincent, 2016).

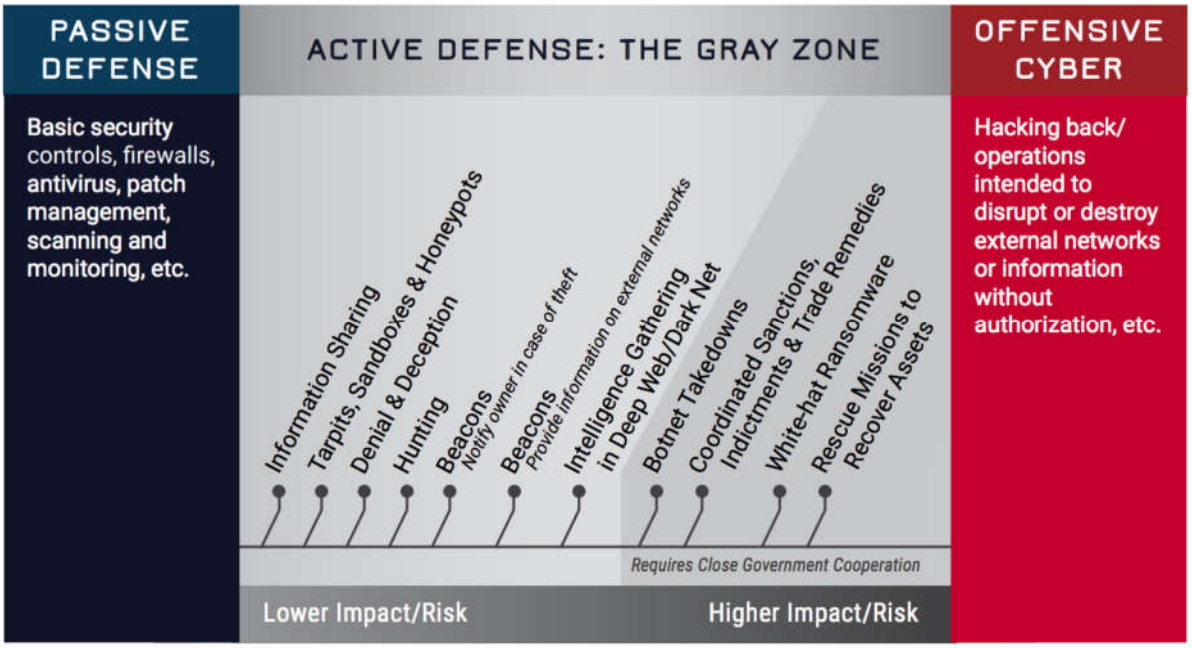

Figure 1 Active Defence: The Gray Zone (CCHS, 2016)

At the extreme end of active defence, the approaches merge into what could be considered offensive behaviour by non-state actors. These are often loosely included in the 'hacking back' colloquialism to describe any action where the victim of cyber-attack responds in kind by hacking the initial attacker in retaliation. This has been described as "*the worst idea in cyber security*", (Lemos, 2018) "*…a terrible idea that just will not die…*" (Schneier, 2017) and by the NSA's Admiral Mike Rogers as "*putting more gunfighters on the streets of the wild west*", (Limbago, 2017) which gives some indication of the prevalent negative view from within the cyber security industry with respect to hacking back.

However, despite this view being expressed within the cyber security community there have been a number of reported instances of 'hacking back' where companies have used offensive cyber capabilities against attackers. This includes, events such as the VDOS criminal DDOS service being hacked with details of customers released onto the Internet (Krebs, 2016), a young internet scammer being 'doxed' by his victim and his details given to his family; an attempted CEO whaling attack (a phishing attempt targeted at a senior executive) thwarted and the attacker exposed with a malware laden PDF file (Pauli, 2016); and Microsoft and a group of financial institutions disabling the Citadel botnet in 2013 (albeit with a court order)

(Harris, 2014 loc 2197). It is likely that not all incidents of hacking back are in the public domain, as hacking back and hack-back services remain illegal in most countries and even the creation or possession of malware can result in criminal charges.

As well as the known instances, there are also suggestions that there is the potential for more use of offensive cyber capabilities by the private sector. There are claims that banking organisations in particular are "*amassing cyber weapons in the event that they feel compelled to retaliate against attackers.*" (Harris, 2014 loc 3512). Singer asserts that there are "*….many private information warriors, who, for the right price, will develop and conduct information attacks on behalf of clients.*" (Singer, 2008, p. 62) and Sean McFate claims that "*Companies are already engaging in cyber-warfare, offering clients offensive 'hack-back' capabilities against intruders.*" (McFate, 2014, p. xiii).

The 2015 data breach and subsequent Wikileaks release of customer details from the Hacking Team showed customers for offensive capabilities included a large number of state organisations from developed and developing worlds, alongside private organisations such as Barclays Bank (Collins, 2015; Ragan, 2015). This list indicated that the market for offensive cyber exploits was extensive. This seems to be confirmed by the range of organisations involved in the provision of offensive cyber capabilities such as Vupen, who describe themselves as "*…a leading provider of defensive & offensive cyber security capabilities including government-grade zero-day exploits*" (Vupen Security, 2017) and FinFisher who describe their products as providing capability to "*…address modern challenges with the utmost efficiency with leading offensive IT intrusion solutions*" (FinFisher, 2017). Alongside these cyber specific providers, there are a number of more traditional defence companies who are now expanding into providing state-level cyber capabilities to meet growing market demand, including Raytheon, Northrop Grumman, and Booz, Allen Hamilton (O'Neill, 2017).

There are some clear arguments against hacking back by the private sector, including the legality of CNA/CNE by a private sector organisation, the danger of collateral damage such as was seen with the Microsoft action against Vitalwerks (Lemos, 2018), the issue of the uncertainty still associated with attack attribution, and the inevitable danger of a private corporation being engaged in a tit-for-tat cyber conflict with a nation state.

Cyber conflict between a private company and a nation state would undermine state authority with a private company engaging in what would normally be considered activities reserved for the state. There are several concerns with such a conflict taking place, including escalation to include kinetic attacks and the risks of a state-on-state conflict being initiated through actions by a private corporation. The engagement of civilian organisations in conflict with nation states also raises raise a plethora of issues with regard to the Law of International Armed Conflict (LOIAC) and the status of civilians as combatants and legitimate military targets (Brenner and Clarke, 2010; Schmitt, 2012b; Watts, 2012).

Unfortunately, the history of (alleged) state or state sponsored cyber-attacks against private organisations would suggest that there is little government response to state attacks that are potentially commercially catastrophic for the private sector victims. For example, In the US, only one indictment was delivered four years after the attack on Sony in the United States, and just one conviction of a Chinese national in relation to the theft of billions of pounds worth of intellectual property relating to the F35 fighter. Writing in a US context, it has been argued that

> "*….in the cyber security sphere, the government has disclaimed primary responsibility for defending the private sector against even foreign-government intrusions, placing that duty solidly on private entities, with assistance in the form of some information sharing. So far, this system is failing to provide adequate security. Although some companies may be sufficiently sophisticated to grapple with nation-state based threats, most—including many critical-infrastructure entities—are not*" (Eichensehr, 2017)

This suggests that private sector organisations may be in a situation where they are unable to defend against state level attacks, yet alone consider mounting a retaliatory strike, but, given the evidence of commercially catastrophic impacts of cyber-attacks (for example, the Canadian telecommunications equipment manufacturer Nortel went bankrupt with the loss of 94,000 jobs, allegedly as a result of Chinese state level espionage (Leydon, 2012)) and the weak state response, it may be unsurprising that hacking back is considered an option by some who have the financial and technical capability for such action to be viable.

Offensive cyber actions by private organisations carry significant risks as there are issues around the status of those who are hacking back as to whether they are a civilian, whether they have, by their actions, defined themselves as a combatant or even a mercenary; and to what extent a retaliatory attack would then make civilian infrastructure a legitimate target.

This creates a danger of conflict escalation outside the boundaries of state relationships, in particular when attribution is so complex and the possibility of 'false flags' and incorrect attribution is so high, with potentially damaging consequences. If a privately owned bank were to attack a state entity it is likely to be interpreted as a state, or state sponsored, attack.

Historically there have been a number of reasons why a state may choose to use private force in the physical world. Based on Sean Mcfate's analysis of these reasons (McFate, 2014, pp. 41–49), cyberspace has three main attributes that make it particularly susceptible to the privatisation of violence.

First, there is a well-documented cyber skills-shortage which makes it difficult for government agencies to recruit or retain staff in competition with the private sector due to the greater rewards available outside government (Committee on the National Security Strategy, 2018).

Second, the economics of employing specialist skills mean that for some specific cyber skill sets it is more cost effective to use contractor resources than it is to employ full time civil servants (Intelligence and Security Committee, 2017).

Third, the use of private actors as a proxy for the state allows for obfuscation of both actors and motives and can hinder or delay the attribution of cyber-attacks. This desire to camouflage the involvement of the state in cyber-attacks applies to both attack execution and the 'back room' activities such as the development of offensive cyber capabilities and the discovery and acquisition of vulnerabilities, both of which are often contracted to private organisations (Maurer, 2018, pp. 75–76). The potential for denial and deception in cyberspace has furthered the adoption of offensive cyber-strategies that include the use of private organisations as state proxies to exercise force in cyberspace and a number of high profile state attacks have been attributed to private actors operating on a state sponsored

basis. This would include a number of suspected state sponsored Advanced Persistent Threat (APT) actors from China, the Lazarus Group acting on behalf of North Korea and others (FireEye, 2018b) alongside Fancy Bears group furthering the political aims of Russia (Crowdstrike, 2016).

However, proxy cyber-attacks are only one way in which state force is enhanced by the use of private capability with two other main approaches evident.

First, private capabilities are used in support functions that enable state cyber actions. One of the major differences in the state's use of private force in cyberspace from realspace, is that the traditional 'point of the spear' PMCs do not seem to be addressing the cyber market in any significant way. Other contractors such as Booz Allen Hamilton, and defence manufacturers such as Raytheon are more clearly engaged, indicating that it is not the front-line areas where (western) states look to use cyber contractors. Although there is no information publicly available from the UK, an analysis of a US CYBERCOM Request For Proposal (RFP) (Lachow, 2016) shows this focus on using contractor resources in support roles such as researching vulnerabilities and the design and development of cyber weapons that can be exploited by legitimate law enforcement and military organisations, rather than in any frontline cyber operations. It is also suggested that this focus on these so called 'left of exploit' roles may be the result of limitations imposed by national and international law regarding the use of private contractors in situations where they "*...exercise discretion that implicates the laws of armed conflict*". (Lachow, 2016)

Second, there are areas where states work cooperatively with private organisations in exercising offensive capabilities in cyberspace, for example Microsoft and the FBI worked together with a number of banks to take down the Citadel botnet in 2012 (Harris, 2014 loc 2211), reports of the UK's NCA working with private corporations to form "*virtual threat teams*" (Cox, 2015) with both private sector and law enforcement staff, and the NCSC's Industry 100 scheme where private sector individuals work alongside NCSC staff (NCSC, 2017h).

State proxies and criminal activity is another aspect that suggest a grey area in cyber operations. There are suggestions that state proxies may lead something of a double life

where their skills are not only used for state purposes, but also for their own - often criminal – purposes (Klimburg, 2017b, pp. 236–238) This situation can be further complicated by individuals working simultaneously in different groups as 'hackers for hire' (Malewarebytes, 2017).

It is often difficult to identify whether an attack is being performed on behalf of a state, as exploits are often common between criminal and state activities. This can be through theft of an exploit, as was the case with the NSA's Eternal Blue exploit used to facilitate the development of the WannaCry ransomware (CERT-EU, 2017), or through the repurposing of state capabilities such as the reappearance of Stuxnet code in Duqu, Flame and Gauss malware (Bencsáth *et al.*, 2012).

Tactics and techniques may also be similar, for example, GCHQ's Operation SOCIALIST was a cyber-attack by a UK state agency, (R. Gallagher, 2014; Gallagher, 2018) that used spear phishing, a man-in-the-middle attack and a malware drop to infect machines belonging to Belgacom systems engineers. This is an attack methodology that would not be surprising if it were seen in criminal activity rather than responsible state behaviour.

The Wannacry ransomware attack is also a good example of the complexity of the situation. A state exploit (Eternal Blue) developed by a private cyber-contractor (Equation Group) was stolen by a criminal gang (Shadow Brokers) and then utilised by a proxy (Lazarus Group) of a state (North Korea) to extort Bitcoin (a criminal activity) from infected users through a ransomware attack (Wannacry). This attack had significant impact on state entities (e.g. the UK's NHS) that was then mitigated by a private cyber security contractor (Marcus Hutchins) (NCSC, 2017b) who was later arrested by a state agency (FBI) for alleged prior criminal activity (Kronos malware). This type of inter-mingling of state and private capabilities can serve to make them almost indistinguishable and adds complexity to any analysis.

The difficulties in distinguishing state and criminal activity are further complicated by the variety of proxy relationships that are believed to exist between state authorities and criminal gangs. These gangs could be state tolerated, state sponsored, or state directed, while simultaneously pursuing their own criminal objectives. The same blurring of lines regarding groups also applies to individuals, and there is a huge grey area between 'security

researcher' and 'hacker' and a lot of overlap in an industry that offers legitimate earning potential from bug bounties, penetration testing and independent contracting and illegal earning potential from exactly the same activities. There is a view that many working in the cyber security industry have, at some point, been involved in the less legitimate side of the business (Wiedeman, 2017).

The case of Marcus Hutchins (known as 'MalwareTech'), referenced above, is instructive. He was responsible for mitigating the Wannacry attack in the UK by identifying the kill switch in the malware and registering the domains that were needed to activate it. He then worked through the NCSC's CiSP to assist in resolution (NCSC, 2017b). Shortly afterwards, he was arrested by the FBI on suspicion of being involved in creating the Kronos banking malware attack (Solon, 2017). Despite the fact that Hutchins was working with the NCSC it was reported that they were aware of his impending arrest and may even have been involved in the planning in order to prevent the need for a long extradition procedure with the United states (Corfield, 2017).

Perhaps the final area of state related private force in cyberspace that is of importance is that of non-state actors engaging in the private use of force without direct state sponsorship, but with their actions being tolerated to some level. These are often referred to as 'patriotic hackers' and would include Russian groups such as Fancy Bears who were reportedly referred to in this way by Russian President Vladimir Putin (Townsend, 2017). So called patriotic hackers are also reported to include a hacker known as 'the Jester', (also known as th3J35t3r), a "lone wolf patriot hacker" or "cyber vigilante" who is believed to be a former US military serviceman who has hacked targets that could be considered anti-US, including Islamic State and countries that had offered asylum to Edward Snowden (O'Connor, 2011; Kimery, 2014).

The case of the Jester is interesting in particular in relation to the range of activities undertaken. This has included feuds with other hacking groups, including Lulzsec, and Anonymous, attacks on Wikileaks, and a range of attacks on US adversaries, including the Libyan media, the Russian Foreign Ministry, jihadist websites, and the Russian Foreign Ministry (O'Connor, 2011; Kimery, 2014). This variety of targets may be an indication of a

situation where there is a lack of state control over the actions of patriotic state tolerated hackers who mix private objectives with those of the state.

There are a number of ethical issues associated with private violence in the realspace PMC industry (McFate, 2014, pp. 53–60) that also need to be considered in a cyber-context.

Mcfate identifies four areas of concern in the real space arena. First, for-profit violence has the potential to change the nature of war to a commercial activity; second, the profit motive could be seen as encouraging war; third, the deniability offered by private violence may be making war fighting easier for governments and allowing oversight to be avoided; and finally, weak contract enforcement and an asymmetry of knowledge, effectively allows contractors to act without control.

Unfortunately, there is no available research that indicates whether these issues are directly transferable to a cyber-environment. Although it would seem a reasonable assumption to make, it is an area that requires further research.

In addition to the above realspace considerations which may also apply in a cyber-environment, cyber-warfare has its own unique ethical dimensions. Of particular concern is whether cyberspace lowers the barriers to war. This could be by enabling smaller states due to the asymmetric nature of cyber-warfare or it may be that states are more likely to engage in a cyber-attack than a kinetic attack due to a possible perception of cyber-attacks as being something that is 'not-quite war'. This is especially the case if cyber-war is considered to be some kind of ideal type of war in terms of minimising bloodshed and destruction (Jenkins, 2016).

It is possible to argue that it is useful to be able to pretend that state use of offensive cyber is an unauthorised criminal act and that the use of proxies has prevented state hacking from escalating to a serious state-on-state conflict by allowing it to be treated as espionage or a criminal act, in response to which, existing protocols can be used proportionately. This was the case with the expulsion of Russian diplomats following the hacking of the 2016 US election (Gambino, Siddiqui and Walker, 2016).

Where the victim of a state level cyber-attack is in the private sector, the approach has been somewhat different. In the US there has been an attempt to maintain the conceit that state-level hacking is a criminal act by individuals rather than statecraft, as shown by civil indictments being made against Chinese individuals in 2014 for attacks against a range of US companies (US Department of Justice, 2014) and again in 2017 (Keppler, Freifeld and Walcott, 2017).

This is despite the scale of Chinese hacking in industries of strategic national importance, for example, telecommunications equipment, where it is alleged that intellectual property theft from Nortel and Cisco by Huawei (Chandler, 2012) may have allowed Huawei to dominate segments of the telecommunications equipment market.

The third of Bull's characteristics of New Medievalism is the regional integration of states. There are direct parallels in cyberspace, in particular through the architectures used for network construction and traffic routing configuration. Early European transnational data networks were often built on a regional basis, for example the Atlas joint venture between France Telecom and Deutsche Telecom (New York Times, 1995) Cable & Wireless's European Network[29] or the Interoute European Network Architecture (of 2017) which shows an integrated European Network with a consolidated interconnection to other regions.

[29] I was personally involved in the deployment of this network, and although no documentation if now publicly available, it conformed to the regional structure evident in the referenced networks.

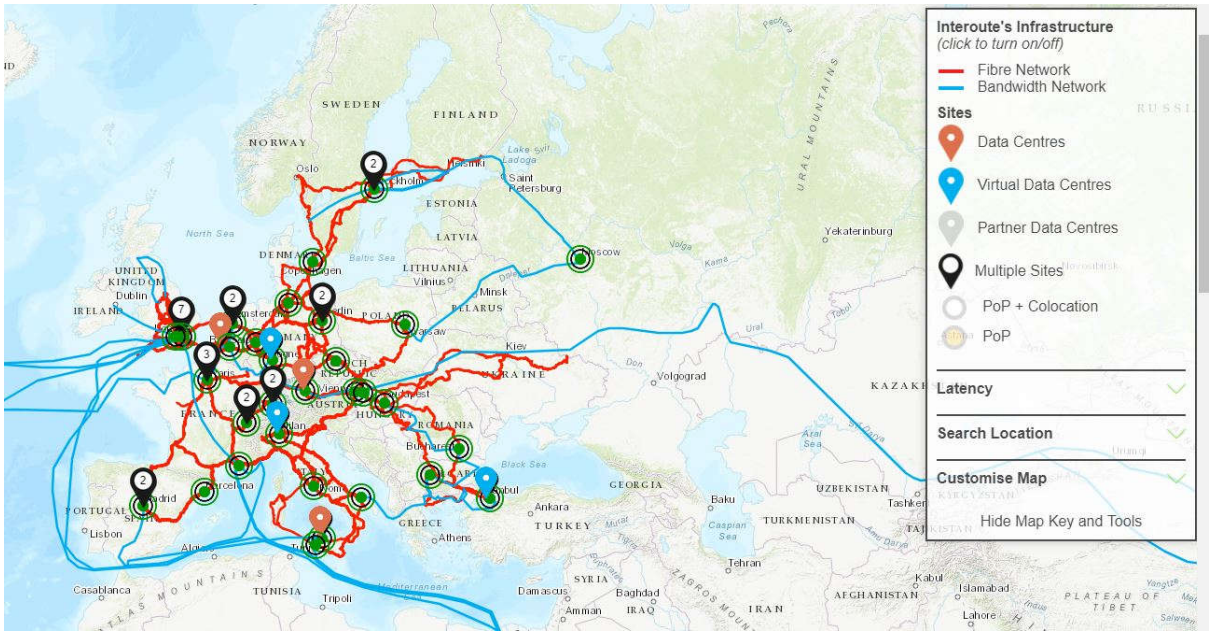

Figure 2 Interoute European Network Map[30]

The same regional integration can be seen in other areas, for example the ARCOS submarine cable network that connects the Caribbean and Central America shown in Figure 3 which effectively brings the connected states together in a regional ring network-based system.

[30] Interoute European Network Map image source (https://www.interoute.com/our-network downloaded on 15/11/2017

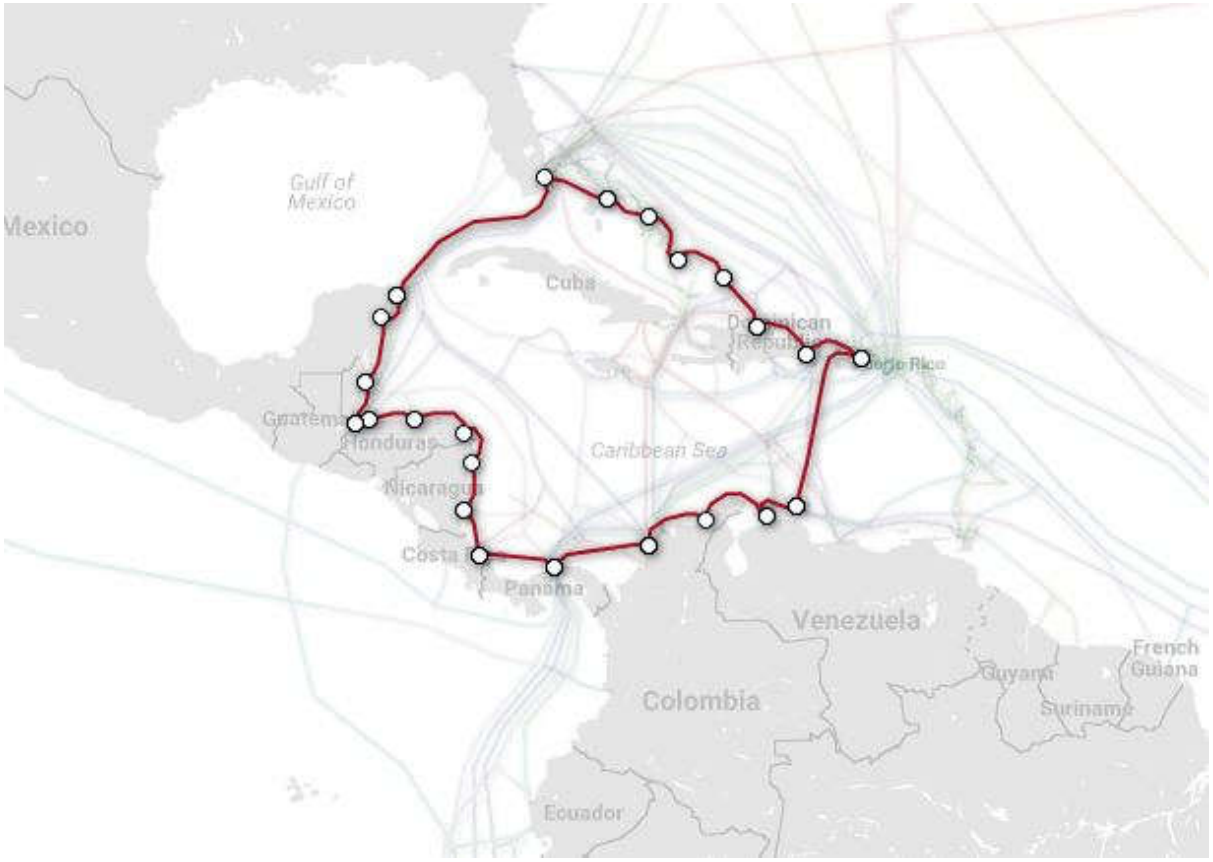

Figure 3 ARCOS Submarine Cable Network[31]

Regional Integration can also be seen in the construction of Level 3's Global Network (important as a Tier 1 Network for the Internet) with regional networking consolidated for inter-regional communications as shown in Figure 4 where the network architecture suggest regional unification in Europe, North America and Asia Pacific regions.

[31] ARCOS Submarine Cable Network image source: https://www.submarinecablemap.com/#/submarine-cable/arcos downloaded on 15/11/2017

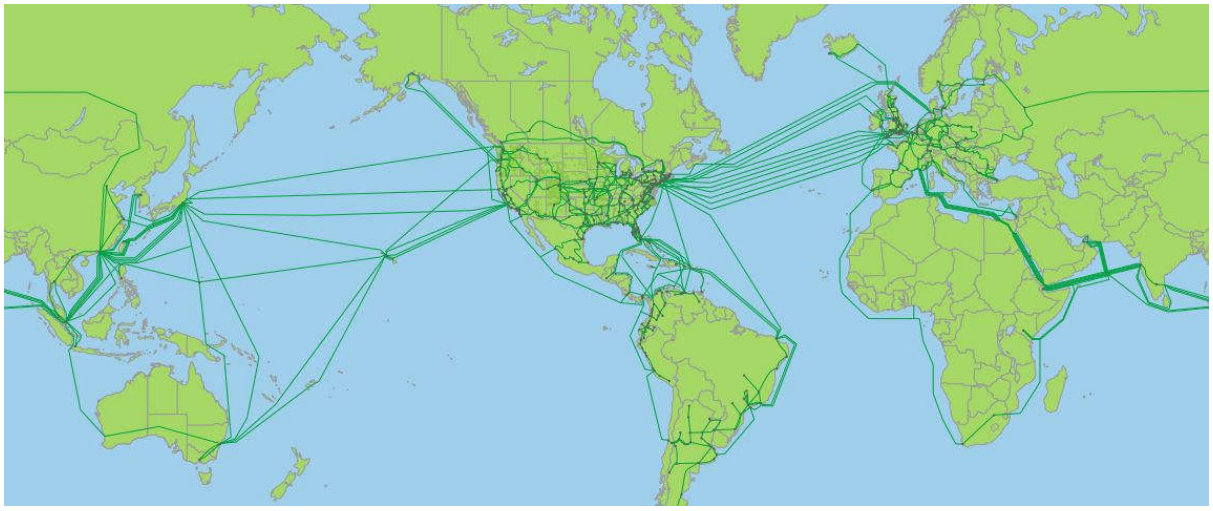

Figure 4 Level 3 Backbone Network[32]

This regional integration is also evident in Global Crossing's European network of the late 20th Century as shown below where European states are connected on a regional basis.

[32] Level 3 Backbone Network image source http://www.level3.com/-/media/files/maps/en-network-services-level-3-network-map.pdf downloaded on 15/11/2017

Figure 5 Global Crossing Pan European Network[33]

Effectively, the architecture of the telecommunications network infrastructure is a force that drives the regional unification of states in cyberspace by driving their traffic into consolidated routes for inter-regional communication at the physical layer.

Cyberspace also has regionally integrated states at the data layer in terms of 'data at rest' through the use of consolidated regional data centres by the major service providers.

Google, for example provides services in every European country, but has only four European data centres in Dublin, Ireland, Eemshaven, Netherlands, Hamina, Finland and St Ghislain, Belgium (Google Inc., 2017) Amazon Web Services (AWS) operate their infrastructure on the basis of sixteen regions with Europe consolidated into three regional

[33] Global Crossing Pan European Network image source https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/globalcrossing2_large.gif downloaded on 15/2/2019)

centres based in London, Ireland, and Frankfurt (Amazon Web Services Inc., 2017), Twitter operates solely from data centres in the USA and Ireland (Keough, 2015); Facebook has data centres in the USA in Prineville, Forest City, Altoona, Fort Worth, Los Lunas, Papillion, and Henrico (Facebook, 2017b) while outside the USA there are data centres in Luleå, (Sweden) and Clonee (Ireland) (Donohoe, 2018), with plans for a third in Odense (Denmark) which is due to be operational in 2020 (Facebook, 2017a). As huge generators and consolidators of network traffic, these data centre architectures are again creating a regionally consolidated cyberspace that further suggests that cyberspace displays the characteristics of a New Medieval environment.

This regional integration of data centres is driven by many factors, including costs of operation, economic and regulatory environment, internet bandwidth availability and security (Cushman & Wakefield, 2016). However, although the overall effect of data centre economics is such that it drives regional integration, there are factors that may lead to a more local deployment, for example when data applications have low latency requirements it may be more effective for data to be held closer (in terms of transport time) to where it is used, and restrictive data protection requirements may force data centre locations to be selected regardless of economics. For example, Microsoft's choice of Germany for an Azure data centre was based on strict German data protection laws and the use of a German data trustee. This meant that Microsoft staff had no access to the data on the service, and the data could not be subjected to US law or the demands of the US government (Microsoft, 2016). This is one example of how states are challenging the New Medieval overlapping governance authorities of cyberspace through the use of territorial laws.

However, the difficulties of this became apparent in 2018 when Microsoft ceased offering the German service to new customers (Chirgwin, 2018) and although Microsoft claimed this was in response to changing customer demands, other reports suggested that it had proved impossible for a global data centre architecture to operate on such a territorially defined basis and data was still being sent to the USA in order to facilitate operational aspects of the service (Grunwald, 2018).

Another example of regionalisation is numbering control on the Internet. This is explicitly regionalised with five Regional Internet Registries (RIR) of AFRINIC serving Africa and based in Mauritius, APNIC serving the Asia Pacific Region and based in Australia, ARIN serving the USA and Canada plus some others and based in the United States, LACNIC serving Latin America and some Caribbean Islands based in Uruguay and the RIPE NCC serving Europe, Central Asia and the Middle East and based in the Netherlands (Number Resource Organization, 2014). These RIRs control the allocation of IP address numbers within a region, effectively controlling a key Internet resource in a unified way on a regional basis.

A final example of how cyberspace is encouraging regionalisation is in the management of cyber-attacks through Computer Emergency Response Teams (CERTs) which have formed on a national basis, but then also regionalised in order to pool resources and share information. Examples include AP-CERT for Asia Pacific and EU-CERT for Europe. Again, it can be argued that cyberspace is encouraging regional unification.

Continuing with the characteristics of New Medievalism and how they can be seen to be present in cyberspace, Bull states that the disintegration of the state is also indicative of New Medievalism. There are several indications of where state disintegration is a feature of cyberspace, especially where state laws and regulations are being undermined by alternative governance mechanisms in cyberspace.

A distinction needs to be made in that this disintegration of states does not refer to a state breaking up into smaller states. As Bull says, if the result of the disintegration of a state is just to create additional sovereign states then this does not particularly impact the institution of the sovereign state (Bull, 1977, p. 257). This suggests that initiatives such as the proposed creation of a virtual Catalonian state (Wired, 1997; Armstrong, 2017), or the development of Sealand as an independent sovereign state (Betz and Stevens, 2011 loc 1143), while interesting in their own right are not an indication of the disintegration of a sovereign state. Bull suggests that the disintegration of states would be typified by the emergence of new governance units that would need to advance far enough to cast doubt on the sovereignty of

existing states, whilst stopping short of claiming the same sovereignty for themselves (Bull, 1977, p. 257).

As we saw in the discussion on cyber sovereignty in *4.2 Cyberspace and Sovereignty,* this characteristic is present in the governance roles being filled by private sector organisations in cyberspace, and if we accept Lessig's assertion that 'code is law' then it can be argued that this includes law making itself through the code and technical infrastructure that forms the basis of cyberspace.

Increasingly it is the case that online service providers in cyberspace are expected to act as an intermediary in enforcing state statutes (Wittes and Blum, 2016, p. 210). For example, enforcing copyright or data protection law (Kohl and Rowland, 2017); taking down phishing or illegal content sites; controlling speech through content filtering; countering terrorism by doing "*…more to proactively detect and remove terrorist content from their platforms*" (HMG, 2017b) (effectively acting as government censors) and providing a level of safeguarding for online users, despite having no legal responsibility or authority to do so.

On a pragmatic basis, any responsible organisation can be expected to do what it can to prevent the spread of material inciting violence and hatred or enabling modern slavery, but at this point, with a legal framework that pre-dates the internet (HMG, 2017b, p. 8), the state is effectively asking the online service providers to provide governance over online activity in the absence of an effective state capability. This suggests limits to the sovereignty of the state in cyberspace, although it is developing rapidly, and it could be argued that the use of intermediaries has enabled the state to impose its authority on a New Medieval cyberspace environment by using intermediaries as an integral part of a regulatory mix (Wu and Goldsmith, 2006, pp. 66–84; Wittes and Blum, 2016, p. 212).

Other pressures on the cohesion of the state include the growth of digital currencies that have been described as *"…a significant blow to governments' attempts to financially control their subjects…*" and a "*…formidable challenge…..to national monetary sovereignty*" (Ammous, 2017), giving almost anyone the capability to anonymously move any amount of money. This is inevitably of use to criminal enterprises in relation to blackmail and extortion activities including ransomware and also for the anonymous acquisition of illegal goods and services,

potentially enabling a number of realspace criminal activities including drug dealing and sex-worker trafficking. It has also been suggested that the development of virtual currencies by non-state actors could be used as a deliberate strategy to undermine state sovereignty, especially where the state currency is weak (Baron *et al.*, 2015), providing another example of how cyber developments can encourage the disintegration of the state.

Bull also saw the technological unification of the world as an indicator of New Medievalism, in that technological advances were leading to the metaphorical shrinking of the globe by improving "*...the means of moving goods, persons and ideas around the earth's surface...*" (Bull, 1977, p. 265). The development of cyberspace (and in particular the Internet) can be seen as one element of this technological unification in realspace, along with improved capabilities for personal travel and goods shipping as well as the growth of transnational actors and changes in power structures (Nye and Welch, 2014, pp. 316–318).

It can also be argued that cyberspace (as distinct from realspace) is displaying characteristics of technological unification, at several levels. This provides more support for the argument that cyberspace can be viewed as a New Medieval environment.

Firstly, telecommunications network architectures have increasingly been designed to use TCP/IP protocols (displacing other network protocols such as SDH and ATM). Data and voice networks have migrated to use the same IP transport network as opposed to using physically distinct networks for different classes of traffic, and a significant proportion of the world's voice traffic is now carried on IP networks (Internet Society, 2012b). The Internet Protocol has served to unify the underlying network capabilities of cyberspace.

A process of technological unification has also created dominant organisations within cyberspace, in particular Google with 78% of all searches (Internet Live Stats, 2017), YouTube with more than 1.5 billion active users (also owned by Google), and Facebook with more than 2 billion active users (Statista, 2017). This unification can also be seen in operating systems with an 83% share for Microsoft Windows in desktop operating systems (Stat Counter Global Stats, 2017a) while Android boasts a 73% share in mobile operating systems (Stat Counter Global Stats, 2017b).

In part, this unification is driven by one of the fundamental laws of networking. Metcalfe's Law states that the value of a network is proportional to the square of the network number of nodes connected to the network. This means that in any situation where networks are competitive there will be a tipping point at which one network will become much more valuable than another. It will therefore attract more users which in turn will make it more valuable, to the point where it will achieve critical-mass and become dominant. This is supported by the idea that networks "*tend to exhibit-winner takes all forms of competition as actors converge on the same network to realise the benefit of a larger network.*" (Mueller, 2013, p. 48). This type of increasing return has been shown to cause an eventual lock in where users are unable to change from an installed technology and are stuck with "*…an outcome not necessarily superior to alternatives, not easily altered, and not entirely predictable in advance.*" (Arthur, 1989).

This potentially adds an interesting dynamic to the overlapping authorities in cyberspace in that the dominant technologies will display hegemonic tendencies and will displace competing technologies over time. There are good technical performance and cost reasons for protocol consolidation, but it does strengthen the position of the Internet Protocol within a code model of cyberspace governance and its relative importance within any model of overlapping and competing governance claims.

Cerny also cites contested and overlapping property rights, caused mainly by a failure to enforce property rights, as a characteristic of New Medievalism. This is another area where cyberspace shows the same characteristics typified in the early days of the Internet by the statement that "*The Net interprets censorship as damage and routes around it*" (EFF Founder John Gilmore quoted in Elmer-Dewitt, 1993) and anything that attempted to prevent information sharing – even on the basis of property rights – was interpreted as censorship.

Early Internet culture had little concept of property rights as such. Internet protocols and standards (RFCs) were freely shared, and a strong culture of 'freeware' and 'shareware' existed within technical communities that continues to this day with the Open Source movement. The same ethos led to the development of information sharing platforms such as Napster that allowed the free exchange of music, and although this was shut down in 2000

due to infringement of copyright (showing that realspace laws can extend to cyberspace (BBC News, 2000)) similar services exist such as those in the academic community like SciHub (Bohannon, 2016) and Research Gate (Hunter, 2017) that by-pass paywalls and intellectual property payments.

Issues around property rights extend to the use of online services. The example of Google Drive is instructive, where usage of the service grants Google seemingly unlimited rights to use any content a user has created through "*a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our services), communicate, publish, publicly perform, publicly display and distribute such content.*" (Whittaker, 2012).

Similar issues of property rights are also evident in issues relating to personal data on the internet with individuals choosing to give away important personal information to corporations such as Google, Facebook and other social media platforms and web browsers – which is then shared with governments and others through data brokers, as well as being used by the services themselves to target advertising and customise content based on user actions and preferences. Personal data in cyberspace is the subject of significant debate, with issues of an individual's control of their own data being central to the principles behind the EUs GDPR and the 'right to be forgotten'.

Cerny also cites as an indication of New Medievalism, opportunities to operate outside the law in so called 'Grey Areas' or 'Zones Grises'. Cyberspace has its own 'zones grises' (uncontrolled areas), most commonly associated with the Deep Web - those areas of cyberspace not catalogued by commercial search engines and made available to the casual web user. The more secretive and frequently illegal components of this Deep Web are referred to as 'The Dark Web' (or Dark Net) and are normally inaccessible from commercial web browsers, depending instead on TOR browsers that enable anonymity in interactions.

The Dark Web has become an enabling environment for criminal activity and has been regularly documented as a source of drugs, illegal pornographic and paedophiliac images, details required for identity theft, credentials for system access, malware and botnet rental,

and so on, through online markets such as Silk Road, Dream Market and others (Bartlett, 2014; Kuhn, 2015; Maxey, 2018).

However, while providing a mechanism for criminal activity it would be incorrect to suggest that there is no governance within the Dark Web. There is a complex self-governing system of vendor and buyer reviews, terms of service, user support networks, administrator enforcement and financial escrow systems providing the basis for trust within the online marketplaces (Bartlett, 2014). However, it remains an area with little or no control at this time although this is rapidly changing as law enforcement and intelligence agencies develop an improved capability to address these issues both through the arrest of individual users and by targeting the marketplaces. This has produced some notable successes in the UK in policing areas of illicit trade in drugs, firearms, and Child Sexual Exploitation (National Crime Agency, 2017b, 2018b, 2018a).

Cerny also states that a New Medieval environment is one of "*social and political schizophrenia*" in which elements of identification will not be easily subsumed in collective identities and identifies the fragmentation of 'cultural identities', 'cultures and societies', 'national identities' and 'nation state based identities' as a key element of New Medievalism (Cerny, 1998, p. 55).

Cyberspace is built on premises of anonymity and fluid identities that create an environment of multiple identities and loyalties. This ambiguity of identity is particularly pronounced in virtual worlds such as Second Life (Stoup, 2008) where it can lead to the failure of realspace social norms and controls, but even at a less extreme level, individuals have multiple identities, for example, their LinkedIn profile will almost certainly be different to their Facebook profile which will almost certainly be different to how they describe themselves on an online dating web site. As the New Yorker cartoon famously explained, "*On the Internet Nobody knows you're a dog.*" (Steiner, 1993).

These examples show that the fragmentation in cyberspace is particularly prevalent at the social level where human interaction in cyberspace takes place. This is also shown in the trend for news and information to be tailored to an individual, thereby leading to 'filter bubbles' where an individual's content reflects their own pre-existing views of the world,

decided algorithmically based on previous clicks and likes, that is never challenged by alternative information (Pariser, 2011, p. 9). This discourages any bridging between groups, magnifying any tendencies of cultural and social fragmentation and hardening identity divisions.

There was an expectation that the Internet would produce 'bridging capital' where non-traditional connections made impossible by physical distance would serve to bring disparate people together in a Marshall McLuhan's 'Global Village' (Nye and Welch, 2014, p. 334). However, it seems that that online activity is serving more to bond existing narrow communities together, confirming existing interests and prejudices, which are then further reinforced by the selective presentation of news and information by online service providers (Pariser, 2011, p. 17). This is not a process that is unique to the internet and online services but is the same 'narrowcasting' exhibited by other elements of cyberspace such as cable news channels, for example, that promote a particular view of the world (Nye and Welch, 2014, p. 334). This fragmentation and polarisation is generally perceived as negative (Rosenau, 2003), but there is debate as to whether it is a price worth paying for the individual empowerment and the disruption of the domination of public discourse by a few media outlets that has been provided by cyberspace (Stille, 2001).

Cyberspace also provides a medium for groups that encourage realspace fragmentation, enabling members to communicate with one another through message boards, IRC groups, Facebook groups, or encrypted communications platforms such as Whatsapp and Telegram. This use of the internet for hate speech and the promotion of divisive ideas that effect social cohesion is a major concern in liberal democracies with groups such as ISIS and Britain First using the communication capabilities of cyberspace to great effect.

There are also examples of more subtle divisive and fragmentary forces in cyberspace that reinforce real-space fragmentising behaviour. This has been clearly shown in the racial bias at work in AirBnB systems that leads to guests with 'white' names being offered accommodation vacancies that were not offered to potential guests with 'black' names (Edelman and Luca, 2014; Edelman, Luca and Svirsky, 2015; Botsman, 2017, pp. 94–96). In this instance cyberspace is providing the vehicle for realspace forces of fragmentation to be

exercised hidden in the large volume of small scale AirBnB providers and so creating a systemic problem that is out of the reach of realspace equality regulation.

Cerny also identifies the uneven consolidation of new spaces, cleavages and inequalities as a characteristic of New Medievalism. He describes New Medieval 'fault lines' that do not reflect traditional territorial boundaries and demarcations. Instead, a "*range of virtual spaces in the global political economy will increasingly overlap with and possibly even replace the 'real' space of traditional geographic and topological territories*" (Cerny, 1998, p. 54). These spaces will become increasingly localised and come to represent the spaces with which people identify. Not all these spaces will be equal, and complex new inequalities and divisions will develop.

In cyberspace itself there are huge fault lines that show the same characteristics. For example, new virtual spaces are not consolidated effectively due to lack of technical skills, lack of network bandwidth or processing capacity. Specialised access devices for virtual environments such as games consoles and Virtual Reality (VR) headsets restricts access to those who can afford and use the equipment. Additional knowledge required to utilise VPNs, TOR, or other anonymising systems put a price on privacy.

Inequalities exist based on physical location, service providers, computing power, bandwidth allocation, traffic shaping techniques and network infrastructure. Even in the UK, rural Internet access remains a significant issue in many places, while countries such as Somalia and Eritrea have an Internet penetration of less than 2% of the population (International Telecommunications Union, 2017).

Cleavages exist in cyberspace, created by, for example, differences in operating systems, network protocols, closed and open systems and software, membership-based systems and restrictive terms of service which all serve to create division within user experience of cyberspace. The technology and services available determine the type of space that is experienced which can be completely different across different communities in cyberspace again reflecting the New Medieval nature of cyberspace.

Cerny also describes the Medieval world as being one of 'durable disorder' in which low level conflicts and crises did not immediately bring about an overall system crisis (Cerny, 1998, p. 58).

I would argue that cyberspace is an environment typified by 'durable disorder', with the characteristic of constant low level violence that never reaches a level that could be considered equivalent to kinetic warfare, but is typified by a "*death-by-a-thousand-cuts set of lower level attacks*" (Hannigan, 2015) that undermine confidence in digital society. The number of attacks is significant, and increasing, (PhishLabs, 2016; Symantec Corporation, 2017, 2018) without historically resulting in the catastrophic failure of cyberspace or escalating to a kinetic conflict, and so creating a New Medieval environment of durable disorder.

There are several reasons why this durable disorder should be expected in cyberspace. Firstly, classical offence/defence (security dilemma) theory would suggest that any environment in which offensive capabilities are at an advantage is more likely to promote conflict (Jervis, 1978). Cyberspace is an environment in which attack is seen as easier than defence. This is exacerbated by factors such as the time-limited utility of cyber-weapons (in that they can be made obsolete by an exploited vulnerability being discovered and a patch being applied); new vulnerabilities regularly being made available; uncertainty of attack motivation, attribution and response; and the difficulties involved in differentiating between attack and defence, particularly in Active Cyber Defence scenarios where malware may be installed on an adversary network for what are ostensibly defensive purposes but which could equally be considered an aggressive act (Buchanan, 2016, p. 189).

Secondly, cyberspace is an environment in which deception plays a major role (Bodmer *et al.*, 2012). Cyber-attacks are almost invariably based on various forms of deception. For example, phishing emails aim to deceive recipients that they are benign; malware aims to deceive systems, so they treat them as valid processes; and defensive measures such as honeypots aim to deceive attackers into believing they are attacking a genuine system. These deceptive operations are seen as "*…less aggressive than outright warfare but far from pacific*" and it is reasonable that "*Cyber warfare, and perhaps all forms of deception-dependent*

interactions is best understood as low-intensity conflict behaviour…" (Gartzke and Lindsay, 2015) suggesting once again that cyberspace is characteristically an environment of durable disorder. Variations on this idea continue to be present in the cyber literature, most recently with the concept of a "*state of unpeace*" (Kello, 2018).

An additional characteristic of the Medieval period is what Cerny headlines as "*the lack of exogenous territorialising pressures*". He describes the end of the Medieval period as being demonstrated by:

"*…the institutionalisation of competition and conflict between increasingly powerful dynastic families in the last Medieval period which led to the consolidation of state bureaucracies and their growing penetration into more and more exclusively territorialised social and economic bases.*" (Cerny, 1998, p. 52)

With only slight adaptation this could almost be a description of what is happening in cyber space at this time. Disorder in cyberspace is driving greater institutionalisation and territorialisation of cyberspace governance through the state. The situation is somewhat different in that a sovereign state based international order already exists in realspace, but this is now being increasingly reflected in cyberspace with the growth of state authority. This has resulted in cyberspace becoming a domain for conflict between realspace state actors which in itself has acted as a further territorialising pressure on cyberspace. It has forced states to take action to protect cyberspace in their own territory through technological solutions such as DNS filters, firewalls, content filtering, data localisation, and mass data collection combined with the application of territorially constructed legal principles to cyberspace such as the use of territorially designed data protection law (Kohl and Rowland, 2017, p. 95).

Having identified the presence of these New Medieval characteristics in cyberspace, this may enable an analysis that could provide an indication of the issues that could be encountered in its future development and security.

Firstly, in a New Medieval cyberspace the lack of a hegemonic authority will mean a continued absence of order. There will be ongoing low level conflict between those

organisations competing for power in cyberspace, including states, private corporations, criminal gangs, hacktivists, and other non-state organisations (potentially both sub-state and supra-state) driven by competing forces of globalisation and state disintegration. The best case scenario in this case is that these competing authorities lead to a situation of 'durable disorder'(Cerny, 1998; Hettne, 2002) in which these underlying conflicts do not lead to complete chaos, but a governance gap in which disorder, conflict and criminality is a constant (Winn, 2004).

If history repeats itself, and an unsustainable New Medieval governance environment in cyberspace is ended by some kind of 'Cyber Westphalia', this may result in moves towards the development of formal cyber-borders and sovereign territoriality within cyberspace (Demchak and Dombrowski, 2014) such as could be the outcome from the propositions put forward by those who envisage a multi-lateral cyber-governance system through the UN and the ITU.

There are, of course, other forms of international order that may be possible outcomes (such as Nye's regime complex), and there are arguments that we are entering a post-Westphalian realspace world order (Falk, 2002), but Bull's "*…tyranny of the concepts and normative principles...*"(Bull, 1977, p. 265) associated with the state system may well still hold sway and despite the pressures of globalisation on a statist realspace world order, it seems plausible that a state based system will be the most likely outcome for cyberspace.

It can be argued that the elements required for a Westphalian order in cyberspace are already in the process of being developed. This would include data localisation regulations, 'Great Firewall of China' type DNS filtering by state organisations, the development of state level institutions such as the NCSC in the UK, and greater regulation in areas such as the security of the Internet of Things (IoT), and regulation that enforces realspace law in cyberspace in relation to issues such as intellectual property, copyright, and bullying.

There is a clear implication that the resolution of issues associated with cyberspace governance will result in a state system. The utopian 'Internet freedom' position of the early 1990s is increasingly difficult to defend in the face of constant cyber-attacks, identity theft, cyber-bullying, modern slavery, fake news and terrorist propaganda. The increasing

dependency of the modern state on cyberspace and the potential for realspace effects of cyberspace actions will leave states with little alternative but to assert their authority in cyberspace.

As a result, states are increasingly looking to regulate online service providers in addition to the existing regulation of infrastructure providers, with the EU GDPR and the NIS directive representing examples of regulatory initiatives that deliver increasing control to the state over cloud services, online service providers and electronic marketplaces.

Much of this regulation is justified by reference to security issues, as a key part of any state authority in cyberspace will be derived from delivering security. It is the security implications of cyberspace that provide, at least in part, the justification for many of the actions that are enabling the state to reassert its authority and change the relationship between the state, the private sector, and cyberspace. The following chapter will show how the UK state is using the issue of security to establish state authority in cyberspace through an identifiable securitisation process.

6 The Securitisation of UK Cyberspace

A key component of the narrative of this thesis is that the New Medieval nature of cyberspace is requiring the state to take specific actions to assert its authority in cyberspace. One particular mechanism by which this is being achieved is by constructing cyberspace as a national security issue that needs to be addressed by the state. The Copenhagen school theory of securitisation has been adopted by this thesis as a framework to analyse the securitisation of UK cyberspace. The Copenhagen school framework depends upon the use of a speech act by a securitising actor to make a securitising move. As discussed in *2.3 Securitisation Speech Act Analysis*, key speech acts by state agents in the research period have been subjected to a deductive thematic analysis based on the key elements of the securitisation speech act as defined by the Copenhagen school (Buzan, Waever and de Wilde, 1998). This analysis focuses on securitising speech acts between 2012 and 2017, with a focus on the period of time around the introduction of the National Cyber Security Centre and the publication of the 2016 NCSS.

This period was chosen because it was a transformational period for the UK state's approach to cyber security due to the acknowledged failure of the 2011-2015 Cyber Security Strategy. This failure initiated some significant changes in both organisational structures and authorities, along with a more assertive approach to cyber security from state agencies. Many of these developments (for example, the introduction of the NCSC) represented exceptional measures demanded by the state, as a securitising actor, to address the cyber security threat. A clear process of securitisation has been used by the UK state to introduce these exceptional measures and to achieve their acceptance by a variety of different audiences, including both the cyber security community and the wider business community.

This analysis of the UK's initiative to securitise cyberspace highlights some interesting aspects of the process. There are indications that there are multiple audiences involved in this securitisation process, and that the securitising actor and threat articulation have been regularly adjusted to address specific audiences. The

continued use of speech acts to different audiences with the rhetorical structure required for securitisation indicates that the need to convince multiple audiences has been a key factor in the securitisation process.

Within the research period there has been evidence that the required effect on 'inter-unit relations' has not yet been realised. Specifically, private sector organisations, equipment manufacturers and individuals have not yet changed their behaviour to deliver cyber security to meet the requirements of the state. As a result, I would argue, that securitising actors have needed to continue to address new audiences through an extended securitisation process using multiple speech acts. Securitisation in this instance seems to be achieved through an ongoing process rather than a single specific act.

The securitisation effort to position greater state responsibility for cyber security as an issue of national security has become one of the main drivers of the relationship between the public and private sector in the provision of cyber security. It has provided the state with the justification for the development of new institutions such as the NCSC and acted as the basis for new regulatory interventions such as the General Data Protection Regulations (GDPR) and the Network and Information Security Directive (NIS).

However, analysis using securitisation theory may support a view that despite numerous securitising moves, the process of securitisation remains incomplete in that the securitisation move has not been fully accepted by the intended audience and there remains a security gap between the capabilities requested by the state as the securitising actor and the actions of functional actors in the private sector. This is particularly in relation to the secure implementation of computer networks and systems by private individuals and organisations and the development of new insecure networked devices associated with the Internet of Things (IoT), ranging from security cameras through to children's toys.

The 'cyber-threat' is present in the first documented UK National Security Strategy (NSS) (Cabinet Office, 2008). The strategy at the time was dominated by the threat

of international terrorism, and cyber was very much presented as a lower level emerging threat seen in the context of an enabler for existing threats, such as transnational organised crime "*…exploiting new opportunities, including revolutionary changes in technology and communications..*" (Cabinet Office, 2008, p. 12).

The 2008 NSS was followed by a Cyber Security Strategy (CSS) in 2009 which set up a Cyber Security Operations Centre (CSOC) in GCHQ Cheltenham alongside the Office of Cyber Security (OCS) (later the Office of Cyber Security and Information Assurance (OCSIA)) in the Cabinet Office. The 2009 CSS provides an early indication of some of the organisational issues that would inform the later Cyber Security Strategies with it being described as having "*missed an opportunity to review muddled structures*" (Norton-Taylor, 2009).

It is an indication of how quickly the cyber threat has developed, that just two years later in the 2010 National Security Strategy (HMG, 2010) "*Hostile attacks upon UK cyber space by other states and large scale cyber crime*" had been defined as a Tier 1 threat based on likelihood and potential impact placing the cyber-threat at the same level as the threat of international terrorism, major natural disaster, or an international military crisis.

In terms of response to the cyber-threat, it was this 2010 strategy that first asserted the need to "*develop a transformative programme for cyber security, which addresses threats from states, criminals and terrorists; and seizes the opportunities which cyber space provides for our future prosperity and for advancing our security interests.*" (HMG, 2010, p. 34). This was supported by an investment of £650 million and included expanding the CSOC in GCHQ.

The 2010 National Security Strategy was followed by a National Cyber Security Strategy for 2011-2016. This strategy was based on four key objectives of firstly, tackling cyber-crime and making the UK one of the most secure places in the world to do business; secondly, making the UK more resilient to cyber-attack and better able to protect its interests in cyberspace; thirdly, helping to shape an open, vibrant and stable cyberspace which the UK public can use safely and that supports open

societies; and fourthly, building the UK's cross-cutting knowledge, skills and capability to underpin all cyber security objectives (Cabinet-Office, 2011, p. 8).

The task of delivering against those objectives was supported by £860 million in government investment with a number of different government departments including the Department of Business, Innovation and Skills (BIS), the Home Office, the Ministry of Defence (MoD) the Foreign Office, the Department of Culture, Media and Sport (DCMS) and the Cabinet Office all taking lead responsibility for groups of actions. As a result, there were a number of organisations that had some responsibility for cyber security including the Centre for the Protection of National Infrastructure (CPNI), the Government Communications Headquarters (GCHQ) unit Communications Electronic-Security Group (CESG) which also provided the UK's Computer Emergency Response Team (CERT-UK), the National Cyber Crime Unit (NCCU), the Office of Cyber Security and Information Assurance (OCSIA) in the Cabinet Office, as well as Cyber Security Operations Centres (CSOCs) in both the MoD and GCHQ.

This complex and somewhat confused approach was highlighted by a 2013 report from the National Audit Office (NAO) which identified six government departments and nine other agencies involved in the delivery of the strategy. However, it is notable that the report identified that 59% of the additional funding had been allocated to the security agencies, showing the preeminent position of national security considerations and the security agencies in the state's investment in cyberspace.

With the exception of the development of military 'sovereign capabilities', the majority of the 2011 strategy emphasised cooperation with the private sector and international partners, building capability within existing organisational structures such as the National Crime Agency (NCA) or through existing programmes (such as CONTEST to counter online radicalisation) with government taking a role in

providing advice and encouragement with an emphasis on information sharing, education and skills development.

However, even as early as 2013 six key challenges faced by the government in implementing this strategy were identified by the NAO. These challenges were, influencing industry to protect and promote itself and UK plc, addressing the UK's current and future ICT and cyber security skills gap, increasing awareness so that people are not the weakest link, tackling cybercrime and enforcing the law at home and abroad, getting government to become more agile and joined-up, and demonstrating value for money (National Audit Office, 2013, p. 24).

By the time of a 2014 NAO report there were additional identified issues, including confused communication of cyber-threat information from multiple government departments. The report stated that "*…the 2014 InfoSec survey found that 67% of information security professionals thought intelligence was not shared effectively between government and industry.*" (National Audit Office, 2014, p. 12)

This report also identified the success of education and awareness initiatives as sporadic, with only 65% of individuals taking 10 out of 17 basic actions identified as fundamental to cyber security and only 8% of small businesses doing the same. Overall the NAO found that the programme "*…cannot yet demonstrate a clear link between the large number of individual outputs being delivered and an overall picture of benefits achieved.*" (National Audit Office, 2014, p. 5)

In another report in 2016 that focused on protecting information across government, the NAO delivered a review of information assurance within government departments which found:

1. Too many bodies with overlapping responsibilities operating in the centre of government;
2. Increasing dependencies between central government and the wider public sector meaning that traditional security boundaries have become blurred;

3. A need for wider reform beyond the introduction of the NCSC alongside a concern as to whether the NCSC would be able to operate effectively with the private sector;
4. The failure of the Cabinet Office to routinely collect or analyse government's performance in protecting information;
5. A need for the Cabinet Office to improve delivery of its centrally managed projects;
6. Uneven attention being paid to information governance across departments;
7. A lack of Cabinet Office access to expenditure and benefits data from departments;
8. Difficulty for government to attract people with the right skills

(National Audit Office, 2016).

This report inspired some very negative reporting in the industry press, for example, with *Computing* headlining it as "*NAO report slates the Cabinet Office's cyber security efforts*" (Leonard, 2016).

The sequence of negative NAO findings reflected the perceived failure of the 2011 cyber security strategy, which resulted in the new approaches outlined in the 2016 strategy. The threat of cyber-attack had become a more serious and complex threat to national security and as a result the 2015 National Security Strategy and Strategic Defence Review (HMG, 2015b) retained the Tier-1 categorisation of cyber threats. This was followed by the publication of the new NCSS in November 2016. This described the 2011 strategy as having: *"…achieved important outcomes by looking to the market to drive secure cyber behaviours…"* but in a clear indication of the difficulties in an environment with shared state and private sector responsibility, acknowledged its failure to deliver the security capabilities required to respond to the cyber threat with *"….this approach has not achieved the scale and pace of change required to stay ahead of the fast moving threat. We now need to go further."*(HMG, 2016, p. 9)

A good example of some of the difficulties inherent in the shared state and private sector responsibilities for cyber security is presented by the implementation of the Huawei Cyber Security Centre (HCSEC) in the UK.

The 2004 decision by BT to award the contract for transmission equipment in the *21st Century Network Project* to the Chinese supplier Huawei was a cause of concern in Government, and eventually led to the direct involvement of GCHQ in equipment deployments in the private infrastructure underpinning cyberspace. The contract was allowed to go ahead in the UK as it was deemed a commercial decision for BT and any interference with that decision (which is allowed for under the 1984 Telecommunications Act) would have potentially made the government liable for any commercial losses as a result[34]. The BT deployment led to a review by the Intelligence and Security Committee (ISC) and the establishment of the Huawei funded but GCHQ controlled Huawei Cyber Security Evaluation Centre (HCSEC) in 2010 to mitigate the risks of the deployment of Huawei equipment. Despite these efforts the ISC have made clear (quoting evidence from GCHQ) that "*…the software that is embedded in telecommunications equipment consists of 'over a million lines of code' and GCHQ has been clear from the outset that 'it is just impossible to go through that much code and be absolutely confident you have found everything'. There will therefore always be a risk in any telecommunications system, worldwide.*" (ISC, 2013, p. 12)

In 2018 the fourth annual report from the HCSEC Oversight Board concluded that it could "*….provide only limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks have been sufficiently mitigated.*" (HCSEC, 2018, p. 3) This was due to two major issues. Firstly, in being unable to validate that the code being tested by HCSEC was the same code as the network operators were installing in the UK infrastructure, and secondly an exposure due to a lack of control over security critical third-party components. It is worth noting that the strategy of validating code through 'binary equivalency' had been stated as

[34] Both the US and Australian governments went on to declare the deployment of Huawei equipment in similar network upgrades to be a risk to national security in 2012.

the objective for risk mitigation since the first oversight report of 2015 (HCSEC, 2015, p. 15). This would mean that the limited assurance admitted in 2018 has been the situation since HCSEC's inception.

The BT (and other telecommunications operators') decision to deploy Huawei equipment was a stark example of how commercial decisions could impact the CNI, and how little effective control the UK Government had over such decisions made by global private corporations with global supply chains. It also showed how little concern was given to national security considerations by the private sector due to the *"…conflict between the commercial imperative and national security, as a result of increasing private ownership of CNI assets combined with the globalisation of the telecommunications marketplace*" (ISC, 2013, p. 4). It would seem likely that the ISC analysis of the BT and Huawei decision has informed some of the thinking behind the UK cyber security strategy since 2013 especially as the HCSEC development was directly referenced in the November 2015 speech at GCHQ by the Chancellor of the Exchequer announcing the new development of new cyber capabilities. (Osborne, 2015).

As a result of the perceived failures in the 2011 strategy, the 2016 National Cyber Security Strategy and the introduction of the NCSC both represented a change in direction in terms of the provision of cyber security capabilities within Government, and the way in which Government would look to work with the private sector to deliver cyber security at a national security level.

In particular there has been an increase in the centralisation of cyber security responsibility and a change in strategic approach that suggests much more assertive government engagement in cyber security issues as opposed to the advice, guidance and encouragement that had reflected the themes of the 2011 strategy. This approach also included a strand of "International Action" which has been typified by a process of cyber security capacity building.

Cyber Security Capacity Building (CCB) has been a component of the National Cyber Security Strategy in both 2011 and 2016, with Foreign and Commonwealth Office leadership to build cyber security capabilities internationally. As well as bringing benefit to the countries in which cyber security capacity is being created, these initiatives are seen as representing a desire to "*protect against the spread of negative cross border externalities of vulnerabilities*" (Hohmann *et al.*, 2017, p. 10) on the basis that vulnerabilities in one country are a threat to another. This could include vulnerabilities that, for example, lead to safe havens for cyber-criminals, and the deployment of unsecured devices that could form part of damaging global DDOS attacks.

CCB is also seen as a tool for foreign policy, in particular by advocating specific models of internet governance and creating markets for cyber goods and services.

The FCO describes it as follows:

> "*The FCO works internationally to support a free, open, peaceful and secure cyberspace and deter malicious cyber activity. We work with partner countries to strengthen their cyber security capacity, reinforce the application of human rights online, promote stability in cyberspace and promote the multi-stakeholder approach to internet governance*"

With projects focused on what they described as *"…a wide range of cyber security capacities depending on individual countries' needs."*

This includes cyber security policy and strategy; cyber incident management and critical infrastructure protection; cybercrime; cyber security culture and skills; and cyber security standards. (HMG, 2018a).

In 2011 the FCO organised the 2011 Global Conference on Cyberspace (GCCS) that has since led to bi-annual conferences that collectively are known as "*The London Process*". These conferences are attended by government, civil society, and industry representatives.

The 2015 conference in the Hague, led to the creation of the Global Forum on Cyber Expertise (GFCE), which aims to "*…strengthen cyber capacity and expertise and to make the existing international cooperative efforts in this field more effective.*" (GFCE, 2016) In March 2020 the CYBIL database of GFCE projects lists more than than 570 projects ranging from training courses on cyber operations through to the development of security strategies and incident response capabilities (GFCE, 2019)

In the UK, as part of the 2011 Cyber Security Strategy the Foreign Office funded the Centre for Global Cyber Security Capacity Building in Oxford (HMG, 2013).

The 2016 National Cyber Security Strategy included International Action as one of the Government's responses to UK cyber security. This was based on objectives to "*safeguard the long-term future of a free, open, peaceful and secure cyberspace, driving economic growth and underpinning the UK's national security*" (HMG, 2016)

In order to achieve this, the strategy stated that the UK would champion the multi-stakeholder model of internet governance, oppose data localisation, and work to build the capacity of international partners to improve their own cyber security, and improve international cooperation.

This was an acknowledgment of the overseas origination of much of the cyber threat and the strategy defined a number of actions to deliver this:

- strengthen and embed a common understanding of responsible state behaviour in cyberspace;
- build on agreement that international law applies in cyberspace;
- continue to promote the agreement of voluntary, non-binding, norms of responsible state behaviour;
- support the development and implementation of confidence-building measures;
- increase our ability to disrupt and prosecute cyber criminals based abroad, especially in hard-to-reach jurisdictions;

- help foster an environment which allows our law enforcement agencies to work together to ensure fewer places exist where cyber criminals can act without fear of investigation and prosecution;
- promote the resilience of cyberspace by shaping the technical standards governing emerging technologies internationally (including encryption), making cyberspace more 'secure by design' and promoting best practice;
- work to build common approaches amongst like-minded countries for capabilities such as strong encryption, which have cross-border implications;
- build the capacity of others to tackle threats to the UK, and our interests overseas;
- continue to help our partners develop their own cyber security – since we share a single cyberspace, we collectively become stronger when each country improves its own defences;
- ensure that NATO is prepared for the conflicts of the 21st century, which will play out in cyberspace as well as on the battlefield;
- work with our allies to enable NATO to operate as effectively in cyberspace as it does on land, air and sea; and
- ensure that the 'London Process' of Global Conferences on Cyberspace continues to promote global consensus towards a free, open, peaceful and secure cyberspace.

(HMG, 2018b)

However, it should be noted that the international element of the cyber security strategy is (at least in terms of resources) a minor part of the overall strategy forming only 0.59% of the 2011 budget (slightly less than the project office for managing the strategy) (National Audit Office, 2014) and 1.8% of the 2016 budget, as compared with 87% of the budget dedicated to Deter and Defend (National Audit Office, 2019)

Some elements of the more assertive UK state approach to cyber secuirty (later defined in the new strategy) were first made public at the 2016 RSA Conference,

following which, the then Head of Cyber Security for CESG was quoted from a speech at the conference saying that

> "*….we are not winning the fight on cyber security*" and that "*….there's been something of a mantra in the UK that the solution to all of our problems is information sharing and public/private partnerships – that if we keep doing that then somehow it will magically cause improvement to happen. That approach by itself is not sufficient.*" (Alex Dewdney, CESG Head of Cyber Security quoted in Murdock, 2016)

He was also reported as stating that:

> "*We are starting to think about the extent to which government needs to be more interventionist and active in how it takes on some of these challenges – still with industry, but doing more than providing threat information and expecting companies to deal with it*" (Alex Dewdney, CESG Head of Cyber Security quoted in Ashford, 2016).

These comments provided a clear statement of intent for a change in government approach away from reliance on the actions of the private sector and with more emphasis on assertive state engagement in the issue. This intent is also reflected in the formal speech acts by state agents.

6.1 UK Cyberspace Securitisation Speech Acts

The Copenhagen School's theory of securitisation (Buzan, Waever and de Wilde, 1998) requires performative speech acts to securitise an issue. An analysis of speech acts related to UK cyberspace is able to identify specific security themes that have been consistently articulated in relation to cyber security and its relationship with national security issues. The methodology for analysis and a list of all the speeches included within the analysis is included in *2.3 Securitisation Speech Act Analysis*.

The initial speeches included in the analysis are those in 2012 from Jonathan Evans of MI5 and Iain Lobban of GCHQ, progressing through the 2015 announcement of

the NCSC through to the 2016 National Cyber Security Strategy and to the end of research period in January 2018.

The Copenhagen School argues that "*security is a speech act that securitises, that is constitutes one or more referent objects, historically the nation or the state, as threatened to their physical or ideational survival and therefore in need of urgent protection.*" (Hansen and Nissenbaum, 2009). Many of the speeches between 2012 and 2017 are structured in such a way as to indicate that this is their objective.

It should be noted that, writing in 1998, cyber-threats and attempts by the Pentagon to define cyber security issues as a threat were dismissed as a valid securitisation move as they *"….could possibly lead to actions within the computer field but with no cascading effects on other security issues*." (Buzan, Waever and de Wilde, 1998, p. 25) However, the development of cyberspace since 1998, the growth of economic dependency on cyberspace and information technology infrastructure across all sectors, and the use of cyber-capabilities to exert state power, require a different judgment to be made today. As a result it has been stated that "*….its understanding of security as a discursive modality with a particular rhetorical structure and political effect makes it particularly suited for a study of the formation and evolution of cyber security discourse.*" (Hansen and Nissenbaum, 2009)
It has also been argued that in the United States cyber security is effectively securitised on the basis of a number of institutional and organisational developments including cyber security strategies, Homeland Security cyber security focus, and the creation of the NATO CCDCOE (Hansen and Nissenbaum, 2009). This assertion is then used as the basis for identifying "*...cyber security as a particular sector within Security Studies*."

However, I would argue that, given the pervasive nature of information technology throughout Western society, the UK state does not (in securitisation terms) necessarily view cyberspace as a separate sector, but instead views it as a threat vector to any of the military, political, societal or economic sectors. This seems to be the UK Government view, with then Chancellor of the Exchequer, George Osborne,

describing the Internet as "*a vector of attack*" in terms of the threat to realspace entities such as banks, cars, schools, hospitals, electricity supplies, and air traffic control in the speech in which he launched the development of the NCSC and reinvigorated the securitisation of cyberspace in the UK. (Osborne, 2015)

This approach to cyberspace as an attack vector rather than a securitisation sector has been consistent in further statements identified as attempting the securitisation of UK cyberspace. There is little reference to specific cyber security referent objects, with an emphasis instead on economic and societal issues. For example, Defence Secretary, Michael Fallon directly connected cyber-threats to 'real-space' threats in his 2016 speech to RUSI when he said:

> *"Any threat we face…state sponsored aggression…global terror…attacks on elections…electoral machinery…media...and other key features of democracy…lone wolf attacks… any of these can have a cyber dimension."* (Fallon, 2016)

This again would suggest that cyber security needs to be analysed as a threat vector to all existing sectors of security rather than as a sector in its own right.

This approach is particularly appropriate to the state's securitisation of cyberspace as it serves to position cyber security as an element of realspace security with referent objects that are accepted as within the realm of state national security.

One way in which this securitisation is being achieved is through the use of speech acts to construct cyberspace as a national security issue that needs to be addressed by the state. The sue of speech acts by securitising actors is a key component of the Copenhagen School framework for analysis.

It is helpful not to view the speech acts relating to cyberspace as individual stand-alone acts of securitisation, but to position them as part of a developing narrative. In the case of UK cyberspace, securitisation has not been achieved by a single act, but instead by a continuum of speech acts representing a gradual escalation of the

level of securitisation, targeted at different audiences and extending the exceptional measures available to the state as the securitising actor.

The narrative can be seen as consisting of four key stages.

First, the 2012 speeches by Iain Lobban (Director GCHQ) and Jonathan Evans (DG MI5) that represented the first public statements by the Heads of Security Services on the subject of cyber security and positioning their own branch of the security services as key to delivering cyber security. Evans focuses on MI5's CPNI, while Lobban describes GCHQs importance to cyber security due to mastery of high-end communications technology and the combination of their intelligence mission with their information assurance responsibilities.[35] The Lobban speech is also noticeable for the strength of the call for change in the way in which cyber security is addressed, emphasising the increasing scale and complexity of the cyber threat and suggesting the need for new approaches from government, particularly in the realm of partnerships with industry, international partners and academia.

Second, the 2015 speeches by Robert Hannigan (Director GCHQ) and Ciaran Martin (as GCHQ DG Cyber Security) to two sections of the cyber security community, at IA15 (a public sector focused Information Assurance event) and Infosec 2015 (an event focused on the private cyber security industry) both strengthened the positioning of GCHQ with a wider role in cyber security. Martin stated that "*….our role 'such as the Prime Minister may determine' has evolved into a more general one to support the UK's cyber security across the economy…*" and emphasising the importance of the skills available from GCHQ by declaring that "*….our role only really works if we have a world class intelligence capability to draw on.*" Hannigan, meanwhile, referred to responding to the cyber-threat as "*...absolutely central to our mission….*" and called for a "*step change*" in the way in which cyber security was being addressed. He also established GCHQ as a reliable partner in cyberspace who was not opposed to

[35] If this was a sign of competition for mission between these two services, it is, looking back, clear that it was GCHQ that won, with the CPNI being incorporated into GCHQ's NCSC in 2016.

encryption, did not want to weaken security with back doors, and did not encourage or retain known vulnerabilities for their own use.

The third stage was a set of speeches given around the introduction of the NCSC. This included Chancellor George Osborne's 2015 speech announcing the NCSC, Ciaran Martin's 2016 speech to the Billington Cyber Security Conference (his first public speech as Chief Executive of the NCSC) and Phillip Hammond's 2016 speech to the Microsoft Future Decoded conference at which he launched the 2016 - 2021 National Cyber Security Strategy. It is this set of speeches that seem to most clearly adhere to the requirements of a securitisation speech act.

Finally, there is a fourth category of follow-on speeches which are notable for the change in audience from a security and technology audience to a more business oriented community, including speeches at summits organised by The Times, The Telegraph, the Confederation of British Industry (CBI) and the Institute of Directors (IoD) and the renewed engagement of other departments of state in the delivery of speech acts that may have a more immediate connection with these audiences such as Matt Hancock while at the DCMS (rather than the Cabinet Office where speech acts normally did not meet the criteria to be considered a securitisation speech act.)

For the Copenhagen School, a successful speech act is defined as "*a combination of language and society, of both intrinsic features of speech and the group that authorizes and recognizes that speech.*" (Buzan, Waever and de Wilde, 1998, p. 32) This shows the importance of not only what is said in the speech act, but who says it (political agency) and who they say it to (audience). Analysis of political agency and audience is included *in Table 15 Cyber Security Speech Acts Political Agency and Audience* on page 210.

The internal conditions for a successful speech act require that it "*follow the security form, the grammar of security, and construct a plot that includes existential threat, point of no return, and a possible way out….*" (Buzan, Waever and de Wilde, 1998, p. 33)

There are two important elements to the external aspect of the speech act, these being "*the social capital of the enunciator, the securitising actor, who must be in a position of authority..*" and the facilitating conditions for securitisation, specifically that "*it is more likely that one can conjure a security threat if certain objects can be referred to that are generally held to be threatening.*" (Buzan, Waever and de Wilde, 1998, p. 33)

There is some criticism of using the speech act as a means to invoke a process of securitisation, in particular as it is "*potentially too narrow to grasp fully the social contexts and complex communicative and institutional processes at work in contemporary politics*" and that focusing on the rhetorical and discursive attributes of the speech act "*stands in contrast to a communicative environment ever more structured by televisual media and the importance of images*." (Williams, 2003). However, I would argue that in this instance, the speech act offers significant value as a formal, pre-prepared and documented act that allows important elements of the act such as audience and political agency to be identified. As a mechanism for understanding the securitisation process the formal speech acts are also useful in that they are limited in scope (and so more easily analysed in detail), have a known securitising actor and audience and can be placed in a timeline to understand their relevance in context of other speech acts.

The securitisation of UK cyberspace has seen engagement between securitising actors and audience through non-verbal media (most often electronic documents) such as the inclusion of cyber security in national security strategies (HMG, 2010, 2015b) and the resulting cyber security strategies (Cabinet-Office, 2011; HMG, 2016). However, these can be interpreted as having provided context for, or having been initiated by one or more speech acts that have specifically addressed securitisation in the rhetorical form outlined by the Copenhagen School.

Initial analysis of the cyber speeches showed that there was a subset of speeches that conformed to the rhetorical structure of securitisation, and so can be considered securitising moves. These speeches are shown in

below:

Table 9 Securitisation Speeches

Date	Speaker	Position	Audience
26 June 2012	Jonathan Evans	DG MI5	City of London
12 Oct 2012	Iain Lobban	Director GCHQ	IISS
17 June 2014	Ciaran Martin	DG Cyber Security GCHQ	IA14 Conference
2 June 2015	Ciaran Martin	DG Cyber Security GCHQ	Infosec 2015
10 Nov 2015	Robert Hannigan	Director GCHQ	IA15 Conference
17 Nov 2015	George Osborne	Chancellor of the Exchequer	GCHQ
13 Sept 2016	Ciaran Martin	Head of NCSC	Billington Conference
20 Oct 2016	Michael Fallon	Defence Secretary	RUSI Cyber Symposium
1 Nov 2016	Philip Hammond	Chancellor of the Exchequer	Microsoft Conference
14 Feb 2017	Philip Hammond	Chancellor of the Exchequer	NCSC
27 March 2017	Matt Hancock	Minister for Digital & Culture	IoD Conference
13 Sept 2017	Ciaran Martin	CEO NCSC	CBI
15 Nov 2017	Ciaran Martin	CEO NCSC	Times Tech Summit

It is noticeable that this subset of speeches is much more focused in terms of the political agency involved. None of the speeches from the Cabinet Office (either Francis Maude or Matt Hancock) conform to the structure of a securitising move, and the same applies to all but one of the speeches from Michael Fallon while Defence Secretary, leaving speeches only from the security services (and in particular GCHQ/NCSC) and the Chancellor as the Chair of the Cabinet Cyber Security Committee whose 2015 speech was delivered at GCHQ in Cheltenham in addition to Matt Hancock while at the DCMS.

Within these speeches it is that by George Osborne at GCHQ (Osborne, 2015) which stands out as introducing a significant change in the UK state's approach to cyber security, with government agencies taking a more central and proactive role. This speech in particular seemed to meet the standard of the "*…modern state, represented by statesmen embodies the main capacity to securitise questions...statesmen representing the state and uttering security in the name of the state are the privileged agents in the securitising process.*" (Huysmans, 2002).

However, despite the importance of this particular speech act, it cannot be viewed in isolation and is more usefully judged in relation to other securitisation moves that influence the audience and the context in which a specific performative utterance takes place (Balzacq, 2005).

I would argue that Osborne's speech represents the culmination of the securitisation process that had started with the 2012 speeches by Jonathan Evans and Iain Lobban. Osborne's GCHQ speech is also semantically and thematically connected to the earlier 2015 speeches by Robert Hannigan at the IA15 Conference (Hannigan, 2015) and Ciaran Martin at Infosec 2015 (Martin, 2015).

Robert Hannigan's speech as Director of GCHQ set out many of the themes that have driven the actions of the NCSC and have remained prominent in state cyber security discourse through 2017. This speech was notable for its emphasis on partnerships and GCHQ's history of working with industry, coupled with the positioning of GCHQ as a key component of the UK cyber security environment. The speech also included assertions that they advocate encryption, have no desire to implement 'back doors' in security products, and do not encourage or fail to disclose vulnerabilities. This specifically addressed three of the key criticisms that are regularly made of GCHQ.

However, in an interview with *The Cipher Brief* Hannigan went on record in 2017 stating that GCHQ did not disclose all vulnerabilities as "*if you don't withhold anything at all, you have basically no tools to do the job*" and that they shared

vulnerabilities with the NSA with almost no oversight from the executive branch or other areas of government and without any basis in legislation. (Maxey, 2017)[36]

In terms of threats, the speech identified major destructive attacks, theft of personal data, and the cumulative "*pernicious impact of smaller scale attacks*". The main threat actors were identified as hostile states, organised crime, and terrorist groups using the internet for propaganda purposes.

Hannigan's 2015 speech also made clear the need for a change of strategy and a transformation in approach and indicated an approach involving automated mechanisms and "*structural features which would allow more automatic protection from basic attacks*". In addition, the speech made clear that the market for cyber security was not working with both cyber security standards and engagement of the private sector not having progressed to where they should be.

The speech posed as questions, or options to consider, many of the exceptional powers that have since been acquired such as DNS filtering and DMARC implementation that have been implemented by the NCSC, and suggests that the threat warrants a change to established rules.

The process of securitisation is looking to create a "*...shared understanding of what is to be considered and collectively responded to as a threat.*" (Buzan, Waever and de Wilde, 1998, p. 26) and presenting cyber threats as an existential threat is an essential element of all of the securitising speech acts. This is followed by a statement of the negative effects of not responding to the threat (the point of no return) in relation to the referent objects of the securitisation move, and finally a call for the exceptional measures required to respond to the threat or how the threat legitimises breaking established rules. This is the rhetorical structure of a securitisation speech act.

A successful securitisation is described as having three components of "*...existential threats, emergency action, and effects on interunit relations by breaking free of rules.*"

[36] It is worth noting that this was confirmed by the release of the GCHQ Vulnerability Equities' Process in November 2018.

(Buzan, Waever and de Wilde, 1998, p. 26) In this context the speech act is a perlocutionary act that creates the securitisation itself, although it has also been argued that the speech act is simply "*a performatic illocutionary act*" and therefore not the securitising act in itself (Balzacq, 2005).

The analysis of the speech acts that have represented a securitising move in UK cyberspace suggests they were intended as a perlocutionary act, but has also shown that the effect is dependent on the audience for the speech act and that individual speech acts have been required to address specific audiences.

The key securitising phrases from the relevant speeches including referent objects, identified threats and exceptional means demanded are included as ***Appendix A: Key Securitisation Speech*** Acts 2012 - 2017 on page 325.

Any securitising move is undertaken by a securitising actor who has a certain political agency that allows them to make a securitising move. The cyber security speeches that have been identified from the period 2012 to 2017 were from a range of state authorities including the Cabinet Office, GCHQ, Ministry of Defence, Chancellor of the Exchequer, DCMS and the NCSC. Within securitisation theory, identification of the securitising actor can be at an organisational or individual level.

In all the identified instances of securitising speech acts, the securitising actor in relation to UK cyberspace has been the state. There have been speeches from a number of different state agencies and individuals with different authority in relation to cyberspace, but all are speaking on behalf of the state from a position that would give them recognised authority in relation to a specific audience. This explains the choice of securitising actors that have included the Chancellor of the Exchequer (as chair of the Cabinet committee for cyber security); the Secretary of Defence; the Head of the NCSC, the Director of GCHQ, the DG of MI5 and the Minister for Digital Culture, Media and Sport.

The individuals, behaving as securitising actors, have had a stronger relationship with some sectors (societal, economic, military and political) than with cyberspace.

This may add some more weight to the suggestion that in the case of the UK state, cyberspace is not being treated as a sector in and of itself, but as a threat vector to the more traditional security sectors. The idea that cyber-threats are nothing more than 'old wine in new bottles' (Grabosky, 2001) has been used by Ciaran Martin with reference to the motivations behind the cyber threat when he said "*Money, power and propaganda. Hardly new concepts for humanity*." (Martin, 2016a) This, again, represents a justification for existing state structures being applied in the context of cyber security on the basis that if the problems are those that are traditionally handled by the state, then they should continue to be so in cyberspace.

Analysis of the speech acts identified as associated with the securitisation of UK cyberspace seem to support the concept of an effective securitising speech act as being a "*pragmatic act*" that can be broken down into the level of agent and the act (Mey, 2001 cited in Balzacq (2005)). The agent level includes three aspects, identified as firstly, "*…the power position and personal identity of who 'does' security..*"' secondly, "*…the social identity which operates to both constrain and enable the behaviour of the securitising actor..*" and thirdly *"…the nature and the capacity of the target audience and the main opponents or alternative voices..*" (Balzacq, 2005). In relation to the ongoing securitisation of UK cyberspace, the securitising actors are all speaking on behalf of the state from a position that would give them recognised authority.

The specific securitising actors have in some cases been tailored to the audience, so the Chancellor of the Exchequer spoke to GCHQ as the Chair of the Cyber Security Committee, Ciaran Martin as the Head of the NCSC and also a part of GCHQ spoke at a conference attended by members of the US intelligence agencies and Michael Fallon as Defence Secretary has been the only government speaker on cyber issues to a military audience. One noticeable change has been the removal of the Cabinet Office from the securitisation process, with only one significant speech by Matt Hancock to the business community at the Telegraph Cyber Security Summit in 2016. Future speeches, including that at the CBI in 2017 by Matt Hancock were made after he moved to become Minister for Digital, Culture, Media and Sport in

2016. Since that time the Cabinet Office's public engagement has been slight, with only one speech by Damien Green recorded in 2017 to celebrate a year of the National Cyber Security Centre (Green, 2017). Following Green's resignation, his successor (David Lidington) made no set-piece statements relating to cyber security.

Many of the individual speech acts include direct claims to the political agency required to make the act in question. In the UK, the most clearly noticeable direct claims to agency within the speech acts have been those that have been used to establish the credentials of GCHQ in cyber security. This started with Lobban's references to GCHQ's "*clear security mission*" and the assertion that "*Our mastery of high end communications technology is hugely relevant to the problems of cyber security*" (Lobban, 2012). Later, Ciaran Martin claimed that "*…we [GCHQ] have always had the lead role for information assurance in UK government, so our current work on UK cyber security is a natural extension of that*" (Martin, 2015). This was supported by Hannigan's assertion that "*Information Security is every bit as much a part of GCHQ's DNA as intelligence gathering*" (Hannigan, 2015) and Osborne's 2015 speech to GCHQ launching the NCSC which asserted that "*…I am clear that the answer to the question 'who does cyber?' for the British government is – to very large degree – 'GCHQ'*" (Osborne, 2015).

Apart from Osborne's speech as Chancellor, the speeches from GCHQ both assert the role of GCHQ and the political agency of a GCHQ representative to speak about cyber security. These two roles are intricately linked, but not the same thing. For example, George Osborne's position as Chancellor was a role that gave the political agency to speak about cyber security, but clearly not for the Treasury to take on a cyber security function.

Some other speeches have also been noticeable for their 'perlocutionary nature' solely regarding the strength of the speaker's political agency that provides them with the authority to speak on cyber security. For example, Damien Green's 2017 Cabinet Office speech stated that *"…my role as First Secretary of State means that I am responsible for the overarching Government National Cyber Security Strategy and the*

National Cyber Security Programme which delivers it" (Green, 2017) and Philip Hammond's key speech to the Microsoft Decoded Conference in 2016 at which he launched the 2016 National Cyber Security Strategy makes direct reference to his position as Chair of the permanent Cabinet Cyber Committee and his previous responsibility for GCHQ as Foreign Secretary, stating that "*…through that involvement, I've seen the full extent of those threats….*" (Hammond, 2016)

Alongside the securitising actors, there are also functional actors, which are defined as those actors *"…who affect the dynamics of a sector. Without being the referent object or the actor calling for security on behalf of the referent object, this is an actor who significantly influences decisions in the field of security."* (Buzan, Waever and de Wilde, 1998, p. 36)

If we look at the sector as "UK Cyberspace" there are a number of functional actors identified within the speech acts relating to cyberspace that have very different positions within the securitisation discourse. Excluding those identified as referent objects, either specifically or by aggregation through the various speech acts, the main functional actors can be categorised as either Threat Actors, or Security Providers.

Threat actors would include all those who are identified as presenting a cyber security threat to the referent objects, while the Security Providers would include those who are engaged in delivering cyber security solution, including organisations within the cyber security industry.

There are particular groups that could be considered to blur the functional definitions of securitisation. For example, the Cyber Security or Information Assurance Department within a major CSP organisation that would be considered part of the UK CNI, is both a component of a frequently cited referent object (CNI) as well as being a key security actor implementing cyber security solutions on behalf of other organisations as well as their own.

The NCSC, who are a key securitising actor are also a key security provider for UK cyberspace, giving them a unique position of influence within the cyber security

community, effectively creating a position where the NCSC can both claim the need for a cyber security intervention and implement their own solution in response.

This unique cyber security environment has resulted in a common theme emerging from almost all the securitisation speech acts of the need for partnership between organisations that are a referent object, the security providers and the securitising actors. There has been a consistent recognition (both before and after the introduction of the NCSC) of the need for partnerships between the securitising actor - speaking as the state – and the other functional actors engaged in delivering cyber security.

It is important to avoid confusing these functional actors with the securitising actor. Functional actors may make statements concerning security, and they could be involved in delivering security (firewall products, secure software etc.) but they do not have the capacity to securitise in the context of national security and it would be a mistake to interpret their statements as a securitising move. This particularly relates to some of the elements of securitisation identified by Balzacq, including the audience's readiness to be convinced by the securitising move and the ability of the securitising actor to win the audience's support (Balzacq, 2005).

For example, Facebook, Google, Microsoft, YouTube and others may all have significant roles to play in the securitisation of cyberspace – but it is as functional actors – not as securitising actors in relation to UK national security in cyberspace where securitising moves have been exclusively within the domain of the state.

As one would expect, many of the securitising speech acts include these functional actors within the audience, and much of the content is focused on ensuring their commitment to the securitisation proposed by the securitising actor. As examples, the speech by Phillip Hammond to the Microsoft Future Decoded conference (Hammond, 2016), or any of the speeches from GCHQ and the NCSC to Information Assurance and private sector InfoSec conferences (Martin, 2014; Hannigan, 2015), and more recently, the business community through engagement

with the CBI and the IoD (Hancock, 2017; Martin, 2017b) are addressing functional actors.

Interestingly, the key functional actors have changed over time, with a move away from the 'technical community' to the 'business community' that could be expected to be at CBI and IoD events. This reflects a changing focus in the securitisation message to ensure that businesses are doing everything required of them as functional actors in the securitisation process.

Within the securitisation speech acts, there are a number of threat actors within UK cyberspace that emerge. The most common reference is to a generic "cyber threat" which is often represented as a conflation of threat actors such as criminal gangs, attack methodologies such as DDOS attacks and SQL injection, specific attacks such as CloudHopper and Wannacry, and attack consequences such as data loss and business costs. This leads to a wide variety of 'threats' being described.

The threats and threat actors identified from the securitisation speech acts are shown in *Table 10 Threats and Threat Actors 2012 - 2017* on page 187 below.

Table 10 Threats and Threat Actors 2012 - 2017

Date	Speaker	Position	Threat
June 2012	Jonathan Evans (Evans, 2012)	DG MI5	Criminals
			States
			Terrorist groups
Oct 2012	Iain Lobban (Lobban, 2012)	Director GHHQ	States
			E-crime
			Insiders
			Botnets
			Personal data theft
			Fraud
June 2014	Ciaran Martin	DG Cyber Security, GCHQ	Supply chain threat.
			State sponsored attackers
June 2015	Ciaran Martin	DG Cyber Security, GCHQ	Criminals
			State sponsored attacks
			Rogue States
			States
			Terrorists
			Hacktivists

Table 10 - Threats and Threat Actors 2012-2017 (continued)

Date	Speaker	Position	Threat
Sept 2015	Michael Fallon	Defence Secretary	Russia
			ISIL
Nov 2015	Robert Hannigan	Director, GCHQ	Hostile States
			Major organised crime syndicates
			Terrorist groups
Nov 2015	George Osborne	Chancellor of the Exchequer	Criminals
			Hostile powers
			Terrorists
Sept 2016	Ciaran Martin	Head of NCSC	Ransomware
			SQL Injection
			Hostile States
			Criminal Gangs
			Terrorists
			Hacktivists
			Lone Operators
			APTs

Table 10 - Threats and Threat Actors 2012-2017 (continued)

Date	Speaker	Position	Threat
Nov 2016	Philip Hammond	Chancellor of the Exchequer	IoT Botnets
			Spear Phishing
			Hostile Foreign Actors
Oct 2016	Michael Fallon	Defence Secretary	State sponsored aggression
			Global Terror
			Attacks on elections
			Lone wolf attacks
Feb 2017	Philip Hammond	Chancellor of the Exchequer	Electronic data theft
			Online ransom
			Phishing
			Viruses
			State sponsored attacks
Mar 2017	Matt Hancock	Minister for Digital & Culture	Cyber breaches
			Cyber attacks

Table 10 - Threats and Threat Actors 2012-2017 (continued)

Date	Speaker	Position	Threat
Sept 2017	Ciaran Martin	CEO NCSC	State attacks
			Small scale cyber attacks
			Data breaches
			Ransomware (wannacry)
Nov 2017	Ciaran Martin	CEO NCSC	Hostile States
			Rampant criminality
Sept 2017	Ciaran Martin	CEO NCSC	Unsophisticated cyber-attacks (wannacry)
			Cloudhopper
			Mirai botnet
			Global threats

However, despite the lack of clarity in the speech acts, it is possible to identify some consistent threats and threat actors specified throughout the 2012 – 2017 timeframe.

It is noticeable that two of the three threat actors initially identified in 2012 remained the same in 2017, with criminals and states now represented as hostile states and rampant criminality. The only significant change has been the downplaying of the terrorist cyber threat, which may be consistent with the decline of ISIL over the same period.

This threat messaging seems to be trying to ensure that there is a firm distinction between 'high end' state level threats that are presented as being the domain of GCHQ and the NCSC (a view supported by the interview data gathered for this project which indicated that the capability to defend against nation state attacks was beyond most private organisations) and the lower level 'death by a thousand cuts' attacks which are positioned as the responsibility of individuals and private organisations.

This is a reinforcement of messages from 2014 and 2015 such as that from Ciaran Martin at IA14 when talking about the role of industry in cyber security he said:

"*This partnership will allow the Government, and GCHQ in particular, to focus increasingly on how we maximise the impact of our unique visibility and understanding of high-end threats. That's those state groups, their proxies, and serious criminals I've already mentioned. Our global intelligence capability helps illuminate and counter these threats*" (Martin, 2014).

This was reiterated in 2015 when he said:

"*…our direct role has to be focussed on those high end threats and attacks that the state is best placed to detect and frame the response to. Risks to organisations in our critical national infrastructure. Our historic role securing defence assets. Our role in helping Government departments…*" (Martin, 2015).

This fixes the role firmly within the boundaries of the traditional public sector role of CESG and CPNI. The 2017 demarcation between state level and 'other' attacks

was accompanied by a renewal of the distinct differentiation in the role of the NCSC, which was that the NCSC would deliver the response to the state level threats, and would "*provide the infrastructure*" for addressing the non-state level attacks (Martin, 2017b). This again indicates a clear desire on the part of the NCSC not to take on the role of being responsible for responding to non-state level attacks, but to provide the environment for private organisations to develop their own capabilities as security providers.

However, beneath the consistency in this element of the threat identification there are some obvious differences in how the threats have been constructed at different times and for different audiences, in particular through adjustment of the identified threat to suit the audience. For example. the highly technical InfoSec audience were provided with detailed threats based on technical capability in a speech delivered by the then DG Cyber Security of GCHQ, while the securitisation speech acts by successive Chancellors launching the NCSC and NCSS respectively provided a much more generic threat picture. As one would expect, the Defence Secretary's speeches focused on hostile state activity and 'global terror' while omitting any reference to criminality, although including attacks on elections and 'lone wolf' attacks.

In terms of threat actors, the narrative has remained consistent in terms of involving hostile states as a key threat actor, with a range of non-state actors including at various time hacktivists, individual hackers, cyber-criminals, insiders, and terrorists.

There has frequently been a lack of clarity regarding what exactly the threat was from non-state actors. This has developed over time, for example, Osborne's 2015 speech raised the possibility for a destructive and life threatening terrorist cyber-attack on the CNI and Ciaran Martin confirmed a terrorist intent to attack through cyberspace but dismissed it due to a lack of capability (Martin, 2016b). The main speech-act focus on cyber-terrorism has been on the less existential threat of

terrorist use of the internet for command and control, propaganda, and radicalisation as a conduit to the realspace terrorist threat.

Interestingly, despite the attribution of the Talk Talk data breach to the stereotypical "teenager in his bedroom" (BBC, 2016) and the media publicity surrounding alleged US Government hacker Lauri Love (Parkin, 2017) the identification of the threat from 'hackers' and 'hacktivists' as entities acting on their own is extremely limited, with references to hacking and hackers mainly in the context of crime or as a generic term for perpetrators of a computer based attack, regardless of the source of the threat.

Throughout the securitisation discourse there has been a consistent reference to the partnerships that are required with other organisations to enable the securitisation of UK cyberspace. This has generally been based on vague terminology such as "*industry*" (Lobban, 2012; Hammond, 2016) "*business*" (Hancock, 2017), "*private sector partners*" (Martin, 2016b), or "*commercial partners*" (Hannigan, 2015). There has also been little detail on what such a partnership would entail apart from information sharing. The consistency of this call for partnership acknowledges the importance of the private sector within the securitisation process, and is more fully described in *Table 18 The Call for Partnership* on page 221.

The chosen referent objects of securitising moves are also important as a justification for the proposed securitisation. The referent object is defined as "*things that are seen to be existentially threatened and have a legitimate claim to survival.*"(Buzan, Waever and de Wilde, 1998, p. 36). The securitisation approach allows for a greater range of referent objects of security rather than a traditional view of the state as the object of security. However, not everything can be constructed as a referent object. It has to be something that 'has to survive' and so justifies actions being taken to ensure its survival. Individual firms, for example, are seen as unlikely to meet the criteria to be a referent object for security, and as a result, while individual firms may be used as examples of what can go wrong, they are not used individually as referent objects for securitisation.

Scale is a factor in "*...determining what constitutes a successful referent object of security…*" (Buzan, Waever and de Wilde, 1998, p. 36) with individuals or small groups unable to establish legitimacy as an object of security. This is reflected in the case of the securitisation of UK cyberspace by reference to collective-groups, such as the "*critical national infrastructure*" (Lobban, 2012; Martin, 2017b) or "*UK industry*" (Hancock, 2017) as well as generic national issues such as "*confidence in the digital economy*" which provide the necessary scale for the commercial impact of cyber-attacks to be an appropriate referent object.

The referent objects, as referred to in individual speeches, are shown in

Table 11 Referent Objects 2012 – **2017** below. There has been a general coherence to this message over the 2012 – 2017 period around key referent objects of the Critical National Infrastructure and economic prosperity as represented by businesses and the digital economy.

The relative emphasis on different referent objects seems to have been subject to some adjustment, depending upon the audience and occasion, for example with information assets being much more visible in Ciaran Martin's address to InfoSec15, military systems and armaments supply in statements by (then Defence Secretary) Michael Fallon when speaking to defence oriented audiences at RUSI and Chatham House, George Osborne's much less specific referent objects of "*our country*" and "*our citizens*" and Matt Hancock's reference to "*digital society*". These are very different referent objects that have been determined to reflect the political agency of the speaker and appeal to the anticipated concerns of the specific audience.

One noticeable change in 2017, which is judged to be in response to alleged Russian state interference in the US 2016 Presidential election and the UK's Brexit vote has been the introduction of referent objects of "*democracy*", "*the international order*", and "*the lens through which we view the world*" by NCSC Head Ciaran Martin, as additions to the CNI, confidence in the digital economy, and economic prosperity.

While this may reflect a reaction to the current *hack du jour*, equally it has emphasised the importance of state domain elements as referent objects for securitisation, which in turn reaffirms the importance of state institutions in addressing the threats to these referent objects.

Table 11 Referent Objects 2012 – 2017

Date	Speaker	Audience	Referent Object
June 2012	Jonathan Evans (Evans, 2012)	City of London	"integrity, confidentiality and availability of government information"
			"safety and security of our infrastructure"
			"intellectual property"
			"future prosperity"
			"companies and corporations"
Oct 2012	Iain Lobban (Lobban, 2012)	IISS	"critical national infrastructure"
			"individual citizens"
			"Governments services"
			"economic prosperity"
			"economic well-being and national interest"
Dec 2012	Francis Maude (Maude, 2012)	IA12 Conference	"businesses"
			"confidence in the web"
			"government networks"
			"the economy"

Table 11 Referent Objects 2012-2017 (continued)

Date	Speaker	Audience	Referent Object
March 2013	Francis Maude (Maude, 2013)	CiSP Launch Event	"our way of life" "our economy"
June 2014	Francis Maude (Maude, 2014b)	IA14 Conference	*Not a securitisation speech act/no referent objects*
June 2014	Ciaran Martin (Martin, 2014)	IA14 Conference	"the UK economy" "government and industry networks"
March 2014	Francis Maude (Maude, 2014a)	CERT-UK Launch Event	*Not a securitisation speech act/no referent objects*
June 2015	Ciaran Martin (Martin, 2015)	Infosec 2015	"government secrets" "safety and security of our infrastructure" "the intellectual property that underpins our future prosperity" "commercially sensitive information" [37]
Nov 2015	Robert Hannigan (Hannigan, 2015)	IA15 Conference	"the UK and our prosperity" "trust in public services" "critical national assets"

[37] Ciaran Martin directly quoted the Evans 2012 speech as the main referent objects included within this speech.

Table 11 Referent Objects 2012-2017 (continued)

Date	Speaker	Audience	Referent Object
Nov 2015	George Osborne	GCHQ	"our country"
	(Osborne, 2015)		"our citizens"
			"our public services"
March 2016	Matt Hancock	Telegraph Conference	"our digital society"
	(Hancock, 2016)		"critical national infrastructure"
Sept 2016	Ciaran Martin	Billington Conference	"confidence in our increasingly digitised economy"
	(Martin, 2016b)		Critical national infrastructure
			Government systems
Sept 2015	Michael Fallon (Fallon, 2015)s	UK/FR Cyber Symposium	Digitally dependent societies
			"Our transport networks.
			Our energy networks.
			Our banking systems.
			Our economy as a whole."
Oct 2016	Michael Fallon (Fallon, 2016)	RUSI Cyber Symposium	"our systems"
			"armaments or our energy supplies"
			"government systems"
			"elections, electoral machinery, media, and other key features of democracy"

Table 11 Referent Objects 2012-2017 (continued)

Date	Speaker	Audience	Referent Object
Nov 2016	Philip Hammond (Hammond, 2016)	Microsoft Conference	"our economy"
			"the infrastructure of the state"
Feb 2017	Philip Hammond (Hammond, 2017)	NCSC	"critical national infrastructure"
			"businesses"
			"the general public"
March 2017	Matt Hancock (Hancock, 2017)	IoD Conference	"UK industry"
			"Digital economy"
27 June 2017	Michael Fallon (Fallon, 2017)	Chatham House	"national infrastructure"
			"military and civilian systems"
13 Sept 2017	Ciaran Martin (Martin, 2017b)	CBI	"democracy"
			"critical national infrastructure"
			"the lens through which we view the world"
			"economic prosperity"
			"confidence in the digital economy"

Table 11 Referent Objects 2012-2017 (continued)

Date	Speaker	Audience	Referent Object
14 Sept 2017	Ciaran Martin (Martin, 2017a)	EU Cyber Security Conf.	"democracies"
			"critical services"
			"prosperity"
			"citizens"
			"confidence in the digital economy"
15 Nov 2017	Ciaran Martin (Martin, 2017c)	Times Tech Summit	"international order"
			"confidence in the digital economy"
			"individual corporations"

One of the main questions regarding a legitimate security threat is whether the scale of a threat (in addition to the scale of the referent object) is sufficient to create this legitimacy (Buzan, Waever and de Wilde, 1998, p. 106). The scale of the cyber threat is a common thread within the speech acts identified, measured either in terms of the number of attacks, the number of victims, or the consequences of the attacks. For example, George Osborne's reference to a doubling of the number of cyber national security incidents in a twelve month period (Osborne, 2015), Matt Hancock's assertion that "*…one in three small firms, and 65% of large businesses are known to have, experienced a cyber breach or attack in the past year…*" (Hancock, 2017) or Robert Hannigan's quote of a cyber-attack's "*…average cost being between £1.46 and £3.14 million per incident for larger companies..*" (Hannigan, 2015)

The 2012 speech by Iain Lobban, then Director of GCHQ now seems very understated in its articulation of the threat, with a focus on the technical nature of the threats with direct references to "*botnets*", "*e-crime*", "*insiders*" and "*personal data theft*". Although the referent objects of Government Systems, economic success and the CNI have proved to be more persistent themes, the description of the potential effect of cyber-attacks has become much more impactful.

Phillip Hammond's speech to the Microsoft Future Decoded conference in 2016 was a significant escalation of the perception of the existential nature of the threat with references to the "*infrastructure of the state itself*", "*our economic future*", and placing cyber-attacks as "*the precursor to any future state-on-state conflict*" in addition to the threat to critical national infrastructure.

Much of this formal discourse relates to economic security, despite the fact that securitisation on economic grounds presents difficulties due to the inherent uncertainty required by liberal economics to drive efficiency. The system naturally incorporates a level of insecurity. However, securitisation remains potentially legitimate in the case of disruptions to the economic system that are outside of the norm, i.e. *"…that changes occur only within known limits, that is, that the misfortune of individual actors or relations does not trigger damaging chain reactions that threaten the*

system. 'Known Limits' can be interpreted as socially accepted risks of economic enterprise or as calculated risk." (Buzan, Waever and de Wilde, 1998, p. 107)

This is reflected in much of the discourse regarding the exceptional scale and nature of the damage caused by cyber-crime in particular, and the anticipated effect a loss of confidence in cyberspace caused by an aggregate of damage to individual economic actors may have on the potential for the economy to operate. This has been accompanied by a related concern for the ability of the state to deliver digital services such as state benefits and tax collection. It is in the nature of the untargeted mass of cyber-threats that risk to the systems of economic actors will also apply to state capabilities. If confidence and public trust in the digital economy is at risk, it is reasonable to assume that confidence and trust in the state digital services component of the digital economy is also at risk.

An additional scale issue for the securitisation of UK cyberspace (and in particular for securitisation discourse designed to change the behaviour of functional actors) is that for the majority of the functional actors who may be a target of an attack, the threat is not an obvious existential threat, but is instead the background noise of constant small scale attacks that have to be defended against.

In many cases the cumulative nature of this threat has been presented in order to enhance its potential to be an existential threat, for example, "*….those smaller scale but voluminous attacks which cumulatively do so much damage….*" (Martin, 2015); "*the constant, death-by-a-thousand-cuts set of lower level attacks. And it is these attacks, as much as the prospect of a destructive attack, that risks public confidence in our digital world.*" (Hannigan, 2015); "*Imagine the cumulative impact of repeated catastrophic breaches, eroding that basic faith in the internet that we need for our online economy and social life to function.*" (Osborne, 2015); "*…if hundreds of thousands of data breaches become commonplace, that confidence is undermined, permanently and fatally*" and "*…the threat to prosperity from an aggregation of cyber attacks that would damage consumer confidence…*" (Martin, 2017b)

This threat aggregation has enabled what might be considered 'business as usual' type cyber-attacks to be considered, in aggregate, as an existential threat to the

economic security of the UK, in particular through 'confidence in the digital economy' which has been presented as a valid basis for securitisation.

Copenhagen School theory also suggests that "*…a security argument always involves two predictions. What will happen if we do not take 'security action' (the threat) and what will happen if we do.*" These predictions can be seen within the speech acts identified along with the intention to "*…construct a plot that includes existential threat, point of no return, and a possible way out…*" (Buzan, Waever and de Wilde, 1998)

Table 12 Security Predictions Osborne 2015, *Table 13 Security Predictions Hammond 2016* and *Table 14 Security Predictions Fallon 2016* below identify the security predictions of the two Chancellor's speeches and the Secretary of Defence's speech prior to the launch of the NCSC as those that contain the most significant security predictions at the time of the introduction of the NCSC and the 2016 NCSS.

Table 12 Security Predictions Osborne 2015

Speech	Effect of Not Taking Security Action	Effect of Taking Security Action
Osborne 2015	"...there will be no economic security for our country without national security. Nowhere is that more true than when it comes to cyber." "From our banks to our cars, our military to our schools, whatever is online is also a target." "The stakes could hardly be higher – if our electricity supply, or our air traffic control, or our hospitals were successfully attacked online, the impact could be measured not just in terms of economic damage, but of lives lost." "They [ISIL] have not been able to use it to kill people yet by attacking our infrastructure through cyber attack. They do not yet have that capability. But we know they want it, and are doing their best to build it." "Imagine the cumulative impact of repeated catastrophic breaches, eroding that basic faith in the internet that we need for our online economy and social life to function."	"It will ensure that we have the skills the structures, the tools, the companies and the partners we need." "...it will make Britain one of the best protected countries in the world; it will give our companies and citizens the tools they need to stay safe from cyber-attack; and it will create jobs and prosperity."

Table 13 Security Predictions Hammond 2016

Speech	Effect of Not Taking Security Action	Effect of Taking Security Action
Hammond 2016	"Trust in the Internet and the infrastructure on which it relies is fundamental to our economic future. Because without that trust, faith in the whole digital edifice will fall away." "…significant consequences including loss of customer data, significant financial costs, disruption of services, reputational damage, indeed threats to the infrastructure of the state itself." "…threats to our data, to our IP, to our military secrets, to our financial information and perhaps most important of all to our infrastructure itself." "If we do not have the ability to respond to in cyberspace to an attack which takes down our power networks leaving us in darkness, or hits our air traffic control system, grounding our planes, we would be left with the impossible choice of turning the other cheek and ignoring the devastating consequences or resorting to a military response."	"And now we want to add: the most secure cyber environment anywhere; where government, business, security agencies and academia work together to defeat the hackers and the phishers, the criminals and the rogue states. Creating one more reason to make Britain the location of choice for cutting edge digital business to start, to grow and to succeed."

Table 14 Security Predictions Fallon 2016

Speech	Effect of Not Taking Security Action	Effect of Taking Security Action
Fallon 2016	"Any threat we face…state sponsored aggression…global terror…attacks on elections…electoral machinery…media...and other key features of democracy…lone wolf attacks… any of these can have a cyber dimension. What's more…these threats are growing." "It is only a matter of time before we have to deal with a major attack on British interests."	"If we get cyber right we have the potential too (sic) not just to bolster our capability and improve our security…but to bring in the jobs, the investment…the talent to power our economies for decades to come. And if we do that job properly…100 years from now…our successors will look back on this moment…the dawn of a new cyber age…as the moment when a potentially devastating threat turned into a dazzling economic and social opportunity."

All three of these speeches follow the rhetorical structure of security predictions with details on what will happen if action is not taken, a list of actions being taken, and finally a promise as to what will happen if action is taken.

There is an imbalance between the definition of the threat of what will happen if no action is taken, and the somewhat vague promises of economic success that will result from action. In some ways this is inevitable, as often, the net result of any defensive action is simply that 'life goes on'. However, this may impact the effectiveness of engaging private sector commercial enterprises in the provision of state level national security, especially when cyber threats may be based on a risk assessment that can be offset with cyber-insurance.

There is evidence from the United States that the impact of a cyber-attack can be catastrophic for the majority of small businesses, with estimates that 60% of small and medium sized businesses that are attacked go out of business within six months (Aguilar, 2015). However, there is little evidence of the threat to small businesses reaching the forefront of UK securitisation discourse until Matt Hancock's speech to the IoD in March 2017 where he emphasised the NCSC's *"…new role in supporting the 'wider economy and society' – that is, the parts of industry and society the security services have not traditionally engaged with – including small and medium sized businesses…."* (Hancock, 2017).

Although other threats are often mentioned there is often no clear articulation of the effect of that threat. Statements such as "*the whole digital edifice will fade away*" (Hammond, 2016) or "*the stakes could hardly be higher*" (Osborne, 2015) are long on hyperbole but short on any tangible description of the effect of any lack of security action. This too, may not be surprising, as the UK has never suffered a catastrophic cyber-attack.

The Wannacry ransomware attack was explicitly mentioned by Ciaran Martin to the CBI in 2017 as "*the more severe end of the threat*" but even in the case of Wannacry, the long term impact was minimal and the total cost to the NHS was limited at an estimated £92 million (Field, 2018). Other 'cyber attacks' referenced in the

securitisation discourse have included, TV5, Talk-Talk, Equifax, Saudi Aramco, and the UK Houses of Parliament. However, it is possible that none of these are particularly impactful for a UK audience when they are overseas such as TV5, Equifax and Saudi Aramco, and I would argue that the UK attacks were less impactful in their effects. The only impact of the Houses of Parliament attack was MPs were unable to access email, which was less shocking than it could have been due to the revelations of shared passwords and a basic disregard for even the most fundamental cyber security discipline (BBC, 2017). The Talk-Talk attack was a limited number of users and arguably became more notable for the complete lack of understanding shown by Talk-Talk's Chief Executive, Dido Harding (Pemberton, 2015) and the simplicity of the attack on an unmaintained system through an easily patched SQL injection vulnerability by a teenage boy.

None of these attacks resulted in the 'whole digital edifice fading away' or had any discernible impact on confidence in the digital economy or limited the nation's economic success. This may be one factor that could help "*figure out this perplexing conundrum - given people are aware of cyber security and the threat, and there is money to invest, why aren't those simple defences being improved to the extent they need to be?*" (Martin, 2017d). To date the catastrophic events promised in the securitisation of UK cyberspace have yet to become evident in any way that would guarantee a successful securitisation move accepted by the business community.

The audience for any securitising move is important within the Copenhagen School's definition as any "*…issue is securitised only if and when the audience accepts it as such.*" This is a result of the Copenhagen School's social constructivist perspective where "*…the effects are inter-subjectively constructed and therefore not controlled by the agents themselves.*" The success of any securitising speech act depends on the audience acting upon it.

This adds a level of complexity to the analysis of the securitisation of UK cyberspace as (given the nature of cyberspace and its multiple stakeholders) there are several distinct audiences that would need to accept any securitisation move to be able to consider it as having securitised cyberspace. This has been reflected by the number

of different audiences that have been addressed and the choice of securitising agents to address them over the period of securitisation.

The audiences for the key speeches leading up to the introduction of the NCSC included GCHQ (George Osborne at GCHQ), the military community, (Michael Fallon at RUSI and Chatham House), US Intelligence Agencies engaged in cyber security (Ciaran Martin at the Billington Cyber Security Conference), and the wider technology community (Philip Hammond at Microsoft Decoded Futures Conference).

These initial audiences were clearly important to the securitisation of cyberspace and the institutionalisation of the security response through the introduction of the NCSC. There was an element of reassurance to organisations that were affected by the introduction of the NCSC (e.g. GCHQ) and a reaffirmation of existing relationships that would continue to be important moving forward (e.g. the NSA).

A full list of audiences for speech acts is shown in *Table 15 Cyber Security Speech Acts Political Agency and Audience* below

Table 15 Cyber Security Speech Acts Political Agency and Audience

Speech	Agency	Audience
Evans 2012	DG MI5	Military, Government, Private Security related organisations
Lobban 2012	Director GCHQ	Security Analysts
Maude 2012	Cabinet Office Minister	Information security community
Maude 2013	Cabinet Office Minister	Representatives from UK Businesses (Launch of CiSP)
Maude 2014	Cabinet Office Minister	Information security community
Fallon 2015	Defence Secretary	UK/French Military
Martin 2015	DG Cyber Security GCHQ	Information security community
Hannigan 2015	Director GCHQ	Information security community
Osborne 2015	Chancellor of Exchequer	GCHQ
Hancock 2016	Cabinet Office Minister	Chief Executives and Board Level Directors (Telegraph Cyber Security Conference)
Martin 2016	Chief Executive NCSC	US Cyber Security Community
Fallon 2016	Defence Secretary	Defence/Military Analysts (RUSI)
Hammond 2016	Chancellor of the Exchequer	UK IT Community (Microsoft Decoded Conference)
Hammond 2017	Chancellor of the Exchequer	NCSC
Hancock 2017	Minister for Digital	UK Business (IoD)
Fallon 2017	Defence Secretary	Analysts (Chatham House)
Martin 2017 (a)	Chief Executive NCSC	UK Business (CBI)
Martin 2017 (b)	Chief Executive NCSC	European Cyber Leaders (Government)

Osborne's GCHQ speech was important because GCHQ was the home for departments such as CESG, CSOC, and CERT-UK, which would form the core of the NCSC. The NCSC would continue to be a part of GCHQ as it was anticipated that it would continue to require access to the more traditional GCHQ interception and surveillance capabilities[38].

Ciaran Martin's speech at the Billington Conference (also attended by Mike Rogers, Head of Cyber Command and Director of the NSA, who was explicitly referenced in Martin's speech) reflected a need to ensure the relationship with the US Agencies was not disturbed by the changes. Fallon's speech reflected the need for the traditionally independent military cyber community to support the development of the NCSC, and Hammond's speech at *Microsoft Decoded* reflected the fact that the support of the private sector technical community would be required to deliver many of the solutions the NCSC would call upon to improve the security of UK cyberspace.

However, speeches following the introduction of the NCSC show a shift in audience emphasis to the wider business community and an emphasis on the global nature of the cyber threat. This includes most notably the speeches by Ciaran Martin to the CBI (Martin, 2017b) and Matt Hancock's speech to the Institute of Directors (Hancock, 2017). These speeches both used the rhetorical structure of securitisation, but without significant threat exaggeration and with the reduced sense of urgency that results from the process of institutionalisation.

These two speeches are also notable in that they directly addressed the business community at a senior level (i.e. not the security services or the technical community that constituted the 2015/16 audiences for securitisation). The language remained one of securitisation, in particular in relation to more concrete exceptional measures aimed at the business community such as the 2018 introduction of the General Data Protection Regulations (GDPR).

[38] It is worth noting that at the time of the Osborne speech the NCSC was positioned organisationally as that it would 'report to the Director of GCHQ' as opposed to today's positioning as 'an integral part of GCHQ'.

It is clear from both these speeches that the process of securitisation is at best only partially successful at this point. The business community, as a major target audience (of functional actors) for the securitisation process, has yet to respond in a way that has met the requirements of the securitising actors and allowed a successful securitisation.

Table 16 2017 Speeches indicating partial securitisation below shows the speeches from Ciaran Martin and Matt Hancock in 2017 that conform to the rhetorical structure of a securitisation speech act and so indicate that the process of securitisation is ongoing at this point.

Table 16 2017 Speeches indicating partial securitisation

	Martin 2017	Hancock 2017
Threat	"…threats to our way of life or our critical services." "…the threat to prosperity from an aggregation of cyber-attacks."	"…65% of large businesses are known to have experience a cyber breach or attack…" "…the costs of a successful attack can be huge…."
Referent Objects	Confidence in the Digital Economy	UK industry Digital economy.
Exceptional Measures	Regulation including GDPR Increased financial penalties	Requiring suppliers to have Cyber Essentials Certifications New Cyber Innovation Centres Cyber education programmes
Effect of not taking action	Breaches unreported	"...courting chaos and catering to criminals…" Impact of GDPR
Effect of taking action	Reliable data Improved identification of attackers More robust insurance framework Stronger protections	Development of UK cyber security industry. The UK as the safest place to do business online.

A key part of the securitisation process is the demand for exceptional measures to be taken in order to respond to the articulated threat. In relation to UK cyberspace, these exceptional measures have developed over time, and have been different depending on the political agency behind the speech act and the audience.

Table 17 Exceptional Measures Demanded Speech Acts 2012 - 2017

Speech	Exceptional Measures Required
Evans 2012	Engagement with private sector
	Investment in world class capabilities, technologies and skills
	Increased levels of international cooperation
	Balance between regulation and flexibility
Lobban 2012	Prioritisation of cyber in SDSR.
	Direct feed of information from CNI operators
	Change in relationship between national security agencies and key industry players
	International coordination of counter measures
	Different approach to government/industry partnership
Martin 2014	"….applied our world-class technical expertise to assess some of the most critical IT systems in the country…increase capacity to deliver these reviews and advice"
	"…develop our partnership with CSPs by deepening our sharing of threat information…"
	"…focus on how we maximise the impact of our unique visibility and understanding of high end threats."

Table 17 Exceptional Measures Demanded Speech Acts 2012 – 2017 (continued)

Speech	Exceptional Measures Required
Martin 2015	New approaches – working internationally with FBI
	Acceptance of GCHQ advice
	Acknowledgment of position of GCHQ dealing with cyber security in the economy as a whole
	Ability to draw on intelligence capabilities
Hannigan 2015	The capability to access information for national security purposes.
	More capability for automatic defence.
	Structural features to allow for more automatic protections.
	Changes to make the market work better
	Changes to promote cyber security and skills required

Table 17 Exceptional Measures Demanded Speech Acts 2012 – 2017 (continued)

Speech	Exceptional Measures Required
Osborne 2015	"It is right that we invest in our cyber defences even at a time when we must cut other budgets."
	"Only government can legislate and regulate. Only government can collect secret intelligence."
	"…introduce stronger defences for government systems…"
	"…all the internet service providers will as a matter of routine divert known bad addresses."
	"…the regulatory framework it needs, particularly in the sectors we define as the Critical National Infrastructure."
	"…establish a single National Cyber Centre…"
	"…building our own offensive cyber capability – a dedicated ability to counter-attack in cyberspace."
	"Imagine the cumulative impact of repeated catastrophic breaches, eroding that basic faith in the internet that we need for our online economy and social life to function."
	"It will ensure that we have the skills the structures, the tools, the companies and the partners we need."
	"...it will make Britain one of the best protected countries in the world; it will give our companies and citizens the tools they need to stay safe from cyber-attack; and it will create jobs and prosperity."
Hammond 2016	"…government taking a more active cyber defence approach – supporting industry's use of automate defence techniques to block, disrupt and neutralise malicious activity…"
	"…strengthening our law enforcement capabilities…."
	"…continue to invest in our offensive cyber capabilities…"
	"…we will strike back in kind when we are attacked…"
	"...deploy the high level skills the government has, principally in GCHQ, to support the development of commercial applications to enhance cyber security."
	"..[The NCSC] will link up with law enforcement…"

Table 17 Exceptional Measures Demanded Speech Acts 2012 – 2017 (continued)

Speech	Exceptional Measures Required
Fallon 2015	Cyber 'hardwired into UK defence's DNA.'
	Upgrade of military capabilities.
	Creation of Joint Forces Cyber Group
	Improving Public Sector network resilience
	Building new Public Sector Network
	Testing private sector capacity to withstand cyber attack
	CiSP creation
Fallon 2016	£265 M to 'root out' vulnerabilities in defence systems.
	Integration of offensive cyber into military capabilities.
	77 Brigade and 1st Reconnaissance Brigade. Influence operations, counter hybrid warfare, battlefield intelligence.
	New Defence Cyber School.
	Full spectrum response
Martin 2016 (Billington)	BGP & SS7 Protocol Changes
	DNS Filtering Implementation

Table 17 Exceptional Measures Demanded Speech Acts 2012 – 2017 (continued)

Speech	Exceptional Measures Required
Hammond 2016	Active Cyber Defence
	Strengthening Law Enforcement
	Offensive Cyber Capability
	Creation of NCSC
Hammond 2017	Business secondments to the NCSC
	Partnership with business
	Bringing together intelligence and security agencies with the public and business community.
Martin 2017 (CBI)	"…secret intelligence capabilities combined with partnerships with law enforcement, other governments and global industry…"
	Compliance with new regulation. GDPR
	Active Cyber Defence partnerships
	Re-evaluation of corporate security policies
	Boardroom conversations on cyber
	Education of individual employees
	Acceptance of NCSC framework
Martin 2017 (Times Technology Summit)	Acquiring information from corporations on plans and actions
	Acceptance of NCSC frameworks
	Technical defences at scale
	DMARC
	Corporations to focus on reducing vulnerabilities, leaving NCSC free to deal with state attacks

Osborne's speech in particular is significant not only for the allocation of £1.9 billion during a time of government cuts, but also as it represented the first public acknowledgment of GCHQ as the cyber lead for the UK, reorganised the existing cyber capabilities of CPNI, CERT-UK and CESG into a single unit reporting to GCHQ.

The same speech also included a threat of regulation in cyber security, suggested the introduction of internet filtering by the ISP community, and, although an offensive cyber plan was publicly avowed in 2013 by then Defence Secretary Philip Hammond (Blitz, 2013), this speech was the first time it was stated that an offensive cyber capability existed and would be used to retaliate. The offensive cyber capability, DNS filtering, regulation, and consolidation of capability into GCHQ all represented a significant change and an intention to increase the exercise of state power in cyberspace.

There are some consistent themes over specific periods. For example, in the lead up to the announcement of the NCSC there are consistent calls for the acceptance of the unique expertise of GCHQ to address cyber issues, with Hammond, Martin, Hannigan and Osborne all emphasising the role of the state and in particular GCHQ. This continued into 2017 with both Martin and Hammond re-emphasising the central role of GCHQ.

The creation of the NCSC in 2016 can be seen as a recognition of the persistent nature of the cyber threat leading to a situation whereby "*the response and sense of urgency become institutionalised*."(Buzan, Waever and de Wilde, 1998, pp. 27–28) Philip Hammond's speech at the opening of the NCSC shows a change in tone away from the catastrophic images of earlier speeches and an implied acceptance of the urgency of the situation, with a focus on specific actions rather than the threat articulation.

One of the most consistent themes throughout the period has been a call for partnership between government and the private sector. Securitisation theory suggests that one measure of how important a securitisation move may be is the

scale of any impact such a move may have on wider patterns of relations. A successful securitisation move would include "*…effects on interunit relations by breaking free of rules.*" (Buzan, Waever and de Wilde, 1998, p. 26) The requirement for greater levels of cooperation by the private sector would represent such a change in inter-unit relations.

The speeches shown in *Table 18* below provide some of the examples of the regular calls for cooperative action and in particular for the engagement of the private sector with Government.

Table 18 The Call for Partnership

Date	Speaker	Audience	Call for Partnership
26 June 2012	Jonathan Evans (Evans, 2012)	City of London	"The Government's National Cyber Security Strategy makes clear that success in this endeavour is only possible if it engages not just government but also the private sector in tackling cyber crime, making the UK more resilient to cyber attacks, shaping an open and stable internet and developing our skills base."
12 Oct 2012	Iain Lobban (Lobban, 2012)	IISS	"…we need to deepen Government's dialogue and partnership with the Industry partners who deliver the systems and services that need securing. In many cases they have an equal or greater stake in ensuring proper protection and realising efficiencies."
			"…a different approach to Government-industry partnership…"
4 Dec 2012	Francis Maude (Maude, 2012)	IA12 Conference	"Success hinges on government and law enforcement agencies building even stronger partnerships with the private sector to combat the threat."
			"But one thing is certain - to succeed going forward we will have to work together - to share our resources, skills and intelligence. It is through strong partnerships between government, the industry, academia and the public that we will continue to enjoy the many and still emerging benefits of a networked world."

Table 18 The Call for Partnership (continued)

Date	Speaker	Audience	Call for Partnership
27 March 2013	Francis Maude (Maude, 2013)	CiSP Launch Event	"This kind of working is the future: government and industry working hand-in-hand to fight a common threat. Some have suggested a more regulated approach – but our experience here in the UK shows that a voluntary arrangement based on trust and shared interests can work. There is a growing realisation that it is only by working together - not limited by the boundaries of commercial interests – that we can ensure that the UK can continue to realise the benefits of a vibrant, open and safe online environment. This is a shared challenge and we all share a responsibility to meet it."
16 June 2014	Francis Maude (Maude, 2014b)	IA14 Conference	"This is the pattern for success: governments and businesses working together to pool expertise, learn lessons, share capabilities and coordinate action." "The strength of our partnerships, and the trust that enables us to share information, will allow us to build a safe and secure economy, and grasp the opportunity for future growth, so everyone can prosper from the digital age."
17 June 2014	Ciaran Martin (Martin, 2014)	IA14 Conference	"In cyber security, we're not hearing business telling Government to get out of the way. But ultimately, business will want to look after itself, with a strong partnership with Government. This partnership will allow the Government, and GCHQ in particular, to focus increasingly on how we maximise the impact of our unique visibility and understanding of high-end threats."

Table 18 The Call for Partnership (continued)

Date	Speaker	Audience	Call for Partnership
31 March 2014	Francis Maude (Maude, 2014a)	CERT-UK Launch Event	"…no one entity – particularly government - can tackle these threats on its own. So we put partnerships at the heart of that strategy." "…ever closer coordination between government, business and academia to share insights and share advice…"
10 Nov 2015	Robert Hannigan (Hannigan, 2015)	IA15 Conference	"I am all too aware that we can only achieve anything in partnership. Every day I am reminded of the importance of our partnerships - our contractors, who make up a third of our workforce, our suppliers, our commercial partners, those who work with us lawfully on both intelligence and cyber security, and the experts with whom we develop our knowledge and expertise. We have an excellent, proud and long record of working with industry - back through the Second World War - to promote the highest standards of information security in the UK." "…we need these partnerships more than ever because of the scale and diversity of the threat." "There are a whole plethora of partnerships between Government, industry and academia. Cyber Security is a shared problem and no one branch of society can solve it alone. But there is a long way to go. Information sharing partnerships are essential, but progress has been patchy. There is more that can be done with academia. There is undoubtedly more we can do to cooperate on cyber security internationally…"
17 Nov. 2015	George Osborne (Osborne, 2015)	GCHQ	"…the Centre [NCSC] will also have a strong public face and will work hand in hand with industry, academia and international partners to keep the UK protected against cyber attacks."

Table 18 The Call for Partnership (continued)

Date	Speaker	Audience	Call for Partnership
3 March 2016	Matt Hancock (Hancock, 2016)	Telegraph Conference	"...vital to recognise this is an issue for CEOs as well as spooks."
13 Sept 2016	Ciaran Martin (Martin, 2016b)	Billington Conference	"…we'll have formalised and integrated operational partnerships with law enforcement, defence and private industry." "…we'll continue to work with our private sector partners to find and fix vulnerabilities…"
1 Nov 2016	Philip Hammond (Hammond, 2016)	Microsoft Conference	"We will work in partnership with industry to apply technologies that reduce the impact of cyber-attacks, while driving up security standards across both public and private sectors." "…[the NCSS] sets out clearly how we intend to develop our partnerships with business to achieve that. But government cannot be solely responsible for managing cyber risk. Chief executives and Boards must recognise that they have a responsibility to manage cyber risks, just as they would any other operational risk. Similarly, technology companies…must take responsibility for incorporating the best possible security measures into the design of their products."

Table 18 The Call for Partnership (continued)

Date	Speaker	Audience	Call for Partnership
14 Feb 2017	Philip Hammond (Hammond, 2017)	NCSC	"…it will focus on partnership. Our intelligence and security agencies are the best in the world. No question. Our digital sector is also the best in the world – contributing a bigger proportion of our GDP every year than any other country in the G20…….what we are doing here is, bringing them together, this centre will work hand in hand with industry to keep the UK safe. 65% of large businesses reported a cyber breach or attack in the past 12 months. Yet nine out of ten businesses don't even have an incident management plan in the event of a cyber breach. Business has to sharpen its approach as the scale of the threat from cyber increases and intensifies. Just as you would expect a shop on the high street to fix its locks and burglar alarms, so businesses operating digitally need to fix their online security. And this Centre stands ready to help them in doing that. It can be as simple as providing guidance on things like ransomware and device security so that the public and businesses can protect themselves. Or it could be drawing on our most sophisticated capabilities to road-test and make available safeguards against more sophisticated threats. Or mobilising the resources of public and private sectors to intercept, defeat and mitigate the effects of a concerted cyber assault. Either way, its success will rely on partnerships."
27 March 2017	Matt Hancock (Hancock, 2017)	IoD	"This is something which can only be done through partnership between business and Government"

Table 18 The Call for Partnership (continued)

Date	Speaker	Audience	Call for Partnership
13 Sept 2017	Ciaran Martin (Martin, 2017b)	CBI	"GCHQ's secret intelligence capabilities alongside the ground-breaking partnerships with law enforcement, other governments and global industry have helped produce one of the most capable defences around." "It means innovative partnerships, like our threat-sharing with CSPs, which blocks tens of millions of attacks, automatically, every month."

The 2012 speech by Iain Lobban identified an opportunity for "*Government and the telecommunications sector, hardware and software vendors and managed service providers…*" to work together, and that "*…if we get the partnership approach right we can develop a thriving business…*" (Lobban, 2012), although there is no further definition as to what this partnership might look like. Alongside the call for UK partnership there was also a recognition of a need for international partnerships to be in place due to the transnational nature of the cyber threat.

Jonathan Evans (DG MI5) made an early reference to the need for partnership at the inaugural Lord Mayor's Defence and Security Lecture (Evans, 2012) in which he stated that "*…success in this endeavour is only possible if it engages not just government but also the private sector in tackling cyber-crime, making the UK more resilient to cyber-attacks, shaping an open and stable internet and developing our skills base…*" and spoke positively about the sector based vulnerability information sharing partnerships.

The IA14 Conference organised by GCHQ was given the tag line "*Meeting the cyber security challenge in partnership*" (GCHQ, 2014b) and Francis Maude's keynote speech was trailed as one that "*…emphasises that businesses and government are stronger working together to meet today's cyber challenges*" (GCHQ, 2014a), but included the assertion that "*We're all responsible for our own security, in government, in business, in our homes and whenever we go online.*" (Maude, 2014b).

Evans' 2012 speech was heavily referenced by Ciaran Martin in his 2015 speech to Infosecurity Europe. However, there was no specific mention of partnership requirements, but instead an emphasis on guidance from GCHQ such as the 10 Steps to Cyber Security from 2012 (CESG, 2012), Cyber Essentials, and the CERT-UK '*Common Cyber Attacks: Reducing the Impact*' (NCSC, 2016a) that should be followed by private corporations while GCHQ "*…focussed on the high end threats and attacks that the state is best placed to detect and frame the response to.*" (Martin, 2015)

Lobban and Evans' themes were also repeated in Robert Hannigan's 2015 speech to IA15 (Hannigan, 2015) where partnership was one of the three themes for the future of cyber security, but with the description of even information sharing partnerships as "*patchy*" and

an assertion that "*there is a long way to go*" but with an understanding that "*…we need these partnerships more than ever because of the scale and diversity of the threat.*"

It is noticeable however, that in the lead up to the 2016 NCSS, during which, the government acknowledged the relative failure of the 2011-2016 strategy, there is a greater emphasis on the role of the state in cyber security and indications that existing approaches were not working. This was typified by CESG's Head of Cyber Security reported statements at RSA16 which stated that the current partnership and information sharing approaches were not sufficient (Murdock, 2016) and that a more interventionist approach would be required from government (Ashford, 2016).

Osborne's 2015 speech (Osborne, 2015) also indicated a much more central role for the state, asserting that "*Government has a duty to protect the country from hostile attack. Government has a duty to protect its citizens and companies from crime*" and involvement with the private sector was focused on supporting start-ups in the cyber security industry and putting in place a regulatory framework, particularly for the CNI sectors, but emphasised that "*companies in those sectors have a responsibility to ensure their own resilience.*"

Despite an early reference to cyber security as a "*shared responsibility*" this speech was also notable for the limited suggestion of any collaborative partnership with the private sector to deliver cyber security, except for the specific reference to HCSEC in Banbury as an example of "*…encouraging Huawei to invest safely in the UK though partnership with GCHQ*". This could be considered a creative use of the word 'partnership' to describe an oversight mechanism needed to offset the national security risk of Chinese manufactured telecommunications equipment, and it is possibly a reflection of Osborne's enthusiasm for Chinese investment (Warman, 2013; HMG, 2015a) rather than any value it has as a component of national security.

Matt Hancock's 2016 speech at the Telegraph Cyber Security Conference (Hancock, 2016) (which was part of the launch of the NCSC Prospectus) identified "*shared responsibility*" as one of three elements required for a strong cyber defence and "*…a duty that we owe our fellow citizens…*". The speech acknowledged the fact that a majority of the CNI was in private hands but referenced the "*gap between awareness and action*" and the lack of preparedness on the part of the private sector.

Matt Hancock's speech to the IoD asserted that cyber security "*…is something which can only be done through partnership between business and Government*". However he again highlighted "*…the gap between awareness and action…*" in the business community and suggested companies were "*courting chaos and catering to criminals*"(Hancock, 2017). Ciaran Martin's late 2017 speech at *The Times Tech Summit* asked "*….given people are aware of cyber security and the threat and there is money to invest, why aren't these simple defences being improved to the extent they need to be?*" and encouraged organisations to "*get these basics right.*" (Martin, 2017c)

This would indicate that an ongoing process of securitisation is not yet complete and that although the 'securitising moves' have been made for cyber security, the actions of the business audience would indicate that it has not been fully accepted and the securitisation impact on the private sector has been insufficient. This is reflected in the changes to the approach to cyber security from the 2010 to the 2015 National Cyber Security Strategy, with a much more assertive approach being taken in the 2015 NCSS, which has since been followed by the use of EU regulation to further direct the private sector through the implementation of GDPR and NIS.

The organisational design for this new assertive approach was interesting for the positioning of the NCSC as a part of GCHQ. State discourse around this decision has focused on the long-standing GCHQ role providing Information Assurance for the UK Government, and the importance of access to GCHQ technical and intelligence capabilities as justification for the chosen organisational structure.

However, there have been indications of a more difficult relationship between GCHQ and the private sector technology industry. These were exacerbated by the Snowden revelations concerning some of the activities being pursued by GCHQ and the NSA, including allegations of equipment supply chain interference and the targeting of engineering staff in the Belgian national telecommunications operator in Operation SOCIALIST.

This private sector frustration was matched by GCHQ who have described the private sector Internet industry as being 'in denial' of the use of systems by terrorist groups and failing to adequately support law enforcement and the intelligence agencies in fighting terrorism and child sexual exploitation (Hannigan, 2014). The creation of the NCSC has been presented as offering a mechanism for GCHQ to work with the private sector in a more open and

collaborative way and take on a more public-facing role "*without having to compromise its covert operations.*" (Reeve, 2017).

One of the results of the securitisation of UK cyberspace and in particular the more assertive approach indicated during the securitisation process has been the introduction of new institutions to address the threat, accompanied by the expansion of the power of existing institutions, in particular GCHQ.

It is a function of modern society to organise danger by "*providing an institutional environment that plays a central role in the production and regulation of particular dangers*." (Huysmans, 2002) The dangers inherent in cyberspace are no exception and their institutionalisation has played a central role in the securitisation process by expanding the population of securitising actors who are in a position to add to the securitisation discourse from a position of authority with the capacity to successfully securitise.

The most significant institutional change was the introduction of the NCSC as part of GCHQ, and this has enabled GCHQ to consolidate and extend its remit in relation to cyber security and increasingly to monopolise the power to define the cyber threat to the extent that the Chancellor of the Exchequer was able to make the statement that "*I am clear that the answer to the question 'who does cyber' for the British government is – to a very large degree – 'GCHQ'*." (Osborne, 2015)

Since the 2011 Cyber Security Strategy, GCHQ, through the NCSC has extended its influence in the cyber domain by absorbing the cyber elements of the MI5 unit of the Centre for the Protection of National Infrastructure (CPNI) into the NCSC, which includes the CSIRT-UK incident response team; absorbing the UK-CERT (Computer Emergency Response Team) which had previously operated from within the Cabinet Office. This means that NCSC has absorbed CSIRTUK (previously part of CPNI), CERT-UK (from the Cabinet Office) and GovCERT-UK which was part of CESG within GCHQ; absorbing the Cyber Information Sharing Partnership (CiSP) which was formerly within the Cabinet Office; forming a Joint Operations Cell (JOC) with the National Crime Agency (NCA) to address the use of the Internet to enable child sexual exploitation (National Crime Agency, 2015); incorporating the

UK Cyber Security Operations Centre (CSOC)[39]; controlling the National Technical Assistance Centre that is responsible for the technical implementation of any electronic surveillance warrant granted to any of the nine agencies authorised by the Regulation of Investigatory Powers Act (RIPA) (GCHQ, 2016)l; securing involvement in the National Offensive Cyber Programme (NOCP) alongside the military; and chairing the Oversight Board of the Huawei Cyber Security Centre and appointing its Managing Director.

In addition, the NCSC also now controls the certification of individual qualifications in cyber security; the certification of cyber security products; the certification of education (undergraduate and postgraduate degrees) and training in cyber security; and threat evaluation through the Centre for Cyber Assessment (CCA).

The NCSC acquired additional power in 2018 with the introduction of the EUs NIS where it is providing advice and guidance to the Competent Authorities (CAs) that are responsible for security within specific sectors. This includes the Information Commissioner's Office (ICO) who are the CA for cloud providers and online services.

Bruce Schneier notes a similar battle for control of cyber within government agencies in the United States when he states that:

> "*There is a huge power struggle going on in government right now. Between the NSA, Homeland Security, the FBI over who gets control over the Internet and Internet security; and the NSA is winning, and they're winning by pushing this cyber-war fear. This fear of cyber armies attacking us. It's largely nonsense, it's largely hype, it doesn't hold up to scrutiny, but it's big and scary, and when people are scared they're much more willing to give up their liberties their privacy, their freedoms to someone who will make them feel safe.*" (Bruce Schneier quoted in Zerechak, 2012)

The same sort of battle appears to have taken place in the UK between the Cabinet Office, MI5 and GCHQ, with GCHQ the clear winner. The dominance of one agency in cyber security is not necessarily a healthy development, and the same concerns that are expressed

[39] However, it is worth noting that the MoD has continued to operate its own CSOC for military networks, and since 2016 the Home Office has been developing and expanding an independent CSOC for the Home Office estate and NHS Digital is also planning an independent CSOC.(NHS Digital, 2017)

in a US context may also be appropriate in the UK, especially when the NSA and GCHQ work so closely together. However, it could be argued that this consolidation in GCHQ may also be a sign of an improved focus and better coordination of cyber security issues within government especially given the previous criticisms of the NAO.

However, it is worth noting that any significant concerns with the role of the NCSC and its organisational placement within GCHQ have not been supported by data gathered from interviews conducted as part of this project. The majority of responses were either highly positive or neutral in that it is 'early days' for the NCSC at the moment. See Chapter 8 *Deductive Thematic Analysis of Practitioner* Interviews for a full analysis of interview responses on page 295.

This analysis of the securitisation speech acts in the UK using the Copenhagen School's securitisation framework has highlighted a number of aspects that are key to any analysis of the role of the UK state in cyber security. As a result we can postulate that:

1. A clear securitisation process has been at work since 2012, and that the engagement of specific securitising actors is not accidental. The speech act has been fundamental to the process of securitisation.
2. This process has been driven by the security services, and in particular GCHQ who have been at the forefront of the securitisation process.
3. The securitisation moves have in most cases equated cyber-threats with realspace referent objects, which serves to justify the state's greater authority in cyberspace.
4. At this point, states and criminals are constructed as more significant threat actors than terrorists in cyberspace.
5. There has not, to date, been a major cyber-attack that has significantly impacted the key referent objects (e.g. CNI, digital economy etc.).
6. There have been some key areas where securitising moves have been successful, including the introduction of the NCSC and the acceptance of the NCSC and GCHQ's role in the cyber security of non-government networks and systems.

7. The securitisation moves have only been partially successful, with the commercial sector still not delivering the cyber security capability baseline that is being demanded.

8. The process of securitisation can be expected to continue to address these areas, and the implementation of GDPR and NIS are both examples of an aggressive regulatory approach being adopted by the UK government (in line with the EU). This is potentially likely to continue with regulatory proposals now being considered for social media platforms.

9. The Copenhagen School approach represents a useful tool for the analysis of the construction of cyber security issues in the UK.

The result of the securitisation process has been a much more assertive cyber security approach from the UK government. At this time, this continues to be tempered by the continued need for partnership with private sector organisations, but regulatory initiatives may serve to reduce that dependency.

The way in which securitisation has been used by the UK state may also have implications for an understanding of securitisation theory. Securitisation through perlocutionary speech acts is a complex sequence of speech acts that are heavily dependent on political agency, context, and audience. Elements of individual speech acts change, depending on political agency and audience, especially in relation to the threat articulation and the referent objects.

7 Cyber Security as a Wicked Problem

The final element of the theoretical basis for this thesis is an understanding of cyber security as a wicked problem. This chapter describes how cyber security has the characteristics that indicate it can be considered a 'wicked problem'. It shows that the wicked problem concept represents an effective characterisation of the cyber security issue in the UK and a useful framework to use for the analysis of both the issues and the potential solutions associated with cyber security. A short summary of the characteristics of wicked problems provides context for an analysis of how the same characteristics can be seen in cyber security. This analysis is supported by a deductive thematic analysis of the practitioner interviews using the defined characteristics of wicked problems as coding for instances within the interviews. This coding was described in the Methodology Chapter in section 2.5 *Interviews* on page 52.

Building on the analysis of cyber security as a wicked problem, a number of case studies of wicked problems in unrelated areas are referenced to try and develop an understanding of the relative strengths of current policy approaches to cyber security in the UK. These case studies are drawn from the existing literature, particularly in relation to case studies of United Nations' (UN) interventions in Afghanistan (Roberts, 2000), global climate change (Levin *et al.*, 2009, 2012), Common Agricultural Policy (Termeer *et al.*, 2015) and Information Technology (DeGrace and Stahl, 1991; Denning, 2007).

In addition, an analysis of UK cyber security policy interventions shows that (in particular since the 2016 National Cyber Security Strategy (NCSS) and the introduction of the National Cyber Security Centre (NCSC) within GCHQ) these interventions have many of the key characteristics of approaches to wicked problems identified in the literature. This analysis shows there is evidence that UK cyber security responses may be being developed in line with an evaluation of cyber security as a wicked problem, although it has never been explicitly stated.

Finally, as part of this analysis, there are indications, based on the case-study literature, of where the current responses to cyber security may require adjustment

or enhancement to be successful, particularly emphasising the importance of developing genuinely collaborative solutions that engage the stakeholder community and respond effectively to the social complexity of cyber security.

The original 1973 definition of a wicked problem (Rittel and Webber, 1973) identified ten distinguishing characteristics.

1. That a wicked problem has no definitive formulation with *"…the information needed to understand the problem depends upon one's idea for solving it*" and that *"…every specification of the problem is a specification of the direction in which treatment is considered…*" (Rittel and Webber, 1973, p. 161)
2. That wicked problems have no stopping rule meaning there is no definitive solution that ends work on the problem and efforts only end when "….*he runs out of time, or money, or patience.*" The lack of a definitive rule to show that the problem has been solved means that there can be no end to the efforts to try and resolve it.
3. That solutions to wicked problems are not true or false, but are good or bad, so solutions to wicked problems are subjective and dependent on the interests and value-sets of stakeholders.
4. That there is no immediate and no ultimate test of a solution to a wicked problem as any solution will have consequences generated over a "*…virtually unbounded period of time…*" (Rittel and Webber, 1973, p. 163).
5. That every solution to a wicked problem is a "*one shot operation*" with no option for repetition due to the side-effects of every attempt to solve the problem.
6. That wicked problems do not have an exhaustive list of possible solutions and the limits to plans is based on judgement alone.
7. That every wicked problem is essentially unique and despite potentially having similarities with previous problems may contain an over-riding important unique element.
8. That every wicked problem can be considered a symptom of another problem in which the removal of the cause of a problem will identify another problem of which the original problem is a symptom.

9. That there are numerous explanations of the cause of a wicked problem and the choice of explanation is guided by attitudinal criteria.
10. That "*the planner has no right to be wrong*" when addressing a wicked problem. These are 'real world' problems and those addressing them are liable for the consequences of their actions.

Not enumerated as part of the ten distinguishing properties of wicked problems, but clearly identified as an issue for any possible resolution is the social context in which these wicked problems are addressed, in particular in that "*…different values are held by different groups of individuals – that which satisfies one may be abhorrent to another, that what comprises problem solution for one is problem-generation for another.*" (Rittel and Webber, 1973, p. 169) also constructed as the issue of "*…social complexity and the involvement of multiple actors involved in the formation, and potentially in the solution or the problem.*" (Peters, 2017)[40]

This chapter will show that cyber security can accurately (and usefully) be constructed as a wicked problem, displaying every characteristic from the original definition.

7.1 The Wicked Problem Characteristics of Cyber Security

There are dangers in applying wicked problem criteria to any complex problem, in particular due to a lack of coding guidelines and the temptation to 'stretch' the concept to fit any given problem (Peters, 2017). However, by evaluating cyber security issues against the ten characteristics of a wicked problem plus 'characteristic eleven' of social complexity, it is possible to make an informed judgment as to whether this is the case.[41]

The indications of cyber security being considered a wicked problem emerged from an initial review of the interview data which, then prompted a deductive thematic analysis of the interview data using the characteristics of a wicked problem as the

[40] For ease of reference I refer to social complexity as 'characteristic eleven'.

[41] A previous analysis of cyber security as a wicked problem used the reduced list of six criteria (Clemente, 2011) instead of the original ten.

codes for the identification of codeable events within the data. This process is more fully described in Chapter 2: Methodology on page 31. The codeable events from each interview are included in Appendix I.

What was noticeable during this analysis was that multiple of the characteristics of wicked problems can reference a single attribute of the cyber security environment as described in the interview data. For example, the statement by Participant A that changes to Industrial Control Systems are "*incremental and slow*" indicates both that wicked problems are essentially unique (characteristic seven) in the ICS issues are different to other computer systems, and that there is no stopping rule for solutions to wicked problems (characteristic two) in that the changes are incremental dependent in response to security issues with no defined stopping rule.

When conducting a thematic analysis, it is accepted that much of the coding is based on the coder's judgement, (Boyatzis, 1998) and where possible the judgment has been to try and assign any statement to just one wicked problem characteristic, except in a small number of situations where it was clearly applicable to multiple characteristics. The lack of accepted coding rules for wicked problems places more reliance on the judgment and integrity of the coder.

However, the thematic analysis of the interview data does show that multiple wicked problem themes occur within each of the interviews. The occurrence is not necessarily consistent across all interviews, with some participants having specific views that weighted the data from their interview towards individual characteristics of the problem, and some interviews had less to add across all the characteristics, but as the following analysis shows, there are multiple codeable events across all the interview transcripts.

Characteristic 1: There is no definitive formulation of a wicked problem

The lack of a definitive formulation is important for wicked problems as it indicates a concomitant lack of a 'stopping rule' and the need for solutions to be attempted in order to define the problem. It is impossible to definitively formulate the cyber security problem for a number of reasons. These include, the absence of universal

norms and international agreements for cyberspace, the nature of threats that are highly adaptive to any response that improves security; threat actors that are difficult to identify, in part due to the well documented issues of attribution, but also due to the way in which these actors adapt to a situation, for example, potentially working for themselves, for a non-state actor and a state, at the same time; the contested nature of the definition of an 'attack' (for example, whether pre-installing dormant malware is an 'attack' or whether it required malware to produce effects); the construction of cyber security as a defensive problem of software and patching levels, while potential vulnerabilities also include 'backdoors' incorporated into systems, procedural failures, attacks on the physical infrastructure, compromise by 'insiders' and other diverse issues.

The cyber environment is constantly changing, with the development of new systems and software that introduce new vulnerabilities and threats, (for example the massive DDoS attacks possible with the advent of IoT devices), the discovery of additional vulnerabilities in the existing environment, the availability of new exploits, and the introduction of new institutions and individuals into the cyber security environment. The definition of the cyber security problem is subject to constant change.

The characteristic that there is no definitive formulation of a wicked problem is shown in many of the interview statements relating to the number of different specifications of cyber security problems. This included statements such as "*attacks are both opportunistic and targeted*" (Participant A) showing different types of cyber attack and "*we will see the symptoms and indicators of compromise but we may not know what it is*" (Participant A) and "*The threat is always changing and adaptive*" (Participant B) and "*the threat picture does change*" (Participant E) and that it varies by organisation and industry (Participant B) showing that there are a variety of attacks that may occur. The lack of definitive formulation was also referenced in relation to the vulnerabilities within systems, for example "*we don't know whether a piece of software has a flaw in it*" (Participant C) and generically with reference to the fact that cyber security is a wide ranging issue with statements such as "*there is no one*

model" (Participant G) "*there is no one size fits all approach to cyber security*" (Participant B) and "*no one size fits all process*" (Participant D). It is noticeable that a wide range of threat variations were mentioned in the interviews along with a range of comments about the changing threat picture (Participants B, C, E, F, G), both of which suggest a multi-faceted problem lacking any definitive formulation. Coded interviews statements indicating that there is no specific formulation of the problem are shown in *Table 19 Interview statements coded as indicative of there being no definitive formulation of the cyber security problem* below.

Table 19 Interview statements coded as indicative of there being no definitive formulation of the cyber security problem

Interview	Text
Participant A	"attackers don't really care who it is they are attacking or whether it is out of malice, to make money, or to damage a country or industry"
	"attacks are both opportunistic and targeted"
	"we will see the symptoms and indicators of compromise, but we may not know what it is"
Participant B	"need to remain aware of the risks involved with extending the boundary"
	"[key threats] depends very much on the industry"
	"…systems such as NATS would be focused on availability. For other organisations focus will be on the security of customer data"
	"threat is always changing and very adaptive"
	"there is not a one size fits all approach to cyber security"
Participant C	"ransomware as a major future problem"
	"we don't know whether a piece of software has a flaw in it"
	"new threats are starting to materialise"
Participant D	"no one size fits all process"
	"worry at the moment is the hybrid nature of what is happening in Eastern Europe and Ukraine – high grade organised crime"
	"negligence will allow criminal activity to be perpetrated from your machine in a bot net"
	"lack of anti-virus and unpatched system or illegal copies of windows"

Table 19 Interview statements coded as indicative of there being no definitive formulation of the cyber security problem (continued)

Interview	Text
Participant E	"Threat picture does change"
	"Script kiddies are getting more sophisticated as the tools that can be taken off the internet are more sophisticated."
	"cyber is a human problem more than a technical problem"
Participant F	"outdated government systems and data architecture"
	"the Public Sector is a mess in some areas"
	"attacks becoming more targeted and less opportunistic"
	"there is no long-term government plan"
	"what we see as criminal gangs may be state agencies"
	"data leakage via social media is becoming a major issue"
Participant G	"Private sector focus has been that cyber security is a technical issue and the solutions must be technical. Changing in the last few years – security being more people centric"
	"people talk about AI when what they mean is machine learning or not even that"
	"all a bit of a muddle as to who takes responsibility for all the bits of cyber security"
	"there is no one model. Different threat actors have different motivations and different methodologies and different resource and targets therefore differ"
Participant H	"not every incident is the same"
	"no rules on where public ends and private begins"

Table 19 Interview statements coded as indicative of there being no definitive formulation of the cyber security problem (continued)

Interview	Text
Participant I	"Intelligence led defence will not deal with untargeted attacks"
	"Intelligence led models work well against campaign level attacks"
	"Top of the pool is constantly churning or moving around and threats are constantly changing"
	"Ransomware removed the time element from an attack"
	"When a new methodology comes along it may bypass more levels of controls or multiple layers simultaneously."
Participant J	"The bigger you are the easier it is for outside agents to infiltrate the company"
	"A management issue and not just a security issue."
	"won't make any difference as the consumer doesn't care if their IoT device has a security tested watermark. Until the consumer is forced to take responsibility for the home network then they are never going to care"
Participant L	"Private sector is based more on a risk assessment. State more concerns with intangible items such as political costs of attack on state institution."
Participant M	"Difficult to protect from every possible angle"
	"Not always a bad thing to have vulnerabilities that enable the state to be able to keep an eye on what is going on"

Characteristic 2: Wicked problems have no stopping rule

When there are no criteria that enable a definitive formulation of the problem and when the process of solving the problem is identical with the process of understanding its nature, there is no logical point the problem can be considered 'solved'. The changes in the environment and the unending causal chains mean that there is always the opportunity to do something slightly better. In cyber security there are new variants of malware, new threat vectors, new vulnerabilities being discovered, new systems being deployed that may have vulnerabilities within them and new technologies that enhance the capabilities of threat actors, all ensuring that the problem can never be solved.

The cyber security wicked problem characteristic of the problem having no stopping rule (as a result of there being no definitive solution) is again indicated by the thematic analysis of the interview data. This is particularly shown in statements regarding the never ending nature of the problem such as "*there is more that can be done, but the issue is how*" (Participant E) indicating that there are unknown possible future solutions that need to be applied, and that the "*key point about cyber is it is about the journey and not the destination*" again indicating that there is no definitive solution, but a never ending direction of travel. (Participant E). The idea of a process of constant change was also present in the interview from Participant A where he referred to ICS developments as "*changes are incremental and slow*". In terms of the threats and how they influence the ability to reach a stopping point, Participant B referred to "*IoT as just another example of an old problem of badly configured devices*" indicating that the introduction of new technology with old problems has, in this instance, prevented a stopping rule from being applied, and participant C echoed the threat issue when saying that "*we do not understand today what we will need to do tomorrow*" Participant I also referenced the threat development saying "*speed and automation...ransomware automatically sending bitcoin…then there is no effort*" as an indication that changes in threat technology would provide an impetus for more attacks in the future by making attack methodologies easier for threat actors. Participant D referenced the change in the

problem with reference both to the information sharing in that "*by the time you have written it down on a sharing platform it has probably changed*" and with reference to regulatory solutions with "*by the time regulation is in place, everything has changed*" both showing that there are no definitive solutions. The idea of no stopping rule was reinforced by participants indicating issues with returning problems that were thought to be solved (Participant F) and issues with no identifiable solution such as preventing the purchase of cheap insecure devices, and enforcing global regulation (Participant H).

Coded interviews statements indicating that there is no specific formulation of the problem are shown in *Table 20 Interview statements coded as indicative of there being no stopping rule for cyber security* above.

Table 20 Interview statements coded as indicative of there being no stopping rule for cyber security

Interview	Text
Participant A	"changes are incremental and slow"
Participant B	"has pushed the security boundary out to a point where the boundary is almost irrelevant"
	"worry about how the threat is going to change and who is next to come at the organisation"
	"IoT is just another example of an old problem of badly configured devices"
Participant C	"kill-switch and sand-box evasion techniques pre-used"
	"we do not understand today what we will need to do tomorrow"
	"it isn't like a car safety program where you can drive dummy cars into a wall"
Participant D	"an increasing challenge"
	"by the time you have written it down on a sharing platform it has probably changed at a tactical and operational level"
	"by the time regulation is in place, everything has changed"
Participant E	"if [a telecommunications] operator has mitigated risk then why should they change"
	"there is more that can be done but the issue is how"
	"key point about cyber is it is about the journey and not the destination"
Participant F	"Partnership seems to involve providing people and skills for free. Not clear what the upside is"
	"reactive rather than proactive"
	"seeing the same attacks coming back at some point"
	"many organisations are not aware of the scale of the problem they face"

Table 20 Interview statements coded as indicative of there being no stopping rule for cyber security (continued)

Interview	Text
Participant G	
Participant H	"…and then how do you stop people buying cheap devices on the Internet"
	"global regulation required – but how do you enforce that"
Participant I	"speed and automation...ransomware automatically sending bitcoin…then there is no effort"
Participant J	"Need to layer security"
	"It's an arms race between defence and attack and it always will be"
	"…everything is getting worse and at some point, it will be so insecure that it becomes secure. So tainted that nobody wants to use it and people won't connect to the internet."
Participant L	
Participant M	"systems connected everywhere are vulnerable everywhere"
	"Tit for tat hacking could be highly unproductive"

Characteristic 3: Solutions to wicked problems are not true-or-false, but good or bad

Cyber security has no true or false answers. There are always many parties who can judge the solutions and the judgement as to what is right and wrong will necessarily be subjective. As an example, the debate around password usage is one where there is no definitive answer. The relative weight given to considerations of ease of use, cost, password construction, strength of encryption, use of biometrics, (and associated ethical considerations), suitability of password managers, and other issues all serve to inform the discussion on how the 'password problem' should be addressed, and a number of alternative approaches are available as a result. All require some kind of trade off and all may be suitable in certain circumstances or for certain organisations or individuals.

This is one explanation for the number of alternative solutions to the problem that are presented. Continuing with the password example there is debate about whether passwords should be complex or simple, whether password reuse is allowable, or whether password managers are a good thing, whether they should be 8 characters long, or 10, or 16 or longer, should they mandate special characters, capital letters and numbers, whether copy and paste should be allowed for password entry, whether password reuse should be allowed and the like - and yet the permutation of answers to the password issue do not provide an answer that everyone can agree is 'right'.

The characteristic of solutions being good or bad rather than true or false was also judged to be present within the interview data. This is particularly the case with reference to the number of comparative statements such as "*security is not as good in cheaper products*" (Participant C) that indicate partial solutions or solutions that are providing the best possible option under the circumstances, such as "*it's an unwinnable war but we do our best to stop most of them*" or " *if you can cope with 90%...then doing better than most people*" or the idea of regulation as a "*balancing act and difficult to get right*" (participant J). The balancing act metaphor was also used by Participant L when referring to the trade-off between public security and cyber security in terms of state-hacking capabilities. The absence of a 'true or false'

solution was also indicated by the qualification of positive statements as being representative of progress rather than any sort of end point, for example talking about systems as being able to "*catch up with the threats*" (Participant A) or "*moving forward and being better*" (Participant E) and "*if you've done the basics like network segmentation then you massively reduce the risk of high-level impact*" (Participant J). It was also indicated as qualification in terms of solutions being imperfect, such as the explanation of routes for the monetisation of stolen data still being available even after dark markets were closed (Participant I) and the statement about the failure of market solutions for cyber security as "*in an ideal world that is how it would work*" (Participant H). This mix of partial progressive solutions and imperfect but best effort solutions shows that the judgment of solutions is very much on whether they are good or bad, rather than true or false.

Coded interview statements indicating that cyber security solutions are good or bad rather than true or false are shown in *Table 21 Interview statements coded as indicative of cyber security solutions being good or bad rather than true or false* below.

Table 21 Interview statements coded as indicative of cyber security solutions being good or bad rather than true or false

Interview	Text
Participant A	"we have developed strategies to enable systems to catch up with the threats"
	"other mechanisms as well in terms of security assessment processes"
	"if an assessment is felt to be unreasonable or lead to unnecessary demand"
Participant B	"agencies that provide best practice information but it make no difference unless there is funding available from the top"
	"Most will say that "CiSP is a good thing……something they will draw on rather than share with the government"
Participant C	"security is not as good in cheaper products"
Participant D	
Participant E	"moving forward and being better is the best way to defend"
Participant F	"Not sure whether being part of GCHQ is a help or hinderance to the NCSC"
Participant G	"need to engage the wider conversation and for it to be a two way conversation rather than just saying what people should do"
Participant H	"In an ideal world that is how it would work, but costs are externalised"
Participant I	"Still routes to sell data and different ways to monetise an exploited system [after closing dark markets]"
Participant J	"If you've done the basis like network segmentation then you massively reduce the risk of high-level impact"
	"It is an unwinnable war, but we do our best to stop most of them"
	If you can cope with 90% …… then doing better than most people.

Table 21 Interview statements coded as indicative of cyber security solutions being good or bad rather than true or false (continued)

Interview	Text
Participant L	"Balance between public security and cyber security – balance now for public security at cost of Info Sec with state hacking, surveillance capabilities etc."
Participant M	"Threat of regulation will induce self-regulation in some areas. Need to be careful about stifling innovation. Balancing act and difficult to get right."

Characteristic 4: There is no immediate and no ultimate test of a solution to a wicked problem.

Cyber security is a problem where any solution creates consequences which means that it is impossible to evaluate the relative success of a solution when it is implemented. For example, the success of signature-based anti-virus software created attackers to develop new skills in obfuscation and signature variation that prevented malware from being detected (Cobb, 2016; Kumar, 2017); education and awareness of emails from Finance Ministers needing to move millions of pounds offshore (the so called '419 scam') has created more sophisticated phishing techniques; and introducing additional security such as two-factor-authorisation (2FA) may in fact lead to more attackers (Fenton, 2013). While all of the above were 'solutions' to a problem, it may be difficult to identify whether any particular attempted solution was 'successful' or created more problems than it solved.

The wicked problem characteristic of there being no immediate test to a solution to a wicked problem because any solution would create ongoing consequences was also indicated in most interviews. Specific examples of changes that generated consequences were mentioned such as the introduction of the NCSC leading to less work being done with the Critical National Infrastructure than previously (Participant F), and that law enforcement actions can create insecurity in other areas (Participant L), in particular in that law enforcement agencies were focused on particular outcomes and "*if there is any collateral damage then just too bad*" (Participant A). Hacking back was also referred to as solution that would cause ongoing consequences, described as having the potential to "*create more chaos*" (Participant L) Particular successes, such as countering cyber-crime, were also seen as having created insecurities, for example in that cyber-criminals had "*diversified into state sponsorship*" (Participant E). This lack of a solution test leads to a level of uncertainty concerning the effectiveness of solutions that are proposed. This was indicated by statements such as "*the conclusion of the analysis is always debatable*" when discussing understanding attribution of attacks as to whether they are criminal or state in origin (Participant G) and "*good practice can always change*" showing the temporary nature of any solution. There were some statements

suggesting that aspects of solutions could have ongoing benefit, but when applied to new problems, for example Participant B suggested that organisations should "*look at what's there and already works*" and Participant J stated that "*learning from a first attack can prevent a greater impact form a subsequent and different vulnerability*". In these instances there is a potential positive benefit of the ongoing consequences of a solution.

Coded interviews statements indicating that cyber security solutions have no immediate solution test are shown in *Table 22 Interview statements coded as indicative of cyber security problems having no immediate solution test* below.

Table 22 Interview statements coded as indicative of cyber security problems having no immediate solution test

Interview	Text
Participant A	"ideas they would like to test with their customers for a security improvement possibility"
	"If there is any collateral damage then just too bad"
Participant B	"look at what's there and already works"
Participant C	"good practice can change"
Participant D	"as soon as the Shadow Broker was made public that authors of wannacry modified it to use a different exploit"
Participant E	"[cyber criminals] diversified into state sponsorship"
Participant F	"there is less work being done with CNI than before the NCSC"
Participant G	"Reliability of the conclusion of the analysis is also debatable"
Participant H	"Relying on consumer being aware of the security risk"
Participant I	
Participant J	"learning from a first attack can prevent a greater impact from a subsequent and different vulnerability"
Participant L	"[hacking back] will create more chaos"
	"law enforcement actions that can create insecurity in other areas"
Participant M	

Characteristic 5: Every solution to a wicked problem is a one shot operation.

Every attempt to resolve a wicked problem has consequences and "*…leaves 'traces' that cannot be undone.*" (Rittel and Webber, 1973, p. 163). This is very much the case in cyber security where attempts to fix security problems have an effect on the cyber security environment that results in consequences for security. If we take the example of the Microsoft patching process that issues fixes for software flaws on the first Tuesday of every month. This is known as 'Patch Tuesday". There are good reasons for issuing patches in this way in terms of managing system changes and allowing a controlled implementation of the patches on affected systems. However, every time a patch is made available in this way there are potential consequences. Issuing a patch for a problem immediately makes the details of the original problem publicly available and it becomes possible to more easily identify systems that have not yet installed that patch. There are good reasons why many organisations will not immediately install a patch, especially when they may have complex organisation specific systems that may be adversely affected by any software change.

However, in this case, the production of a solution for a cyber security problem (the original software flaw), has the consequence of creating a window of opportunity for the exploit of that flaw. As a result, Patch Tuesday is followed by what is known colloquially as "Exploit Wednesday" when malicious actors attempt to exploit the problems resolved the day before. The patches issued on Tuesday leave the 'trace' of the original issue being resolved allowing it to be used as an exploit mechanism. The solution to issuing security patches has, in effect, had the consequence of potentially creating a wider security issue.

Another example of this would be that of system passwords. There remain huge problems on many systems with insecure passwords being used such as 12345678, 00000000, ABCDEFGH and the like, as well as many simple passwords that can be found online in password dictionaries that can be used to try and break into systems by working through all the possible common passwords (known as a brute force attack).

The 'solution' to this has been to enforce complex passwords, for example by insisting on the use of capital letters, special characters and a mix of letters and numbers. This solution has created password management problems for users leading to passwords being re-used across multiple systems, simple password creation strategies being adopted (e.g. using a numeric zero instead of the letter 'o') and passwords being written down on pieces of paper (NCSC, 2016b). Solving the problem of simple passwords has, in effect, had the consequence of creating an insecure password environment.

The idea that wicked problem solutions have ongoing consequences as a result of there being no test of a solution, feeds directly into the idea that a potential solution is a 'one shot operation' due to the side-effects of every attempt to solve a problem. The analysis of the interview date showed that this was particularly the case in relation to technical solutions with Participant B stating that "*once they [hackers] have figured out what you are doing then they by-pass it*", and "*good hackers recognise when they are in a sand pit and how to defeat it*" showing that defensive solutions are susceptible to being overcome by experienced adversaries. Hacking back was also characterised by its potential for side effects with Participant I stating that it "*has the potential to get out of hand*" and Participant G stating that "*there can be a far more damaging chain of events initiated*" and that it could "*cause a lot of collateral damage*". The failure of technical solutions was also referenced in that "*more technology increases the threat landscape*" (Participant J), reference to "*the huge threat of blowback*" (Participant D) and that "*some devices have strong security settings but customers do not switch them on*" (Participant H) suggesting that implementing solutions can make the problem worse or introduce a false sense of security. The side effects of regulation were also referenced as something that "*could cause more problems than it solves*" (Participant B) and "*drifts into prescription*" (Participant C) suggesting that regulation may also have side effects that make it a one shot operation.

Coded interview statements indicating that cyber security solutions are one shot operations are shown in *Table 23 Interview statements coded as indicative of cyber security solutions being a one-shot operation* below.

Table 23 Interview statements coded as indicative of cyber security solutions being a one-shot operation

Interview	Text
Participant A	"one breach of trust and all this collapses"
Participant B	"yes it [regulation] could help, but it could cause more problems than it solves"
	"Once they have figured out what you are doing then they by-pass it"
	"good hackers recognise when they are in a sand pit and how to defeat it"
Participant C	"potential for side effects is huge"
	"regulation drifts into prescription"
	"…people do things whether they are appropriate or not and people drive down cost by doing as little as possible.
Participant D	"huge threat of blowback with state research being used"
Participant E	"the psychology of a fast moving and prepared to fail attitude"
Participant F	"private sector push back from first NCSC initiative may have changed approach"
Participant G	"If you hack back on incomplete evidence and are wrong then there can be a far more damaging chain of events initiated"
	"[Hacking back] is a fundamentally flawed idea that could cause of lot of collateral damage"
Participant H	"Some devices have strong security settings, but customers do not switch them on. Tomorrow's threats will come from the connected devices."
Participant I	"[hacking back] has the potential to get out of hand but could also be very useful"
Participant J	"it has not prevented any further breaches because everyone is worried about the latest thing"
	"More technology increases the threat landscape"

Table 23 Interview statements coded as indicative of cyber security solutions being a one-shot operation (continued)

Interview	Text
Participant L	"State environment potentially damaging cyber security – needs elected officials to understand the implications of the intelligence agencies hanging on to zero days"
	"DDOS C2 computers are probably not the perpetrator's computers so hack them and you are really hacking someone else"
Participant M	

Characteristic 6: Wicked problems do not have an enumerable set of potential solutions

In the case of a wicked problem without pre-defined stopping rules that enable a 'right or wrong' answer it is impossible to ever say whether all possible solutions have been tried. This means it becomes a matter of judgement as to how many and which solutions should be attempted. When every solution has consequences and uncovers consequential problems, it is inevitable that the number of solutions is innumerable. This may be one cause of the growth in the global cyber security market which (as previously referenced in *Chapter 3 Background: Cyber Threats and Vulnerabilities*) is anticipated to grow in value to more than $300 billion per annum in 2024. This growth is indicative of a continued need to address ever more cyber security problems on a wider scale.

The wicked problem characteristic that there is not an exhaustive list of potential solutions was also present in the interviews, in particular in that there were a large number of solutions identified through the interviews, showing the variety of solutions available, but also in that there were indications that the solution landscape was one of continuing change and development.

The wide range of solutions offered by participants ranged from regulatory interventions to building a new Internet. This was supported by statements describing the need to understand different risks for different elements of the business and understanding different business models (Participant B), cyber now being "*a part of all conversations with customers*" (Participant F); lists of possible security controls and approaches (Participant A and Participant D) and the statement that "*what targets can do to defend themselves is also varied*" (Participant G). The constant change was evident in statements such as "*flexibility and innovation is also emerging*" (Participant E) and "*it's an arms race*" (Participant B). Coded interview statements indicating that there is no limit to possible cyber security solutions are shown in *Table 24 Interview statements coded as indicative of there being no limit to possible solutions* below.

Table 24 Interview statements coded as indicative of there being no limit to possible solutions

Interview	Text
Participant A	"ideas they would like to test with their customers for a security improvement possibility"
	"stronger controls are put in place such as air gaps, controlled remote access, firewalls, and the like"
Participant B	"have to look at risk in context...understanding risk for each element of the business"
	"down to organisations to understand their own business model and understand use cases where things apply"
	"it's an arms' race"
Participant C	"Possible false flag and false attribution situation"
	"Microsoft produced the vulnerability which the NSA discovered and did not choose to tell anyone"
Participant D	"difference between active defence and hacking back (macho crap) – but a trace back and forensics is fine."
Participant E	"know where your critical data, systems and technology is. Know your own systems and do simple things well."
	"change to making security enable your business"
	"flexibility and innovation is also emerging"
	"bringing good tools to the marketplace that would not have been thought of"
	"if it is malicious traffic that impacts service then they should stop it and that is a core part of the service"
Participant F	"cyber is now a part of all conversations with customers"
Participant G	"…talking about hacking back. But also look at defences – mitigate risk – look ahead"
	"how to disrupt, delay and confuse any attackers"
	"what targets can do to defend themselves is also varied"

Table 24 Interview statements coded as indicative of there being no limit to possible solutions (continued)

Interview	Text
Participant H	"Difficult decision as to where to put the regulatory intervention"
	"could require cyber security in annual audit, but relying on GDPR as a driver for making companies take cyber more seriously"
Participant I	
Participant J	"No good trying to defend against the latest NSA zero-days - patching should have been done before hand"
	"but the same idea in China is forced on people rather than being given as a tool to use."
	"…the Internet as we know it will never be secure so what we need to do is create another Internet from the ground up with built in security"
Participant L	
Participant M	

Characteristic 7: Every wicked problem is essentially unique

I would argue that every instance of an organisation (or a country) trying to secure its own little corner of cyberspace is essentially unique. Social context, people, culture, processes, legal and regulatory environment, enemies, friends, systems environment all serve to create a completely different problem in every instance. In the search for cyber security solutions this means it may be unwise to try and take (for example) what works in the USA and apply it in the UK environment. The problems are unique, and the solutions will need to be unique as well. This is the case in particular with software environments, where different products configurations and patching levels serve to create multiple unique environments, and so, unique problems.

The long list of possible approaches and solutions shown in the interview data for characteristic six also contributes to the argument that cyber security exhibits the seventh wicked problem characteristic of being essentially unique. Judgements regarding codeable events in both characteristic six and seven could have been interchangeable. In the interviews, this unique nature was emphasised in terms of specific attributes about certain systems (Participant A, Participant F) or unique approaches to cyber security, both between industries but also within organisations (Participant B), as well as the different motivations and capabilities of different attackers (Participant E, Participant F) showing that individual attack methodologies all represent unique challenges. Important within this example was the view that private sector organisations could not compete with the unique challenge of state level attacks (Participant F, Participant J). The unique nature of the problem was shown in terms of the target systems, the risk assessments of the target organisations, the motivations of attackers, and the capabilities of both attackers and defenders. Coded interview statements indicating the unique nature of cyber security problems are shown in *Table 25 Interview statements coded as indicative of every wicked problem being essentially unique* below.

Table 25 Interview statements coded as indicative of every wicked problem being essentially unique

Interview	Text
Participant A	"ICS systems have a very long life and changes are incremental and slow"
Participant B	"even within organisations the concerns are different"
	"if the cyber security capability is configured for the wrong type of attack then that is a problem"
Participant C	"if it is a critical industry then it needs to be a community led activity but otherwise it is up to the organisation"
Participant D	
Participant E	"cannot compete with the technology that the state will deploy"
Participant F	"there are malicious actors who just want to destroy things"
	"difficult for private sector to defend against state level capabilities"
	"legacy systems are particularly difficult to identify all vulnerabilities"
Participant G	"…organisation may not know enough about the attack for it to be possible to act on that kind of varied model"
Participant H	"sectors working with NCSC – retail cyber toolkit"
Participant I	
Participant J	"No company can defend against a government sponsored state attacker"
Participant L	
Participant M	"Traditional methods of protection don't apply and something different is needed"

Characteristic 8: Every wicked problem can be considered to be a symptom of another problem

Almost any cyber security problem can be evidence of the existence of another problem. The existence of a software vulnerability may be a symptom of poor installation practices in a single implementation, which may in turn be a symptom of software complexity in an individual product, which may in turn be a symptom of poor coding in a department, which may in turn be a symptom of poor training and education across the industry, and so on. Choosing the right level at which to address the problem is complex in itself, with too high a level making the problem vague and more difficult to deal with, and too low a level not providing any guarantee of a change in the situation.

The thematic analysis of the practitioner interview data showed that some of the attributes listed within characteristics six and seven also add weight to the eighth characteristic that cyber security problems can be considered a symptom of another problem. This was further emphasised by statements that showed the way in which one cyber security issue can lead to another. For example, when talking about the ability of zero-day to move laterally, the problem of "*a lack of diversity in client operating systems*" was cited (Participant A), or references to attacks becoming more sophisticated due to the issue of tools being available on the Internet, (Participant E) or major attacks being due to the problem of unreported vulnerabilities (Participant D). Areas where there were policy disconnects also featured in this issue with examples where neither policy makers or technicians fully appreciated the issues (Participant L) or where there was a logical conflict such as the desire to ban encryption while also making the UK the safest place to work online, or people having valuable information but not sharing it because it was valuable (Participant I). There were also issues that indicated that problems were a symptom of a lack of understanding, for example, hacking back (Participant L), encryption (Participant G), not understanding the need to 'do the basics' (Participant J) or an ill-informed press and senior management (Participant A). Participant M provided a useful summary of the multi-layered symptoms of cyber security problems when they referred to "*Human error. People losing passwords, being members of Ashley Madison –*

catastrophic mistakes and consequences create a chain of events – virtualised data systems that provide access to everything – systems connected everywhere are vulnerable everywhere."

Coded interview statements indicating that cyber security problems can be considered to be a symptom of another problem are shown in *Table 26 Interview statements coded as indicative of every wicked problem being a symptom of another problem* below.

Table 26 Interview statements coded as indicative of every wicked problem being a symptom of another problem

Interview	Text
Participant A	"…we are aware of weaknesses such as a lack of diversity in client operating systems"
Participant B	"ill-informed press cause problems in dealing with senior management fall-out"
Participant C	
Participant D	"world would not have had wannacry if US had not spent large amounts of money in finding vulnerabilities and not reporting them"
Participant E	"script kiddies getting more sophisticated as tools off the internet become more sophisticated"
Participant F	"concern over proliferation, blowback and control"
Participant G	"nobody providing guidance, and nobody knows who should"
	"ridiculous statements [about encryption] shows a lack of understanding. Row over encryption causes a disconnect"
	"How can government want to make the UK the safest place to do business and talk about banning encryption at the same time?"
Participant H	"Massive skills problem, inflated wages…government see best people being poached"
Participant I	"Lot of people have valuable information, but as it is valuable it is not being shared"
Participant J	"Biggest risk is not doing the basics and people still don't understand that"
	"you are likely to be breached so you need to know what the response to the breach will be"
Participant L	"Hacking back is a good example. Policy makers don't know what issues it can create – techies looking at it are keen on it but don't know what problems they can cause."
Participant M	"People losing passwords, being members of Ashley Madison – catastrophic mistakes and consequences create a chain of events – virtualised data systems that provide access to everything – systems connected everywhere are vulnerable everywhere"

Characteristic 9: The existence of a discrepancy representing a wicked problem can be explained in numerous ways. The choice of explanation determines the nature of the problem's resolution

The range of symptom and problem possibilities in cyber security allows the problem to be constructed in many different ways. How the problem is described determines the nature of the proposed solution. The subjective nature of this process means that at any point in time both the nature of the problem and the potential solutions are contested. For example, there are many alternative explanations for why software vulnerabilities exist, which could include anything from vulnerability-hoarding by government agencies, through to deliberate installation by a software vendor, through inadequate testing processes, through a lack of patching and so on. Starting from the problem of software vulnerabilities it is possible to identify numerous possible causes, all of which are potentially valid, all of which may require resolution, and all of which will require a different solution and all of which will create different consequences which in turn will create new problems and demand new solutions.

The characteristic that every wicked problem has multiple explanations as to its cause is again indicated by the interview data. This is, in part, shown by the wide variety of underlying causes that were offered during the interviews, ranging from human error (Participant M), the underlying system architecture (Participant J), difficulties in identifying the perpetrators of specific attacks (Participant F, Participant G), and many specific technical issues relating to insecure protocols and anonymity (Participant E), supply chain issues (Participant C), maintenance and patching (Participant A, Participant D) and resources and focus (Participant A, Participant G, Participant H).

Coded interview statements indicating that cyber security problems can have numerous explanations are shown in *Table 27 Interview statements coded as indicative of every wicked problem having numerous explanations as to its cause* below.

Table 27 Interview statements coded as indicative of every wicked problem having numerous explanations as to its cause

Interview	Text
Participant A	"…malice, to make money, or to damage a country or an industry. Not bothered about who they are attacking as long as they are making money or getting what they want."
	"patching is a much slower cycle"
	"we don't have the time or expertise"
	"difficult to get fraudulent domains shut down...too easy to set up a fraudulent domain"
	"lack of diversity in client operating system"
Participant B	"needs recognition from the top that this is a business issue and not just a technical plumbing issue"
Participant C	"if you choose the cheapest thing you have to accept there are compromises"
	"it is about ethical purchasing rather than an ethical requirement on a supplier"
Participant D	"lack of anti-virus and unpatched system or illegal copies of windows"
Participant E	"[criminals] have a high level of anonymity that allows them to be fast moving"
	"SS7 is an inherently insecure protocol and needs changing. But it needs to be paid for"
Participant F	"difficult to distinguish war and crime"
Participant G	"Attacks that look as if they are criminal attacks may be a state"
	"A lot of being successful in cyber security comes down to having the right mindset"
Participant H	"Lot of companies are quite complacent"
Participant I	

Table 27 Interview statements coded as indicative of every wicked problem having numerous explanations as to its cause (continued)

Interview	Text
Participant J	"The bigger you are the easier it is for outside agents to infiltrate the company"
	"Reactive nature is just a lack of understanding"
	"issues related to the basic architecture of the system"
Participant L	
Participant M	"…sleeper type threat is almost undetectable until you understand normal behaviour…"
	"Human error. People losing passwords, being members of Ashley Madison – catastrophic mistakes and consequences create a chain of events – virtualised data systems that provide access to everything – systems connected everywhere are vulnerable everywhere."

Characteristic 10: The planner has no right to be wrong

The original articulation of the wicked problem concept was in the context of policy planning with the 'planner' as the person who generates actions in response to the wicked problem. For cyber security in an organisation this could read 'the CISO has no right to be wrong' or in the case of the UK government response to cyber security even 'the NCSC has no right to be wrong', the point being, that addressing wicked problems is not an academic search for truth; it is about addressing 'real world' issues and improving the situation inherent in the wicked problem. The planner/CISO/NCSC must be cognisant of the potential consequences of any action taken and take responsibility for the results.
The difficulty of the role undertaken by those responsible for cyber security was often referenced in the interviews, in particular with respect to the balance that has to be achieved in relation to decisions and the consequences of wrong decisions. Some of the comments reflected frustration at those who were not getting things right, for example Participant B stated that "*the business model is what matters and none of the vendors understand that*". This was supported by Participant C who stated that there was a need to "*understand the real risks and what the problems are we need to fix*" and Participant B who called or a focus on simple things like getting a decent firewall and patching. Participant F was particularly critical of Government actions in terms of the NCSC role definition, the amount of funding, and the lack of a long-term plan. Participant A identified issues in balancing the amount of security in terms of ease of use and decisions that need to be made regarding where the line between security and function is drawn.

Coded interview statements indicating that the planner has no right to be wrong are shown in *Table 28 Interview statements coded as indicative of the planner having no right to be wrong* below.

Table 28 Interview statements coded as indicative of the planner having no right to be wrong

Interview	Text
Participant A	"you have to be sure you can trust the people you are dealing with"
	"one breach of trust and all this collapses"
	"desk access to social media and webmail is one example of where it would make sense to block it, but that may be a step too far"
	"we have to walk a line between enough controls to stop the bad guys and enough leeway [for staff] to do their jobs"
Participant B	"The business model is what matters and none of the vendors understand this sufficiently"
Participant C	"understand the real risks and what the problems are we need to fix"
Participant D	"People need to focus on doing some of the simple things – patching and getting a decent firewall."
Participant E	
Participant F	"NCSC is struggling for a role"
	"There is not enough money to set up a proper agency"
	"Government is not getting to grips with cyber"
	"there is no long term government plan"
Participant G	"Potentially attacking innocent bystanders"
Participant H	"How can government change that thinking?"
Participant I	

Table 28 Interview statements coded as indicative of the planner having no right to be wrong (continued)

Interview	Text
Participant J	"If you think technology can solve the problem then you don't understand technology and you don't understand the problem."
	"If you think one box or software produce from a vendor will fix the underlying issues with a network is wrong – you are probably just installing another vulnerable device."
	"Almost certainly a lack of knowledge. A lot of people are not security minded. Do not understand that they need to know about security."
Participant L	
Participant M	"Believe mediated data – believe instruments and tools above own senses."
	"problems with companies driving understanding with marketing dollars to drive sales"

Characteristic 11: Social complexity adds a further level of difficulty to wicked problems

Cyber security is a pluralistic environment to which many significantly differentiated actors contribute. Private security providers, software developers, operators of critical national infrastructure, the military and military contractors, intelligence agencies, law enforcement, individual users, netizens, civil society organisations, and governments all have a potentially different view as to what cyber security is and have different demands as to what they expect from it. The globalised cyberspace environment then multiplies those views many times depending on local cultural and political norms.

This strongly reflects the situation described for policy planners in 1973, in that:

> *"…diverse values are held by different groups of individuals – that what satisfies one may be abhorrent to another, that what comprises problem solution for one is problem generation for another. Under such circumstances, and in the absence of an overriding social theory or an overriding social ethic there is no gainsaying which group is right and which should have its ends served."* (Rittel and Webber, 1973, p. 169).

It could be argued that anybody working in cyber security would recognise this, perhaps most obviously in the realms of privacy, civil liberties, and the needs of national security with respect to cyberspace, where the requirements of the security services such as encryption back-doors, vulnerability hoards and mass data collection would be considered abhorrent by other communities in cyberspace.

The practitioner interviews provided a particularly rich source of data indicating the social complexity of cyber security. There is an emphasis on community approaches to cyber security involving government, security vendors and user organisations (Participant A, B, C, E, G, I, J, L M) but within that community approach the complexity was often seen as a hinderance in areas such as the

potential for collaboration to be construed as anti-competitive behaviour (Participant A) or where different members of the community have different objectives (Participant C, Participant D) or where relationships were unclear such as between public and private sector (Participant B, Participant C, Participant F), or levels of trust were insufficient to enable collaborative approaches (Participant I, Participant H).

Coded interview statements indicating social complexity are shown in *Table 29 Interview statements coded as indicative of the social complexity of cyber security* below.

Table 29 Interview statements coded as indicative of the social complexity of cyber security

Interview	Text
Participant A	"it can be a very sensitive issue speaking to a competitor especially when it can be construed as an anti-competitive activity"
	"there are introductions that can be made to bring the right people together"
	"critical infrastructure groups and invited vendors to be able to understand their patching strategies and future development plans"
Participant B	"what is best for the organisation and its customers and other stakeholders"
	"organisational and industry differences determine where the boundary for cyber security is"
	"where the boundary is, depends on to what extent the other stakeholders play a part in the security system"
Participant C	"if it is acritical industry then it is a community activity"
	"there isn't a consistent private sector and it depends on philosophy as to where the public sector and private sector begin and end"
	"partner with organisations like BT, partner around the world with different specialisations bringing complementary solutions"
	"different agencies and states have different objectives and end-games"
	"difficult to take action due to a myriad of different agreements and different laws"
Participant D	"different levels of collaboration at practitioner, commercial, national and international levels"
Participant E	"in some aspects of cyber, community is everything"
	"bigger players in cyber have a responsibility to drive the market"

Table 29 Interview statements coded as indicative of the social complexity of cyber security (continued)

Interview	Text
Participant F	"Too many different departments, DCMS, Cabinet Office"
	"Not sure whether being part of GCHQ is a help or hinderance to the NCSC"
	"difficult to distinguish public and private – infrastructure and responsibility"
Participant G	"[NCSC] has been a really positive influence. They have reached out to the community"
	"events engaging academia and industry"
	"Depends on which part of the government and which part of the cyber security industry. Some are more privacy focused than others."
Participant H	"Cyber Growth Partnership modelled on other industry government partnerships…been through several iterations"
	"Revolving door between industry and government which shared skills and insights"
	"some companies have had difficulties working with GCHQ as an organisation"
Participant I	"Useful [networks] are those that have a high level of trust – typically quite closed networks where you know everyone in the room."
	"Some do not want to share as it can give away that they are not as good as they should be."
Participant J	"All security like this is shared. You cannot have government, business, or individuals solely responsible"
Participant L	"Definitely collaborative. Inter-sectoral. State, private sector and civil society. Skills shortage driving development of public private partnerships. Threat information sharing, specific schemes to exchange staff between state and private sector. Private public cooperation essential"
Participant M	"…a level of social pressure and a normalisation of behaviours and social community"
	"Issue with other countries not conforming"

7.2 Addressing Wicked Problems

Evaluating these 'ten plus one' issues in the context of cyber security alongside the thematic analysis of the interview data would seem to indicate that it can reasonably be considered a 'wicked problem'. If we accept that this is the case, then it has clear implications for how the problem of cyber security should be addressed. Case study literature concerning how issues have been identified as wicked problems and then addressed as such, identifies the different possible approaches that have been taken, along with important elements to be considered as part of any strategy designed to address wicked problems.

Nancy Roberts identifies three distinct strategies that can be adopted to address wicked problems, designated as authoritative, competitive and (Roberts, 2000). The first of these are *authoritative* strategies These are described as 'taming strategies' (i.e. strategies designed to tame the problem to become something more manageable) where the issues associated with wicked problems are reduced by putting problem solving into the hands of a limited number of stakeholders who have the authority to define the problem and come up with a solution.

While there are advantages to this approach in terms of problem solving being quicker and less contentious with fewer stakeholders, and an expectation that reliance on experts can make the whole process more professional, the approach also has significant disadvantages. Roberts documents five specific disadvantages; authorities and experts can be wrong about both the problem and the solution; experts tend to seek solutions within their own narrow horizons; the limited engagement of a wider community of stakeholders can limit both the options for solutions and the opportunity for new knowledge to be created; where an authoritative strategy attempts to tame a wicked problem through the process of consolidating power, and reducing the extent to which the solution and the problem definition are contested, it may create the very belief systems and power relationships that ensure its continuation; and, where the problems are truly wicked with no one in control, then an authoritative strategy will only temporarily tame the

problem and may in fact have a long-term negative influence on the problem-solving process.

From her analysis of UN efforts in Afghanistan, Roberts cautions against turning wicked problems over to groups of experts or some other authoritative power for definition and solution, as a wicked problem is one over which nobody has control and the experts are unlikely to be able to act unilaterally to define the problem or the solution, and may in fact hinder any problem resolution through their actions (Roberts, 2000, p. 16).

Peter Denning adds the caution that a never-ending wicked problem can become a comfortable environment for those who benefit from the existence of the problem, especially when it is embedded in social systems (Denning, 2009). These are described as the 'mess-dwellers' who inhabit the existing belief system that has failed to resolve the wicked problem and "*only a belief changing innovation*" will be able to change the situation, and therefore "*…many in the mess feel threatened about the prospect of a solution*" as this disruptive change will potentially undermine their beliefs and change existing power relationships in which the mess-dwellers are vested. Rittel and Webber observed that there were no value-free solutions to wicked problems, which suggests that entrusting decision making to professional experts and politicians would not necessarily improve the resulting outcomes.

Secondly, *competitive* strategies rely on competition to spur the search for solutions. Where there is no clear problem or solution definition, competitive strategies may be appropriate to ensure that no single path is followed, resulting in more opportunity for one of the competitors to achieve a solution. This is in direct contrast to a resource conscious authoritative strategy where the costs associated with multiple solutions may not be seen as appropriate.

Finally, *collaborative* strategies are described by Roberts as perhaps the most difficult approach to wicked problems. Reasons for this are considered to be the increased costs of engaging multiple diverse stakeholders, despite a reduced cost per stakeholder (Australian Public Service Commission, 2007, p. 10), and the limited availability of collaborative skills, especially in traditional bureaucracies with a

strong hierarchical culture and management system. However, there are arguments on either side as to whether collaboration or centralisation represents the most effective strategy (Daviter, 2017).

In terms of when a collaborative approach will be considered, it is claimed by Roberts that "*...people have to fail into collaboration…*" (Roberts, 2000, p. 12) and it is only when other approaches have failed that they are willing to take on the extra effort and cost involved in a collaborative approach.

At the core of the collaborative approach is a win-win view of problem solving (Roberts, 2000, p. 6) and an understanding that a collaborative approach brings together fragmented knowledge from a wide range of stakeholders and ensures the legitimacy of any solution through the development of a sense of common purpose and shared ownership (Daviter, 2017, p. 574). Collaborative solutions are supported by much of the literature on wicked problems, although also acknowledged to be the most difficult to implement.

An unconnected, but useful case study analysis of Common Agricultural Policy reforms as a wicked problem (Termeer *et al.*, 2015) also emphasises the need for collaborative approaches to wicked problems. This is based on the need for any approach to wicked problems to engage different ways of thinking and overcome a tendency for wicked problem solutions to focus on 'action' strategies to the exclusion of observation and enabling activity.

This analysis identified the need for four key governance capabilities of "*reflexivity, resilience, responsiveness and revitalisation*" that are required to respond to characteristics of wicked problems. This included the variety of possible framings of the problem (reflexivity), the ability to adjust actions to uncertain changes (resilience), being able to change agendas and expectation (responsiveness) and the capability to overcome and unblock stagnation (revitalisation).

The requirement to evaluate wicked problems through different lenses and the organisational demands of these four capabilities suggests that one theory or approach will be insufficient to deal with wicked problems and *"…the inherent variety of wicked problems requires actors to have a commensurately large variety of*

observing, acting and enabling repertoires to come to terms with them." (Termeer *et al.*, 2015, p. 21)

In a separate study, Falk Daviter identifies three strategies of 'taming' coping' and 'solving' (Daviter, 2017) in a study that claims these three alternatives are empirically distinguishable as approaches to wicked problems. This study also identified an emphasis on finding solutions to wicked problems which, as wicked problems are unresolvable is "*…in stark contrast to the widely shared notion that solving wicked problems is not a viable option…*" (Daviter, 2017, p. 574). This observation suggests that although wicked problems cannot be solved (due to the absence of a 'stopping rule)', it is important that those responsible 'try anyhow'. Although attempts to resolve wicked problems may in themselves have unintended consequences and could prove to be counter-productive there is no option to 'do nothing'.

Given the contradictory nature of possible methods for solving wicked problems (authoritative, competitive, collaborative) and an understanding of their ineffectiveness in actually solving a wicked problem it is possible that the strategy of 'taming' a wicked problem may be seen as the only practical way forward.

A taming strategy tries to redefine the problem in such a way as to enable it to appear as if some solution has been found by transforming a wicked problem into a series of simpler problems more suitable to being solved. By hiving off components of the problem rather than attempting to solve the (unsolvable) wicked problem, a taming approach aims to reduce and control it, typically by aligning it with existing expertise and policy responsibilities, thus leading back to an authoritative approach based on giving authority to experts to define and resolve a problem (Daviter, 2017).

This may have some advantages in terms of reducing the costs involved in resolving at least elements of a wicked problem. By simplifying the problem, it can ensure the focus moves to finding a resolution rather than constantly framing and re-framing the problem, but taming is fundamentally an authoritative approach with the same inherent problems.

Giving power to existing experts may leave solutions in the hands of those who are comfortable in the 'mess' and ensure a continuation of unsuccessful paradigms. This may have the effect of limiting identified solutions and having a negative effect on the understanding of the overall problem by reducing possibilities for social learning and problem reflexivity and encouraging tunnel vision on the part of the expert community. (Termeer, Dewulf and Breeman, 2013). Actions taken to resolve an element of the problem may have consequences that will not be understood and may aggravate problem interdependencies.

As a result of the limitations of taming strategy solutions, a taming strategy has been described as morally wrong in that it:

"*…tames the growl of the wicked problem: the wicked problem no longer shows its teeth before it bites. Such a remark naturally hints at deception: the taming of the growl may deceive the innocent into believing that the wicked problem is completely tamed. Deception becomes an especially strong moral issue when one deceives people into thinking that something is safe when it is highly dangerous. The moral principle is this: whoever attempts to tame a part of a wicked problem, but not the whole, is morally wrong.*" (Churchman, 1967)

An alternative to the taming strategy is 'coping' in which "*….fragmented policy responses and the division of policy responsibility are not seen as inherently detrimental….*" (Daviter, 2017, p. 580) especially when there is no holistic alternative approach. Coping strategies do not necessarily depend on centralisation and authoritative hierarchical control and suggest a wide range of partial solutions that are anticipated to improve the overall situation, but which require a focus on quickly detecting and correcting any interventions that produce negative results.

Coping strategies offer an alternative to taming where there is an acceptance that the wicked problem cannot be 'solved' but instead represent a process aiming for continual improvement or "*progressive incremental change*"(Levin *et al.*, 2009) which triggers path-dependent processes in such a way that *"...small policy changes can have significant transformational effects…*" (Levin *et al.*, 2012, p. 125) which will instil characteristics of durability and expansion in any intervention.

The case-study analysis of the wicked problem of climate change (Levin *et al.*, 2012) indicated a need for any intervention in a wicked problem to have three key characteristics of *stickiness*, *durability* (or *entrenchment*) and *expansion* in order to be successful. Stickiness, ensures that actions to address wicked problems actually take some initial effect on a target population; durability means that this effect is not short lived but can be sustained in order to see some benefit, and expansion means that the intervention delivers benefits in such a way that it extends its reach to new targets.

However, actions that create stickiness and entrenchment may give early adopters a vested interest in preventing expansion. For example, any 'approved supplier' type arrangement that creates a competitive advantage through being approved creates an immediate incentive for those with approval to limit entry to a club that provides this benefit. This would encourage entrenchment at the expense of expansion. Alternatively, it is possible that policy interventions that encourage expansion may result in a loss of support from the initial beneficiaries, so undoing the stickiness and entrenchment achievements. This would be the case if the expansion of an approved supplier scheme reduced the benefit to existing members sufficiently to create a disincentive to continued membership, or if, a new scheme diverted focus and finance away from an existing scheme in such a way as to make it unattractive to existing members.

Proposals to avoid this include addressing 'stickiness' by taking advantage of existing institutions and using any windows of opportunity where the balance of benefits and costs is changed in favour of policy adoption; secondly, by delaying or offsetting the cost of participation and thirdly by utilising areas where indirect policy interventions can initiate further developments.

The danger of entrenchment being encouraged at the expense of expansion points to the importance of the development of collaborations and shared values. It is suggested that collaborations emerging from a policy intervention may be more effective than the intervention itself as they may start a continuing sequence of events by developing positive feedback loops, increasing returns and self-

reinforcing processes (Levin *et al.*, 2012, p. 141) while also ensuring that technical standards and regulation do not create barriers to long-term expansion. Values and norms are an additional self-reinforcing process that develop acceptance and legitimisation of actions while providing a normative basis for influencing future behaviour.

There are also possible specific strategies for expansion to create new interests in line with a solution. This includes education and training in specific skill sets to create a community vested in the solutions and utilising government procurement policies to influence technology adoption by using government purchasing power to create a market large enough to influence wider market adoption.

7.3 Addressing UK Cyber Security as a Wicked Problem

The qualitative data gathered from semi-structured interviews conducted as part of this project indicate that cyber security has the characteristics of a wicked problem in particular in relation to the complexity of the environment, the ongoing escalatory nature of cyber security issues constructed as a cyber-arms race, the changing nature of the environment and the failure of authoritative approaches such as regulation. Full details are included in *Chapter 8 Deductive Thematic Analysis of Practitioner* Interviews on page 295.

The wicked problem literature suggests that there are number of elements to be considered in any approach to a wicked problem. Firstly the structural nature of the approach in terms of it being collaborative, competitive or authoritative; secondly, the strategic approach to the problem in terms of taming, coping, or solving, and for specific interventions the characteristics of stickiness, endurance and expansion, the encouragement of positive feedback loops, increasing returns and self-reinforcing solutions (including the development of values and norms) and the development of the key capabilities of reflexivity, resilience, responsiveness and revitalisation.

If we accept that cyber security is a wicked problem, then on the basis of the wide case study literature it would be reasonable to expect to see these strategies being considered (either by accident or design) as part of the policy response to issues of

cyber security, and on the basis of the existing analysis of the challenges faced by specific approaches to wicked problems, to then be able to judge the potential for success offered by current cyber security policy initiatives. Effectively, it is possible to reverse engineer the policy responses and certain initiatives to uncover the wicked problem strategies that are being adopted and evaluate where weaknesses may exist.

UK policy for cyber security, as outlined in the 2016 National Cyber Security Strategy (NCSS) (HMG, 2016), is focused around the National Cyber Security Centre (NCSC) which was formed as part of GCHQ incorporating a number of pre-existing government cyber security elements including the CPNI, CERT-UK, CiSP, and CESG. The NCSC represents a quite explicitly authoritative approach (in wicked problem terms) to cyber security, establishing a single authoritative institution to address the problem. The introduction to the NCSS even describes the NCSC as "*…the authority on the UK's cyber security environment, sharing knowledge, addressing systemic vulnerabilities and providing leadership on key national cyber security issues.*" (HMG, 2016, p. 10) and adds that the NCSC is intended to be "*…an authoritative voice and centre of expertise on cyber security...*" (HMG, 2016, p. 28).

An emphasis on the technical expertise and authority of the NCSC is a key component of many of the government statements regarding cyber security. These frequently emphasise the NCSC and GCHQ as being the experts in cyber security, for example with references to "*...the deep expertise of GCHQ…*" (Martin, 2017b), "*…GCHQ's world class expertise…*" (Hancock, 2017), "*…[GCHQ's] secret world class expertise...*" (Osborne, 2015) and references to the NCSC technical director as "*…an expert of global standing..*" (Martin, 2016b).

This expert status of GCHQ and the NCSC is reinforced by criticism of the expertise, competence, and motivations of other organisations. For example, it was reported that the NCSC had accused the whole cyber security industry of scare-mongering in order to sell their solutions describing cyber security as an arena where "*…the narrative is set by a massively misincentivized set of people*" (NCSC's Ian Levy quoted in Lomas, 2016b). While, this was perhaps an inevitable element of the

process of a new organisation establishing its authority within a competitive environment, and there may be a positive argument for resetting the narrative of a wicked problem, there is something slightly ironic about an organisation that espouses the benefits of their "*secret sauce*" (Levy, 2016b) eschewing industry's "*magic amulets*" (NCSC's Ian Levy quoted in Lomas, 2016b).

The introduction of the NCSC seems to indicate that a taming approach has been taken to cyber security. This is firstly in terms of its authoritative nature, with the delegation of responsibility to technical experts, and second in terms of some of the initial activities which have tried to segment the problem into more addressable components, such as address spoofing of government email systems and password management.

Almost inevitably with an authoritative approach being undertaken by technical experts, the key programmes have been oriented towards action rather than observation or enablement. The description of the main programmes as *Active* Cyber Defence defines the action-oriented nature of the approach, which is then born out in the specific programmes such as DMARC implementation, and proposals to 'fix' the core telecommunications switching protocol of SS7 and the internet Border Gateway Protocol (BGP). This seems indicative of the type of action-oriented leadership that the NCSC is trying to provide.

However, in terms of dealing with wicked problems it is possible that the 'solution hero' approach is not what is required. There is a view that when dealing with wicked problems, the job of the leader is not to devise the solution but to "*…build and sustain trust around the table*" (Dr Kate Isaacs quoted in Manville, 2016) as part of a much more collaborative approach that builds quick wins that in turn encourage entrenchment and expansion.

There are a range of problems with taming as a strategy for cyber security. For example, if solutions are developed that address one set of vulnerabilities or one attack vector (for example DMARC on government domains) it will not solve the problem of email spoofing. It may provide some protection to one set of addresses

but could be expected to cause attackers to search for other high value domains that are susceptible to the same type of spoofing attack.

When the prevalent cyber-attack methodology is one of untargeted attack based on a malicious actor with an exploit searching for systems that are susceptible, rather than developing an exploit to target a specific installation (NCSC, 2015; Schneier, 2015, pp. 166–167; Barysevich, 2016), taming one element of the cyber security wicked problem by securing one a particular installation will almost inevitably have consequences for other systems as malicious actors seek out those installations that remain vulnerable. Any partial solution deployed as part of a taming strategy would need to be developed with an understanding of the potential consequences.[42]

The issue of unexpected consequences resulting from taming approaches adds to the complexities inherent in GCHQ's engagement as the authority addressing cyber security. Actions taken in relation to GCHQ's national security responsibilities or CESG's Government Information Assurance responsibilities may have unknown and unintended consequences across UK cyberspace. For example, the hoarding of vulnerabilities leaves systems exposed to other attackers by not disclosing the vulnerability to the manufacturer so that a patch can be developed (Smith, 2017), and the development of exploits for state use carries with it the danger that these exploits are re-used, as was seen in the case of Stuxnet with malware variants such as Duqu, Flame and Gauss being described as 'cousins' of Stuxnet (Bencsáth *et al.*, 2012) and the use of the NSA's Eternal Blue in the Wannacry attack of May 2017 (CERT-EU, 2017).

There are many cyber security examples where solutions cause problems in other areas. For example the previously mentioned patching development and

[42] It should be noted that although this may seem intuitively to be correct, there is no guarantee that introducing a solution on one system should necessarily displace attacks to unsecured systems. Research into the effect of burglar alarms did not reveal a displacement of crime from alarmed to unalarmed homes, but instead showed that the installation of alarms "diffused benefit onto neighbouring unalarmed homes." (Hakim, Rengert and Shachmurove, 2000) Further research is required to understand if this same counter-intuitive result occurs in relation to cyber security.

distribution process where the very act of creating a solution creates another problem. This is one of the defining characteristics of wicked problems. The same can be seen in the 'bug bounty' system in which security researchers are paid for discovering vulnerabilities in systems and services, but as part of which it is possible that legitimate bug bounty activity may act as camouflage or a distraction for malicious hacking to take place. Again, the solution can create the very problem it is trying to resolve (Jackson Higgins, 2016).

This would seem particularly relevant in a cyber security environment where partial solutions offer no security to many stakeholders and can potentially increase insecurity for others while deceiving them into believing that cyberspace is safe when it remains a highly dangerous environment. It is important for the NCSC to take an honest approach to any taming solutions and ensure the benefits are not over sold, particularly in relation to the global nature of cyber threats.

Other key activities undertaken as part of the UK's NCSS has included supporting education programmes through a degree certification scheme and the appointment of academic centres of excellence in cyber security research who also make up the centres for doctoral training in cyber security. By mid-2017, the NCSC had certified twenty-five Master's degree courses and two Bachelor's courses from nineteen universities (NCSC, 2017f) and had engaged with thirteen universities through three research institutes and fourteen universities as academic centres of excellence. This small number of engaged institutions providing certified courses may be an indicator of a desire to encourage initial entrenchment over expansion. This may reflect an incremental approach to expansion, with public calls for additional institutions in late 2017 (NCSC, 2017f).

The strategy of NCSC certification is also being used as validation of cyber security products and professional services and training courses. However, as of December 2017 only 135 cyber security software and hardware products appear on the certification list (NCSC, 2017a) which has a number of major companies conspicuous by their absence including the main anti-virus providers and major information technology and cloud service providers.

The same approach is being used with government suppliers through the 'Cyber Essentials' scheme which certifies a basic level of cyber hygiene and is now mandatory for all suppliers on certain types of government contracts, and forms the basis of the MoD's Defence Cyber Procurement Partnership (DCPP). Using government purchasing power in this way to encourage changes in behaviour creates immediate economic benefits to those who adopt the scheme, and so provides the immediate stickiness needed for wicked problems, and may initiate further path dependent processes, for example by instigating further supply chain integrity.

However, expansion of cyber security solutions may be proving to be more of an issue. Speaking in November 2017 Director of the NCSC Ciaran Martin said

> "*….the second thing we've done is look really hard at things like economics and behavioural science and try to figure out this perplexing conundrum - given people are aware of cyber security and the threat, and there is money to invest, why aren't those simple defences being improved to the extent they need to be?*" (Martin, 2017c)

The NCSC's 2017 Annual Report (NCSC, 2017e) indicated a new focus on 'Economy and Society' to widen their engagement with the voluntary sector, small businesses and educational institutions.

A staged and sectorised approach such as this, again reflects a taming approach to the problem in that the problem of cyber security is being approached by sector, in order to try and reduce it to manageable levels. This does of course appear highly pragmatic in an environment where resources and skills are constrained, but fixing the issue for one area does not necessarily contribute effectively to a wider solution and as with all taming solutions may have unexpected negative consequences.

The key issue in reaching out to these new areas will be to achieve the level of 'stickiness' that is needed to ensure that any initiatives are successful in the longer term and themselves provide the beginnings of a path for entrenchment and expansion. However, the British Retail Consortium (BRC) Cyber Security Toolkit, which was cited as an example of a sector based initiative, represents little more

than the re-packaging of existing advice into a single 44 page PDF document, and may be more a reflection of a need for retailers to navigate a confusing plethora of schemes rather than any genuinely new thinking (BRC, 2018).

There are indications that the taming solutions may be driven by thinking based on the CESG and CPNI heritage of the NCSC with a focus on government systems and CNI providers (and to some extent commercial cloud providers as they are used by government departments). Again, it is possible to argue this on pragmatic grounds of effective prioritisation, but this approach will once again carry with it the problems associated with a taming approach to a wicked problem.

There are other indications that the approach to the wicked problem of cyber security has at times been limited by the authoritative nature of the UK solution. This has shown itself in an apparent lack of understanding and consideration of the commercial environment in cyberspace, as shown by the initial approach to BGP and SS7 security issues, which, while valid issues, were presented with a "we can fix this, it's easy" attitude by GCHQ, while the industry saw it as a much more complex issue that required collaboration on an international basis in particular as any solution was seen as just displacing the problem to other countries (McGoogan, 2016) .

Even the UK Government's DMARC implementation, which has been successful in almost eliminating phishing emails pretending to be from HMRC is struggling to expand beyond organisations that are particularly at risk of email spoofing because "*very few organisations care*". (Tucker, 2017) [43]

DMARC may in some ways lack the attributes required to encourage expansion beyond the initial population, especially if organisations cannot see the benefits that accrued to HMRC as being applicable to their own organisation as well. Partly, this may be caused by the fact that the victim of phishing is most often seen as the

[43] This view is supported by a review of DNS records for the FTSE 100 undertaken as part of this project in March 2019 which showed that less than had had a DMARC record on their DNS entry.

receiver of a spoofed email rather than the organisation whose email is being spoofed.

There is an expectation that organisations and individuals should protect themselves from phishing rather than that the organisation whose email address is being misused should protect them. DMARC deployment has only been successful with organisations where direct benefit seems to accrue especially in the finance industry where customers may lose financially and pharmaceuticals where phishing (or 'pharming' as it was known) was a prime mechanism for selling counterfeit pharmaceutical products (Agari, 2017).

Again, it may be that a more genuinely collaborative approach is required to ensure the expansion of DMARC adoption, for example by persuading large organisations to insist on it being deployed by their suppliers as a part of a supply chain security strategy, and the taming approach of partitioning the problem may be proving counter-productive in terms of driving the expansion of DMARC. While it is part of the NCSC's strategy to use government departments as case studies for cyber security solutions to sell the benefits more widely, and HMRC is a reasonable example of a government case study, with HMRC having been good ambassadors for the success of their DMARC implementation with good press coverage (Perez, 2017), the example of a huge government department may not resonate with (for example) a mid-sized retail organisation.

Case studies that are available from the NCSC all reflect government or quasi-government organisations. There will be a good case for seeking out and developing sector specific case studies with influential organisations within key sectors, with a focus on making clear the benefits of DMARC, even if the NCSC had not been involved in their deployment.

Within the public sector this seems to be the thinking behind the Secure by Default programme (NCSC, 2017g) which is looking to provide funding and support for the implementation of a range of technologies that will then allow case studies to be produced. This again, as part of the strategy of trialling solutions within

government seems to be aimed only at the public sector, and may not have the wider impact that is required.

In terms of collaborative approaches to cyber security, the Cyber Security Information Sharing Partnership (CiSP) seems to be the most successful element for the NCSC with a 43% increase in visits listed in the NCSC 2017 annual review (NCSC, 2017e), alongside a 43% increase in corporate members and a 60% increase in individual members, showing at least a level of engagement that would suggest it was a valuable vehicle for collaboration. However, CiSP can still be criticised for not engaging with everyone in the cyber security industry due to restrictive membership rules and procedures (NCSC, 2017d). This is not a positive attribute in the context of a response to a wicked problem as it is preventing expansion of the solution and denying benefits to a segment of the population, while potentially creating a vested interest in exclusivity among existing members (Levin *et al.*, 2012, p. 136).

CiSP is one element of a range of collaborative initiatives. Across law enforcement the NCSC is, for example, working closely with the NCA, with NCA officers embedded in incident management teams. A joint GCHQ and NCA operations cell to address online child sexual exploitation was announced in 2015 (National Crime Agency, 2015) and a joint NCA and NCSC cyber-crime threat assessment was produced in 2017 (National Crime Agency, 2017a).

The NCSC has also formed the "Industry 100" scheme which provides places for up to 100 staff from the private sector to work on secondment within the NCSC, which is intended to ensure the NCSC "*can achieve a greater understanding of the cyber security environment using wide and diverse thinking*." (NCSC, 2017h) This particular approach would seem to be strongly supported by the wicked problem literature as a mechanism for overcoming the danger of tunnel vision and the beginning of trying to "*get the whole system into the room*" which is recommended by the literature (Roberts, 2000; Manville, 2016).

However, there are three underlying issues that may impact private sector collaboration with the NCSC as part of GCHQ.

The first is the question of trust, which was highlighted by a number of this project's interview participants. This is, in part, due to activities made public by the Snowden revelations such as the GCHQ cyber-operation against Belgacom (R. Gallagher, 2014), which may affect a willingness to work collaboratively on the part of other organisations, and incidents which were described as using industry collaboration to increased surveillance capability (Dr Steven Murdoch quoted in McGoogan, 2016).

Secondly, there is the issue of recent state regulation, in particular GDPR and NIS which have large fines attached to non-compliance, which is being introduced alongside an increasing expectation that the private sector will take on the costs and responsibilities involved in meeting state objectives, such as content filtering by online service providers.

Thirdly, there is the issue of understanding the different environment of the private sector world. This is especially the case where there is a disparity between the requirements of national security and the commercial operations of private sector organisations. Examples include the use of Huawei equipment in the UK telecoms network, the mediation of content by online service providers, and the requirements for access by security agencies to encrypted communications.

However, it should be recognised that the need for collaboration with the private sector has long been acknowledged in the National Cyber Security Strategy of the UK. It can be argued that the 2010 National Cyber Security Strategy gave a significantly larger share of the responsibilities to the private sector and the authoritative approach of the NCSC in the 2016 NCSS is only a recognition of the failure of the private sector to respond to the challenge, which has necessitated a much more interventionist approach by government.

In summary, cyber security appears to have all the characteristics of a wicked problem although there is little literature or analysis available that directly addresses cyber security as a wicked problem in any depth. However, case studies based on wicked problems as diverse as global climate change, trade policy, food

standards, post-conflict reconstruction and others, seem to offer useful direction for addressing cyber security as a wicked problem.

There is no direct evidence that UK cyber security is being treated as a wicked problem to an extent that is driving the design of the Government's response, or that the issues involved in addressing wicked problems have been considered as part of the UK approach. Reverse engineering some of the UK activity and evaluating it in the context of cyber security being a wicked problem has indicated areas where the UK response may experience difficulties in addressing cyber security as a wicked problem.

In particular, the allocation of responsibility to a national government agency, staffed by experts, to address cyber security indicates an authoritative approach to cyber security, which then suggests a taming strategy is being adopted by aligning the solution with existing institutions with expertise, and allocating responsibilities to these existing actors. Many of the resulting initiatives that have emerged from the NCSC also reflect this taming strategy, by dealing with components of the problem and attempting to tame the problem by segmenting it into smaller and more manageable sections, either by vulnerability, industry sector, or attack vector. This process compartmentalises problems in such a way as to enable action to be taken. If cyber security is truly a wicked problem this may prove to be the worst possible thing to have done, not only pragmatically by potentially creating bigger problems, but also morally, by deceiving people into believing that the wicked problem is being 'fixed'.

There is a strong literature that suggests the need for collaboration in resolving wicked problems (Roberts, 2000; Denning, 2007, 2009; Grint, 2010) but also indicates a number of inhibitors that may prevent effective collaboration in particular when wicked problems have become integrated into the social systems. Cyber security today is a large and complex social system encompassing corporations, civil libertarians, intelligence agencies, hardware and software manufacturers, a thriving consultant industry and a large population of experts, commentators and

academics. This may well be indicative of Peter Denning's "mess" and would suggest the need for disruptive change to overcome these inhibitors.

There are a number of NCSC statements and initiatives that could be interpreted as being an attempt to provide a transformational element to the mess, including revising traditional password guidance, a new focus on the role of people as a security strength rather than the weakest link and the BGP and SS7 proposals, but it is also the case that the status and power of the NCSC is dependent on the continued existence of the mess and this in itself may already be a disincentive to any resolution.

A collaborative approach is often seen as being a last resort after both authoritative and competitive approaches, with a need to "*fail into collaboration*" (Roberts, 2000; Denning, 2009). Although there are elements of UK cyber security that seem to be developing a more collaborative approach such as CiSP and Industry 100 schemes, they also have serious limitations in the extent of the engagement they offer.

However, the key issue with the UK Government's approach may emerge as the leadership that is offered. While, there is a need for leadership, and that leadership role has been placed on the NCSC, wicked problems require a style of leadership that may not sit easily with an organisation whose background is rooted in civil service management and intelligence agency secrecy. Wicked problems require a particular style of leadership, based on reflection and engagement, and the ability to 'bring the whole system to the table' in a collaborative manner. The type of leadership that may be appropriate for a tame or critical problem where a command or management form of authority may be effective is not what is required for wicked problems. Ironically, this may in fact drive problems not to be constructed as wicked problems, as the 'solution hero' driving effective and efficient problem resolution can be a more attractive role for the expert than that of a collaborative leader whose expertise is in bringing people together rather than finding a solution.

In wicked problem resolution there may be no place for the "*solution hero*" (Manville, 2016) or the heroics associated with decisive action (Roberts, 2000; Grint, 2010). This will necessarily limit the problem solving contribution of any expert.

Wicked problems are not "*vehicles for ego massages*" (Grint, 2010, p. 11) and typical taming approaches may be counter-productive when a more collaborative leadership style is required (Grint, 2010).

There is some evidence that there has been a change in tone from the NCSC since its inception. Statements by the NCSC became very focused on the actions the NCSC were going to take, and, I would suggest, symptomatic of an approach based on the heroics of decisive action. For example, the NCSC's flagship Active Cyber Defence (ACD) programme (in particular referred to the NCSC plans to "*fix the underlying infrastructure*" and "*drive the UK software ecosystem to be better*" (Levy, 2016b) and some reported statements were anything but collaborative in tone (Lomas, 2016b).

The tone of public statements has become much more collaborative over the life of the NCSC, with Jeremy Fleming (appointed Director GCHQ in 2017) stating in August 2018 "….*we need to work even harder with businesses, technology companies, academia and privacy groups to protect the public from real-world and online harm*." (GCHQ, 2018a). This built on statements at Cyber-UK 2018 when he said that *"...relations with industry, academia and other parts of the public sector are growing as we invest time and effort. Programmes like the NCSC's Industry 100 scheme are good for all sides. And we're looking for other ideas and ways to build these partnerships further*." (Fleming, 2018b). The outgoing Head of GCHQ (Robert Hannigan) was reported as saying that "*…the intelligence community has to build bridges with the tech industry because only together can they tackle the problems of crime and terrorism on the internet*" (Reeve, 2017). This is despite having previously been a critic of the private sector, accusing them of aiding and abetting terrorism by refusing to cooperate with the intelligence agencies, and blaming Edward Snowden for poisoning the relationship between Government and the private technology companies (Reeve, 2017).

This change in tone may suggest that a more collaborative approach will act as the basis for future actions, which, in the context of cyber security as a wicked problem should be a positive development.

8 Deductive Thematic Analysis of Practitioner Interviews

A deductive thematic analysis of the interview data (as described in *Chapter 2 Methodology*) showed that seven key themes emerged. Many of these themes were present in multiple answers to multiple questions, so were often a consistent theme within a single interview as well as being a common theme across multiple interviews. These themes are:

1. The complexity of the cyber security environment.
2. The failure of the market to address cyber security and the potential need for regulation as a result
3. The limitations on the role and capabilities of the private sector
4. The need for collaboration and the difficulties inherent in collaborative approaches
5. The difficulties in working with government and state agencies
6. The changing and adaptive nature of the cyber security environment
7. The need for better education and understanding

The coding of the interviews in relation to these seven themes is included as Appendix H. This is in addition to the inductive analysis of the interview data that indicated that cyber security could be described as a 'Wicked Problem' whichh has been fully described in *7.1 The Wicked Problem Characteristics of Cyber Security*.

The specific themes from the deductive analysis are further explored in the following sections.

8.1 Theme One: Complexity of the Cyber Security Environment

One of the most commonly referenced issues to emerge across the answers to several of the interview questions was the complexity of the cyber security environment. This was evidenced in several different ways.

Firstly, every organisation is potentially subject to different threats, meaning there is no single identifiable construction of the threat environment or the relative importance of specific threats within the threat environment. It is different for every organisation and potentially different in relation to different elements of the same organisation.

Secondly, complexity of the environment is evident in the information technology infrastructure that is being secured which was described as having "*changing network boundaries*", "*more numerous end-points*" and including "*personal devices with dubious security controls.*" (Participant A), leading to the potential for an incomplete awareness and understanding of the information technology estate and the need for different strategies to secure different types of system. This was particularly the case in relation to ICS/SCADA systems that operate with much longer patching cycles and were seen as representing a "soft underbelly" in some organisations as they were never intended to be connected to the Internet. There was a common reference to the fact that security 'needs to be designed into the system' or embedded within a network architecture, and an acknowledgment that many of the cyber security issues are due to historical decisions that did not embed security within the system.

Concerns about the difficulties of defending the information technology infrastructure were also present when the infrastructure was homogenous (especially in terms of the operating system), as this provided greater opportunity for lateral movement of exploits. An obvious potential solution to the complexity of the environment is to restrict the technological diversity of the system environment, but this in fact only serves to create what is perceived as potentially greater problems inherent to a homogenous system environment.

Concern regarding the social complexity of cyber security was also present in many of the interviews. This included references to the different levels at which collaboration took place, including practitioner, commercial, national, international, governmental and law enforcement, (Participant C) in particular in terms of the range of commercial and legal constraints that inhibited collaboration, such as concerns over anti-competitive practices (Participant A). There was concern expressed about the different objectives of some organisations and specific reference to how working with law enforcement in particular had resulted in negative consequences for individuals and organisations. The "*…velocity, volume, and value of data*" meant that "*the sharing concepts do not work any more…*" and there is "*just too much information for one organisation or one sharing platform to process.*" (Participant D)

The social complexity was also described as changing dependent on the level at which organisations were engaged with one another. Threat investigation was seen as being

highly collaborative, but "*…once you get beyond that level then different agencies and states have different objectives and end games*". (Participant C) There were also suggestion that the success of collaboration was dependant on the organisational levels that were engaged. At a practitioner level collaborative actions were seen as delivering value, but that anything further was inhibited by commercial considerations and legal constraints such as concern over security collaboration being interpreted as an anti-competitive practice. (Participant A)

The multi-faceted nature of the cyber security problem, the specificity of networks and information infrastructure, and the complexity of the social environment defines a need for multiple solutions dependant on the mix of elements of any particular implementation or threat, and there is no 'one size fits all' solution available. This has led to a large number of disparate sharing platforms, security frameworks and collaborative groups all trying to address similar problems. An example that indicates the specificity required is that the European Central Bank (ECB) devised individualised cyber incident reporting requirements for each of 121 banks (Pinsent Masons, 2017).

This type of complexity and specificity is typical of the wicked problem characteristic of there not being any definitive formulation of a wicked problem.

8.2 Theme Two: Market Failure & Regulation

The failure of the market to deliver cyber security solutions was a common theme that emerged in response to questions relating to the capabilities of the private sector, the roles of cyber security solution vendors and communications service providers.

There were specific references to the inadequacy of the take-down process where Internet Service Providers remove fraudulent domains and the ease with which fraudulent domains can be registered and put to criminal use.

In part, the issues were presented as a symptom of the failure of cyber security to be considered as a business issue rather than purely a technical issue, leading to approaches that did not adequately consider the business risks presented by a problem. This same view was articulated several times in relation to cyber security vendors who were described as "*not understanding the nuances of the business models*" (Participant B) and trying to sell "*a technical solution to a technical problem*" (Participant G), and containing a "*snake oil element to*

it" (Participant D), echoing the criticism from the NCSC of the cyber security marketplace selling "*magic amulets*" (Levy, 2016b). There is recognition of a conflict between commercial pressures driving cyber security implementations, both in that internal corporate security controls are limited by the fact that "*people have to do their job*" (Participant A) and so have to have access to potentially insecure or compromised external systems (including personal email and social media) as well as access to corporate systems from personal devices (so called BYOD) that may not have the same security or software controls as a corporate device.

Commercial issues were also present in purchasing decisions which may be taken on the basis of price point, with the potential for security compromises to be made as a result. The UK telecoms industry's deployment of Huawei equipment can be seen as such on a national basis where the Huawei decision seems to have been based on a significant cost differential against other suppliers, and the government's decision not to mandate a change of supplier was based on the potential liability for the cost differential.

There was a view that there was a lack of market drivers for security, especially with reference to IoT devices. This was also reflected in comments about the need for greater education of the general population and the level of market maturity that was required for consumers to understand risk sufficiently to make a purchasing decision that places security ahead of price.

References to the failure in the market echo the thoughts of Robert Hannigan (at the time Director of GCHQ) when he said in 2015

"*But standards are not yet as high as they need to be. Take up of the schemes is not as high as it should be. So something is not quite right here. The global cyber security market is not developing as it needs to: demand is patchy and it is not yet generating supply. That much is clear.*" (Hannigan, 2015)

The emphasis on the need for the private sector cyber security market to improve has continued to be a focus, with Ciaran Martin asking a CBI audience in 2017 "*Why haven't normal market forces taken care of more of the problem?*" (Martin, 2017b) The view that the market is failing does not seem to have changed in the intervening years, and was one of the

considerations in the development of GDPR and NIS, as well as the more assertive NCSS of 2016.

The change in approach to cyber security in the 2016 NCSS indicated that the perceived failure of the 2011 Cyber Security Strategy was rooted in the assumption that the role of the state would be to encourage security to be delivered by the private sector. Two key environmental changes have taken place since then which have forced that assumption to change. The first is that cyberspace (and the Internet in particular) has become a fundamental part of the UK economy and society, from online shopping to the delivery of government services, which has made cyber security an issue of national security. The second is that private commercial organisations are seen as having been unable to deliver the type of security in cyberspace that is required for national security. However, there is also an acceptance that cyber security cannot be provided solely by government institutions. As a result, a number of different strategies are being adopted, including:

1. Continued programmes to encourage and educate such as *Cyber-essentials*.
2. Use of government purchasing power to spread security through their supplier base.
3. Government systems security as a proof of concept and an exemplar for commercial adoption such as has been seen with DMARC initiative with HMRC.
4. National level actions being enforced by the UK government such as BGP and SS7 changes that are seen as delivering a security benefit across the whole of UK cyberspace.
5. The development and promotion of standards for cyber security (over and above accepted standards such as ISO2001) such as 'secure by design'.
6. Regulatory approaches where necessary such as GDPR and NIS.
7. International governmental cooperation to extend national approaches internationally in response to the transnational nature of many cyber vulnerabilities and threats.

This wide range of strategies to approach a problem is again also an indicator of a wicked problem in that wicked problems do not have an enumerable set of potential solutions.

8.3 Theme Three: The Limitations on the Role of the Private Sector

One of the issues consistently raised regarding cyber security relates to where the boundaries are between state and private sector responsibilities. This is particularly the case with regard to private organisations in industries that provide components of the Critical National Infrastructure, where there is a national security implication to their security (HMG, 2016) or where they are part of the privately owned communications infrastructure that is fundamental to the technological underpinning of cyberspace and have a role to play in delivering against national security requirements in cyberspace, for example, ISPs supporting take-down requests and implementing DNS filtering on behalf of the state.

Much of the interview data supported the notion of the lack of clarity around the boundaries between state and private sector in cyber security with it being described as "*all a bit of a muddle*" (Participant G) and different norms being applied to CNI organisations from other areas of the private sector, with a clear expectation of increased state-level engagement with CNI organisations.

Participants within CNI organisations were clear that they remained responsible for their own cyber security. There was no expectation that as part of the CNI, the state would be providing security on their behalf, but there was an expectation that the state would be engaged in ensuring that private organisations were providing adequate levels of security through guidelines, assessments and other process controls. At this level, engagement with state agencies was described as normally being "*mature and sensible*" and "*working well*" (Participant A).

In contrast there was unanimous clarity on the subject of the limits of private sector action in terms of active cyber defence and offensive cyber techniques (so-called 'hacking back'). Here, a mix of both pragmatism and principle was evident in opposition to private sector organisations being able to 'hack back' against adversaries in response to an attack. Conceptually hacking back was described as "*macho crap*" (Participant D), "*fundamentally flawed*" (Participant G), and even "*the stupidest thing that humanity has ever thought of*" (Participant J). It was stated that it was wrong to "*make the victim of a crime responsible for addressing the wider issues just because they were a victim*." (Participant D). Identification of

attackers, investigation and any consequential activity was seen as firmly in the hands of state authorities.

The principle of hacking back was dismissed because of the complexities and the potential for catastrophic mistakes and escalation. Specific references were made to the potential for an organisation to incorrectly attribute an attack that had been routed through multiple compromised systems that could belong to medical or other critical systems resulting in any 'hack back' appearing to be an unprovoked attack on critical systems. The example of the potential for a multi-national organisation to be put in a position where it was hacking its own systems in another country was also offered as an indication of the difficulties involved in any hacking back strategy.

Hacking back was also dismissed on practical grounds in that most private organisations did not want to be engaged in illegal activity and that internal cyber security departments had neither the interest, the capabilities nor the resources to consider any offensive action, stating that "*once an attack is over we lose interest in it, apart from looking at what lessons can be learned.*" (Participant A)

There were indications of a desire to use more 'active defence' capabilities in terms of sink-holing and DNS redirection alongside technical deception measures such as tar pits and honey pots to enable analysis of attacks. There was disagreement on where the boundaries were for non-destructive action of this type with some participants suggesting that 'trace back' to the attackers system was an acceptable action for a private organisation, while others suggested that any action at all should be confined within their own network boundaries.

There was again almost universal agreement on a preference to hand-over any post-attack actions to state authorities for a state level response either through law enforcement or other state agencies such as the NCSC. There was also agreement on the need for wide collaboration in this area in order to share threat and attack information.

In relation to state-level attacks, participants believed that there was little that the private sector could do to protect themselves from a targeted state-level attack. This was explicitly

distinguished form the majority of untargeted attacks for which the general view was that 'doing simple things well' and 'basic cyber hygiene' would be sufficient protection.

However, there was a view from one of the larger organisations within the Communications Service Provider (CSP) industry that the larger organisations had a wider role to play, both in providing leadership within the industry and providing mechanisms that would enable smaller (and less capable) organisations to defend themselves from attack. Conceptually, this was supported by the example of Microsoft automatic security updates ensuring that patching was up to date for small users which can be seen as Microsoft protecting organisations from the dangers of unpatched systems.

The input provided by participants in this area seems to reflect an acceptance of the status quo in cyberspace based on the transference of realspace norms and legal restrictions to cyberspace. The role of the state in private organisations delivering CNI is accepted especially in managing compliance (effectively mirroring state realspace roles in health and safety, anti-competitive behaviour etc.) and reflecting the position of the CNI as a component of national security.

Realspace norms are also reflected in the limitations on the private sector in terms of restrictions on offensive action and an assumption that any post attack action is handed off to state agencies. This is despite an apparent lack of confidence in their capabilities.

There are both positive and negative aspects to this. On the positive side, there are further indications of an understanding of the need for private sector and state collaboration in the provision of cyber security as well as an acceptance of the need to conform to legal constraints even within the 'wild west' of cyberspace. However, there may be a concern that these realspace norms are not appropriate in a cyberspace environment where anonymity and deception are common. Several participants explicitly referenced the lack of capability (and resources) in law enforcement and how criminal justice approaches to cyber-attacks were potentially not only ineffective but also counterproductive in a cyber environment.

There also appears to be a significant difference in attitudes to offence and defence, with realspace norms being accepted most readily in the matter of cyber offence but less so in relation to cyber-defence where there is an indication of a tendency towards collaborative

self-help, and private sector engagement in providing state-like protection for citizens and engaging in forensics and evidence gathering on behalf of state law enforcement agencies. This would seem to indicate that there are opportunities for further formal collaboration with law enforcement that – within the context of protecting the citizenry - may be beneficial to both the state and the private sector.

8.4 Theme Four: The Need for Collaboration

The interviews identified a perceived need for wide ranging collaboration to address cyber security issues and a belief that cyber security is fundamentally a collaborative activity. This collaboration not only requires engaging with a large number of different groups but also a depth of partnership that requires a high level of trust, shared objectives, and common purpose.

Information sharing was one of the most commonly cited areas where collaboration was important. This encompassed threat information sharing, but also the sharing of experiences with peer organisations operating a similar systems environment that would include "*techniques, infrastructure, incidents and threats.*" (Participant A)

The rationale for collaboration was described most often in terms of shared interests such as "*a common enemy*" or, "*commercial drivers due to shared business interests*" (Participant A), but also as an essential operational element due to industry and systems structure. The CNI was described as having to be a partnership with the state due to the national significance of the infrastructure and its private ownership (Participant A) but more generally the increased interconnection of organisations has "*removed security boundaries between organisations*" making collaboration fundamental to the security of organisations individually and collectively (Participant B). This was also expressed in statements such as "*in some aspects of cyber, community is everything*" and "*all security is shared*" (Participant J)

Collaboration was seen generally as uneven across the commercial sectors, with different areas displaying more successful collaboration than others. For example, collaboration was different at practitioner, commercial, national and international levels; it was different by

sector with Financial Services, and FS-ISAC[44] in particular, being cited as a good example. It was also different depending on which particular aspects of cyber security were the subject of collaboration. Threat analysis and threat information sharing were seen as a good example of collaboration in particular in relation to a specific attack, but collaboration was seen to change once an attack had been stopped. Sharing was less prevalent when faced with issues such as acknowledging a breach had occurred or sharing commercially valuable threat resolution information. Difficulties in attribution also made collaboration less successful as potentially sensitive forensic information would need to be shared.

One positive view expressed was that this may be purely an indication of a lack of maturity of the processes in areas other than threat information sharing and that other processes may just need to reach the same level of maturity to be successful.

Some specific areas were identified where collaboration was proving more difficult and requiring improvement, in particular law enforcement, the ISP/CSP industry for take-down requests, and the cyber security and other systems vendor community – although there was an acknowledgement of the dependency they represent for most organisations in particular with respect to their patching strategies.

Trust was cited as a factor in determining the success of collaboration, with successful sharing examples given in "*closed networks – where you know everyone in the room*" (Participant I) as well as the need for collaborative activity to be "*a two way conversation*" (Participant G) with "*an equal collaboration*" (Participant A) being essential for success.

Collaboration was acknowledged as a key element of delivering cyber security, and while there were positive examples of good collaboration, this was seen as constrained by issues trust, shared interests and costs.

This has created an uneven collaborative environment where there are pockets of good practice, in particular in sector-specific threat information sharing, but the collaborative approaches were seen as diminishing once it extended beyond groupings where they 'knew

[44] FS-ISAC is the global Information Sharing and Analysis Centre which collects, analyses and shares threat information relevant to the financial services industry. More information about FS-ISAC is available at https://www.fsisac.com/

everyone in the room' or where the information that needed to be shared was either commercially sensitive (or commercially valuable) and involved admissions of failure.

This would suggest that there is potential for greater collaboration across industry sectors, across international boundaries, and further through the process of investigating and mitigating an attack – as well as extending collaboration to include greater engagement with law enforcement.

While there is an understanding of the need to collaborate and a willingness to engage in collaborative networks, as one participant described it "*the benefit of sharing has to exceed the cost of doing it*" (Participant I) and there is a precondition of trust in both capability and motivation of collaborative partners, which is reinforced by interview data relating to the difficulties working with government.

8.5 Theme Five: Difficulty Working with Government

Alongside a widely held belief in the need for collaboration between private sector entities and with state agencies, there was evidence of a degree of frustration with the experience of working with government. Specific examples included frequent and diverse requests by government agencies for the secondment of staff, the provision of free resources, and unplanned access to skilled human resources. Frustration was indicated with both the frequency of requests and the unstructured nature of multiple requests from multiple agencies placing a demand on limited resources.

A second difficulty identified was that of being able to build a personal relationship with government representatives due to both reorganisation and staff movement between departments with one participant stating that "a*s soon as you build a relationship with someone they are moved to another function*" (Participant A).

Law enforcement were seen as one of the most frustrating agencies to deal with, mainly as their priorities are seen as being different, leading to a different type of organisation that operated on a 'case' basis along with associated evidentiary requirements which were seen as potentially resulting in embarrassing or confidential materials becoming public.

A lack of feedback was also identified as an issue with dealings with state agencies, with a view that information was only flowing one way and ideas were at times being used and adopted without giving credit.

Reference was also made to the case of Marcus Hutchins who had been instrumental in resolving the Wannacry attack, but who was later arrested by the FBI, allegedly with the foreknowledge of GCHQ, with whom he had worked to resolve the Wannacry attack (Corfield, 2017). This was referenced as a significant breach of trust (Participant E).

Much of the comment regarding dealing with the state revealed a perception of a lack of trustworthiness on the part of the state agencies, for example. "*…there is still a long journey to go for organisations to trust the government…*" (Participant B). Several participants directly mentioned the need for trust, such as "*You have to be sure you can trust the people you are dealing with and they understand the issues involved*" (Participant B) and when talking about sharing information with state agencies "*…we have to trust that information will not be misused or used in a reckless way that breaks trust…*" (Participant A).

This was particularly the case in relation to the arrest of Marcus Hutchins, with one influential member of the cyber security community declaring that "*I am withdrawing from dealing with the NCSC and sharing all threat intelligence data and new techniques until this situation is resolved. This includes through the* Cyber Security Information Sharing Partnership*. Many of us in the cyber security community openly and privately share information about new methods of attacks to ensure the security for all, and I do not wish to place myself in danger."* (Beaumont, 2017)

Interviews showed that both of the conceptual dimensions of trust in terms of competence and motivation (Hardin, 2006, p. 36) were questioned by participants.

Comments describing law enforcement included "*their interests are different to everyone else*" (Participant A) and that state agencies had "*different perspectives*" (Participant L). Government in general was described as having "*too many different departments*" (Participant F) and being "*too slow to deal with cyber*" (Participant F) while in relation to information sharing, Participant B stated that there was "*…scepticism about what government can offer…*" and Participant J described governments as "*….struggling with basic things….*" and not having "*…money resources or expertise…*" but noted that "*…the UK is one of the most capable...*"

A number of participants also directly referenced an industry-wide shortage of cyber-skills as a contributory factor to the difficulties in dealing with the government especially given a perceived disparity in salaries between public and private sector organisations that is supported by evidence presented to the Parliamentary Joint Committee on the National Security Strategy (Committee on the National Security Strategy, 2018).

Staffing and skills issues may also be a factor in the levels of trust that exists between the state and the private sector. One of the main incentives of trust is the anticipated benefit of further interactions (Hardin, 2006, p. 45). Trust experiments indicate that iteration of interaction is key to developing trust and that a 'one shot play' of a game cannot even be used to test for trust as a larger relationship is required. (Hardin, 2006, pp. 51, 53). Participants indicated that in their dealings with government there was a level of change and reorganisation which made this difficult (Participant A, F), and a case-based allocation of law enforcement officers also limited the opportunity for a strong relationship to be built (Participant A) alongside a shortage of resources (Participant G) or that officers were not being given "*the space and time to develop the relationships needed*" (Participant B). A positive comment regarding the NCSC re-affirmed the relationship requirements with dealing with the NCSC described as "*…dealing with a group of people who even with different roles have often been the same people…*" (Participant A).

There were also indications that there was a lack of feedback and recognition that was inimical to the development of a trusting relationship. Participant A stated that "*…we cannot provide information on every attack and get no feedback…*" while Participant B described CiSP as "*one way…with information going from the private sector…*" and Participant J described the NCSC as providing "*…no acknowledgment of where ideas come from which annoys everyone in the industry right away.*"

Trust is important as an essential building block of a collaborative environment, which is perceived as fundamental to the ongoing delivery of security in cyberspace.

This was not an entirely negative picture with (and despite the timings of the interviews being early in the development of the NCSC) some participants expressing optimism for the future role of the NCSC in driving a collaborative environment. Comments such as "*…they know how to engage with the private sector…*" (Participant A) and "*…they have reached out to the*

community and are making a real effort to have a conversation…..and not just lead the way…" which was also seen as "*…a big change in tone over the past twelve months…"* (Participant G) and "*…a good example of outreach...*" with particular reference to "*…good initiatives out of their industry engagement team which means it is not just a one way flow…"* (Participant H)

This supports other comments which suggested that the introduction of the NCSC has been a positive initiative and that their approach to engagement with the private sector is creating an environment in which greater trust may be possible going forward.

8.6 Theme Six: The Changing Nature of the Environment

Cyber security was referenced as an environment in a constant state of change and that this fundamental characteristic was a driver behind many of the issues in cyber security, and an inhibitor of potential solutions. This was typified by the claim that "*….we don't understand today what we will need tomorrow.*" (Participant C)

This changing environment was described in various ways and through many different examples. The adaptive nature of the cyber-threat was a particular concern with it described as "*always changing - very adaptive*" (Participant B) and with "*new threats constantly materialising*" (Participant C). Specific changes in the malware environment were referenced, for example the Wannacry attack which was based on pre-existing malware that was modified to take advantage of the Eternal Blue exploit of the MS17-010 Simple Message Block vulnerability (Participant D).

The same Wannacry example was also an indication of some of the unexpected consequences of actions within cyberspace, in particular the fact that Wannacry would not have existed if "*…the US Government had not spent large amounts of money finding vulnerabilities and not reporting them*" (Participant D).

Related to the adaptive nature of the threat was a concern that proliferation of capabilities was enabling unsophisticated cyber actors such as 'script kiddies' to develop increasingly sophisticated capabilities and so becoming capable of launching significantly more destructive attacks.

The changing environment is also an issue in relation to the information technology infrastructure and its usage inside organisations which make it difficult to identify any kind

of security perimeter for the corporate system environment. Employee access to social media and personal webmail from the desktop and an increase in BYOD requirements have introduced insecure systems inside the perimeter. This has damaged the credibility of any perimeter-based security. Some organisations were also seeing new vulnerabilities being introduced to their environment by the connection of legacy systems that had not previously been connected to the Internet. These changing network structures were seen as a business issue rather than a technical one.

New threats could significantly change some of the underlying assumptions about attacks. Ransomware was cited as removing the time element from a cyber-attack in that prior to ransomware a typical attack would, after initial compromise, require time for an attacker to identify, access, and exfiltrate the data that had value that could be realised by attacker such as credit card numbers or passwords. Ransomware does not require the time or the effort that a data theft requires to be profitable, and so changes the way in which defensive systems need to respond to any attack (Participant B).

However, there is also a view that some threats are genuinely 'old wine in new bottles' with malware threats in particular being recycled, but also with reference to the challenge of IoT being just an old problem of inadequately secured devices reappearing – albeit at a scale beyond anything that has been seen before.

There is an acceptance that the threat is not going away and that whatever defensive mechanisms are put in place only serve to make the attackers adapt their behaviours to work around them. This was described as "*an arms race*" in terms of cyber security and defensive capabilities (Participant J).

One of the implications of the changing nature of the environment, particularly with regard to the threat, is that it is an environment with a large population of metaphorical black swans that cannot be easily predicted or planned for. This would suggest that there is no one answer to the problem of cyber-attacks, and this was expressed by participants as there being no "one size fits all" process that could be applied, with the volume and the rate of change creating organisational process issues. This again points to cyber security having the characteristics of a wicked problem.

The increasing capabilities of script kiddies has been shown by the attack on Talk-Talk by a teenage boy, and the Mirai botnet which originated in attacks on Minecraft servers and eventually came to the point where it compromised key components of the global infrastructure of the Internet (Graff, 2017). The development and easy availability of sophisticated and cheap hacking tools is potentially adding to the random nature of attacks. Attacks can be based on crafting an exploit for a certain vulnerability rather than trying to attack a specific target organisation. With tools that can scan the internet for hosts with specific vulnerabilities, any number of potential targets can be easily identified.

The unpredictable and changing nature of attacks means there are no simple solutions, and that a long-term approach has to be adopted. Installing more security devices will not fix underlying solutions, and "*…focusing on the latest 'hack du jour' is not fixing anything.*" (Participant J) In particular there is an emphasis on accepting that security will be breached, and architecting systems in such a way as to minimise the impact and mitigate the effects of multiple potential attacks, but it was also recognised that what should be considered good practice can also change in response to changing threats.

However, although the threat picture is changing, the underlying threat is not seen as one that is going to go away, but there is a concern that in some quarters there is a view that cyber security is a problem that only appeared five years ago, and that it will be gone in another five years, whereas the reality is that there is no visible end to the issue.

8.7 Theme Seven: The Need for Better Understanding

One of the key issues to emerge from the research was the need for educational initiatives that would deliver a greater level of understanding of the non-technical aspects of cyber security and importantly their connection and inter-relationship to the technical aspects. Cyber security is seen as encompassing a number of disciplines that require engagement at both a high-level policy and a micro level.

This need for education was evident at several levels:

Firstly, in the understanding of the business environment in which cyber security operates. There was a strong view expressed that much of the discourse around cyber security is too generic with the reality requiring a more nuanced discussion. It is not possible to talk

generally about a threat to 'the private sector' or even a specific industry sector as there are significant differences in terms of the risk and impact of any specific threat that are different for different organisations. For example, a DDOS threat to a trading or online gambling organisation is potentially much more significant than it is to a manufacturer, as being unable to trade for a period of time could be catastrophic for a trading company. There is a clear view that there is no single process or solution that can be applied and as a result, the way in which cyber security problems are segmented and defined will be key to their resolution. Such an approach, which aims to segment the problem into manageable chunks, is typical of a taming approach to a wicked problem.

Secondly, there is a need to be able to bridge the understanding from technical vulnerability to business risk in particular for the 'C Suite' to understand not only the risks that are inherent in their infrastructure and business operations, but also to understand which are the critical data systems and technology, how they are protected, and how potential beaches can be mitigated through network segmentation, encryption and recovery systems.

There is a need to be as proactive as possible in defence, for example to implement an architecture that assumes a breach of the perimeter but limits lateral movement, creates segments that can be isolated, with the equivalent of bulkheads to prevent the spread of damage, and enables incident response and recovery rather than just the ability to patch reactively. It needs to be built in a way that will enable not just the latest high-profile attack to be defended, but to invest in mitigation capabilities that will assist in the response to any attack.

Third, there is a need to understand the motivations, methodologies, capabilities and targets of threat actors, and the business models under which they are operating. This in part is an acknowledgment that it is not possible to know what tomorrow's threat will be. There is an unknown number of 'black swan' events waiting to appear and so defensive initiatives need to include a predictive element where possible.

Fourth, the understanding of risk needs to be achieved without resorting to hype and the pedalling of 'snake oil' solutions. There was significant criticism of the cyber security industry with a suggestion that vendors did not understand their customers or necessarily the technology environment they are selling into. There is a case suggested for larger

'target' organisations to lead by example, to "*communicate how we do business and create a social change towards cyber protections*" (Participant E).

Fifth, the threat is highly adaptive and would seem to be mainly (by volume of attacks) purely opportunistic with "*no change control processes or regulatory approvals they have to adhere to*" (Participant C). This gives the attacker an inherent advantage in that the threat can adapt more quickly than most organisations can develop new defensive mechanisms. The advantage the defenders have is that they should be able to understand their own business more than most threat actors and be able to link the technology with their understanding of the business.

However, given this threat actor adaptability there is also the need for innovative and flexible responses from the organisations trying to defend against cyber-attacks. An entrepreneurial approach of being fast moving and prepared to fail, and a need to look at the problem differently in order to bring different solutions to the market. These types of intellectual skills and organisational competencies will be essential to enable effective responses to be developed.

Sixth, given the need for this level of organisational capability there is a need to properly support and reward the people working in a security organisation. This is both a pragmatic need as they are potentially the resource most difficult to replicate, but also a reflection of the need to ensure they have the skills, tools, processes and infrastructure to deliver in their role.

Seventh, there is need to create an intelligent digital consumer. This is the type of consumer who realises there may be risks associated with a publicly accessible spy camera in their child's bedroom, or someone who wants to understand what happens to their data when they confirm their acceptance of the terms and conditions. It is the type of consumer who is aware of how a shared online quiz could be used against them or how their social media activity can be used to enable an attack. There is a need for areas that the general population can trust, for example a guarantee that an App store is safe, or that Microsoft updates can be installed. This is why the Facebook data sharing issue is so fundamental, and perhaps a 'teachable moment' for a lot of individuals as it shows how we have come to assume these services are operating ethically and somehow looking after the consumer's best interests,

when clearly they may not be. There is a need to create consumers who are aware of the security implications of their own purchasing decisions rather than living with a situation where "*Consumers are unaware if their baby monitor has been part of a DDOS attack on a U.S. bank.*" (Participant I).

Eighth, this understanding needs to make its way into all areas of government. It is difficult for the UK government to appear credible when a stated desire to be the safest place to do business online is followed by a stated intention to ban encrypted messaging apps., or when a confused understanding is displayed by senior politicians as was reported in relation to (then Home Secretary) Amber Rudd's statements on encryption (Collins, 2017).

This need also applies to law enforcement, where there is a perception of a lack of understanding of the needs of commercial organisations. Working with law enforcement was seen as difficult because of different objectives of law enforcement to gather evidence and build a case for criminal prosecution as opposed to a commercial organisation's objectives of defending against a breach and mitigating the impacts.

Strongly related to the need for these non-technical skills and more holistic understanding is the need for extensive collaboration, not only on threat intelligence information sharing, but by taking some of the industry best practice and being able to apply it on a cross sectoral basis. There is a need to build collaborative networks of knowledge that are based on high levels of trust and benefit to all involved.

There is, inevitably, the issue of the commercial value of vulnerability and exploit information (and the sensitivity about sharing information about attacks that were not successfully defended). While GDPR now mandates breach reporting, whether the information that is gathered is sufficient to be able to assist other organisations seems unlikely, and any reporting via CiSP or other sharing platforms remains purely a matter of good will. Among the interview participants there was a perceived national security risk attached to the fact that there is valuable information that is not being shared due to its commercial value and commercial considerations being placed before security.

The interaction of the technical and non-technical elements of cyber security issues is also reflected in an acknowledgment that cyber security is as much a human issue as it is a

technical issue and the education that is required is not just about producing computer science graduates. Addressing these cyber security issues in the future will require people with an understanding not only of the technology, but the human element, business process, risk management, trust and collaboration, and ethical considerations (including privacy and data ownership). The dependency on technology and technicians alone to resolve security issues may be a misjudgement of both the problem and the technology. Participant D quoted Bruce Schneier's oft quoted line, stating that *"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology" (Schneier, 2000, p. xii)*

The knowledge and skills that will provide the ability to effectively link technology to process, to business objectives, or to government policy were seen as fundamental to future success.

The theme of the need for greater understanding emerged as a key factor in that the lack of understanding was seen as something that damages trust and hinders collaboration, prevents solutions that address the complexity of the changing nature of the environment, determines the need for regulatory action in the absence of voluntary action and prevents successful relationship with government agencies.

The importance of developing skills has been reflected in many of the actions taken by the NCSC through a range of training initiatives (NCSC, 2018b). Extending skills beyond the technical has also been recognised through a focus on the human factors in cyber security (NCSC, 2017c) as well as concerns relating to developing an understanding in the business community about the importance of cyber security as a business risk issue, shown by the changes in audience selection for the securitisation speech acts and a focus on business organisations such as the IoD and the CBI.

There are issues that emerge because of the different objectives of different groups, in particular around the commercial value of information which may limit the willingness to share information in a timely manner. Speed of action is important because of the adaptability of the threats and threat actors which needs to be countered by the same flexibility and adaptability in defensive operations.

Network and system defenders should have advantages over attackers in terms of being able to understand their own networks and systems and use that knowledge to be able to respond to attacks in a way that minimises risk, but this requires an in-depth understanding of the assets that are at risk as well as means of compromise.

It is also apparent that cyber security is a 'team effort' that requires engagement of any number of different disciplines and organisations. It is a socially complex and highly adaptive environment.

9 Conclusions

This chapter provides the final conclusions of the analysis documented in this thesis. It is argued that cyberspace is a New Medieval environment in which the state does not have sole authority; that the construction of security threat and a process of securitisation has been used to justify the assertion of greater levels of state authority in cyberspace; that cyber security remains a complex task and a shared responsibility that has the characteristics of a wicked problem; and finally that the nature of wicked problems suggests that current institutional taming approaches may be insufficient to successfully resolve cyber security issues, and that it will be through changes in governance and greater collaboration that any progress will be made.

This research project has identified characteristics of cyberspace that reflect a New Medieval governance environment, including the overlapping authorities and non-state-based governance systems that result in the state being only one of many authorities in cyberspace.

This has suggested a state governance gap in terms of the capabilities of the state in realspace and state capabilities in cyberspace. This has been long documented in terms of the challenge to state sovereignty from cyberspace through transnational actors, as well as highlighting the jurisdictional limits of the state in relation to cyber activities. As cyberspace has increased the extent to which it can influence realspace, the potential threat to the state in realspace has become a more significant issue and has required a response from the state. In the UK, much of this response has been through a process of securitisation in which cyber threats have been constructed as an issue of national security and the engagement of state security agencies in the delivery of cyber security has been legitimised.

Governance in cyberspace is continuing to evolve in relation to the role of the state. The development of state level firewalls and increased regulatory intervention such as GDPR and NIS is leading to a greater role for the state in cyber governance. Initiatives such as DNS blocking, and national level firewalls are indicative of a move towards a more territorial and state based governance structure. This thesis has argued that one of the main ways in which these new governance models are being promoted is through the issue of security in cyberspace. In the UK environment this has been through the construction of the

cyber security threat through an identifiable process of securitisation that has placed the state and state agencies at the centre of the governance of the security response. This is an almost inevitable response to the changing nature of cyberspace, the increased societal dependency, the connection of critical systems, the value of the financial flows, its fundamental contribution to logistics in a just-in-time environment and many other factors. It might be that cyberspace can now be considered too important to be left in the hands of governance systems that depend on humming as a decision-making mechanism.

One of the objectives of this thesis was to try and identify whether New Medievalism cld help to describe Cyberspace as a governance environment. While the Medieval metaphor has been used in the past, the analysis of the eleven characteristics identified in the literature has shown that New Medievalism is a useful framework through which to view cyberspace. The existence of overlapping competing authorities means that the state has not to date been the sole authority in cyberspace. This situation is most often seen as changing states such as Russia, China and Iran who are developing their own controlled cyberspace environments, but the UK state has also taken steps to compete with the other authorities in cyberspace, for example by introducing content filters, and adopting key regulatory initiatives such as GDPR and NIS which effectively offer a level of state based control over how private organisations operate in cyberspace.

One of the main justifications for enhancing UK state authority in cyberspace has been based on the construction of a security threat that extends beyond the cyber realm with realspace effects from cyber threats through an ongoing process of securitisation. This construction of the security threat has been effective in seven key areas.

First, the Information Security community has accepted that there are certain threats that private organisations cannot defend against, in particular sophisticated state or state-sponsored attacks, and so a state level capability is required that has capabilities over and above that allowed to the private sector. This is a regular theme in the securitisation speech acts analysed as part of this project.

Second, the construction of referent objects such as 'digital society' and 'critical national infrastructure' that are beyond the defensive capability of any single non-state security

provider reinforces the idea that the state is the only institution that can defend these referent objects as well as extending the cyber threat to the realspace environment.

Third, this construction of referent objects for securitisation that mirror realspace referent objects of national security, represent a mechanism to justify state security on the basis of realspace precedent.

Fourth, private sector referent objects such as privately owned CNI, or intellectual property have been appropriated as part of the securitisation discourse as requiring state engagement.

Fifth, there has been an acceptance of realspace norms in relation to offensive capabilities being within the sole remit of the state. This has extended to the definition of required defensive capabilities based on 'Active Cyber Defence' which may incorporate offensive elements that are therefore restricted to use by the state.

Sixth, there has been an acceptance of the exceptional measures requested, including additional funding for state institutions, co-option of private sector organisation as regulatory intermediaries, and the adoption of regulation in areas that were previously unregulated including regulatory interventions such as GDPR and NIS.

Finally, there has been a consolidation of state cyber security institutions within GCHQ along with an acceptance that the sovereign capabilities of GCHQ (the secret sauce) are required to deliver cyber security. This has led to a reduction in oversight and a shift in the balance of power to the state.

The overall effect of this has been for securitisation of cyberspace to enable the assertion of greater state authority in the UK cyber environment to the point where it now has influence over regulatory design, educational programmes, skills certification, security standards, and product design criteria.

The development of state authority in this way may have significant implications for the future of the global governance of cyberspace, with the potential for increased state based multi-lateral governance in place of existing multi-stakeholder arrangements. There is already competition between the state based International Telecommunications Union and the multi stakeholder based Internet technical standards development organisations over ITU initiatives described as 'new IP' (Sharp and Kolkman, 2020) or the Network 2030

initiative (ITU FG-Net-2030, 2020). This is despite the introduction of the IGF as a multi-stakeholder element within the multi-lateral ITU, although it should be recognised that the IGF only ever had an advisory capability and was constitutionally unable to decide on anything.

The multi-stakeholder approach can be interpreted as US centric in both style and participation, perhaps due to it's organic development from the early Internet institutions in the United States, however it recognises the importance of the private sector and other non-state actors within the governance system. There are pressures on the multi-stakeholder system from countries such as China and Russia (among others) who argue for a multi-lateral states based system. It is possible that, given the increased importance of the state in UK cyber security, that a multi-lateral system may become a more attractive option for liberal democracies moving forward. In the same way that the UK state has found it unacceptable to rely on the actions of the private sector to deliver national security, it may prove that a dependency on non-state actors in global governance is equally unacceptable especially in an environment in which state based attacks are more frequently undertaken against critical national infrastructure.

It would seem unlikely that the current multi-stakeholder system can be maintained in the face of these pressures. However, the characteristics of cyberspace that emerge from its New Medieval nature are fundamental to the environment and are unlikely to change without the kind of restructuring of authorities that was brought about by the Peace of Westphalia. This (again) suggests the need for the imposition of a nation-state level of authority on cyberspace. Existing developments would suggest that this is most likely to be achieved through the extension of the 'Splinternets' beyond those nations where they are already in process, which in turn would suggest the end of the multi-stakeholder governance systems.

One would expect significant issues with this both in terms of the effective withdrawal of support for a US centric model of cyberspace, and the criticism that would be attracted by the UK following a path that has so far been associated mainly with Iran and China, and generally viewed as being undemocratic and inimical to freedom of expression. However, it is worth noting that there is an alternative vision for future governance models which suggests that rather than multiple Splinternets there will be a bifurcation into one Internet

run by US interests and one by Chinese, with other nations choosing between them (Kolodny, 2018). However, this would not deliver the nation-state authority that seems to be required for effective cyber security at a national security level, but instead may lead to what could be described as a colonial approach to Internet governance, with China and the US exerting authority over their portion of cyberspace. This is counter to the essentially borderless nature of the Internet and the state based nature of realspace and so, conceptually at least, has little to suggest it is a likely outcome.

There are other developments that may have an impact on both the character of cyberspace and the delivery of cyber security, in particular quantum computing and blockchain but it is beyond the scope of this thesis to do more than acknowledge that they exist for future study.

Without some significant change, the underlying characteristics of governance in cyberspace as a New Medieval environment may ensure that the issues relating to security continue unabated. Combined with the implications of cyber security as a wicked problem this would mean that security in cyberspace would remain a completely irresolvable issue. The governance issues implicit in New Medievalism, combined with the characteristics of wicked problems would make any solution mutually exclusive, except for global collaboration on a scale and scope beyond anything that currently appears possible. Without a different non-state based method to deliver security, it is expected that there will a continuation of the growth of state authority and possibly the inevitable migration to state based global governance.

Security issues and a process of securitisation have been the driving force behind the development of state authority in UIK cyberspace. The analysis of the original data collected as part of this project identified several issues in the delivery of cyber security including the failure of taming solutions such as regulation; the need for greater collaboration beyond threat information sharing; the limited capabilities of individual organisations to resolve problems; and the complexity and changeability of the issues involved, leading to a lack of resolution of the underlying problems. The issues pointed to cyber security displaying the characteristics of a wicked problem which suggests a need for a more inclusive approach to delivering cyber security than that which may be offered by a state led solution. The specific themes that emerge from the interview data provide a

construction of the cyber security environment and the relationship of the state and private sector in delivering security in cyberspace that shows a complex environment with some important characteristics.

1. Cyber security is delivered in a complex and rapidly changing environment that does not allow for 'one size fits all' solutions, but requires a range of interventions, that may at times have conflicting objectives.
2. The constant change of the environment is also driven by the consequences of actions within the cyber security environment, creating a cyber 'arms race' between attackers and defenders.
3. A cyberspace environment that is based on private sector development and implementation does not meet the needs of the state, nor is it necessarily motivated to do so. The profit motive is not delivering a cyber environment that is secure and immune to criminal and terrorist use. This current cyber environment is also increasingly open to criticism for failing to protect young people. Again, a range of interventions may be needed in order to manage this situation ranging from education, through regulation to direct actions through state agencies.
4. There is a lack of clarity concerning the roles of state and private sector organisations. Again, there is no model that provides the basis for the relationship across sectors, with clear differences between, for example, CNI organisations and others.
5. There is a need for collaboration that goes over and above the current information sharing paradigm. Neither the state nor the private sector are seen as being able to deliver cyber security in isolation. There is an uneven collaborative environment with pockets of good practice but also areas where collaboration is not as strong and is hindered by disparate objectives and working practices as well as an environment that may not reward collaboration.
6. The cyber security environment is constantly changing in response to new customer demands, new technology, or even old technology being used in new ways (e.g. ICS/SCADA systems being connected).

I would argue that the themes that have emerged from the research interviews support the construction of cyberspace as a New Medieval environment, in particular in relation to of the complexity caused by overlapping authority between the state and the private sector, and also identified many of the issues that have been constructed through the securitisation speech acts

This thesis argued that security in cyberspace displays all ten of the characteristics of a wicked problem with the addition of the social complexity that is also characteristic of a wicked problem environment. The never-ending nature of the problem, the constant adaptation of threats to overcome, and so the constant redefinition of the problem means that it has no 'stopping rule'. The challenge of cyber security is, in the current environment, one that will never go away. Any suggestions that the actions being taken in response to cyber security issues provide any more than a temporary fix or simply the next escalation in an arms race of cyber capabilities have, to date, been shown to be wrong, and given the nature of wicked problems, will almost certainly continue to be so. Wicked problem literature suggests that the authoritative taming solutions which accurately describes the introduction of the NCSC and the 'we can fix this' approach that has since been adopted may not be a guarantee of long-term success and it is noticeable that a 2019 RUSI paper called for a strategic change in the next National Cyber Security Strategy in 2021 that the "*…UK's future approach to cyber security requires a whole of society response*" which "*…involves bringing together the capabilities of the private sector, government and wider society to achieve common goals in cyber security*" while warning that such an approach "*…is easy to express in rhetoric, but will require serious investment of time, energy and intellectual capital to build necessary partnerships to deliver results.*" (Prince and Sullivan, 2019). It is this type of 'whole of society' approach that is associated in the literature with collaborative approaches to managing wicked problems (as explained in Section 7.2 Addressing Wicked Problems) but is generally acknowledged as being the most difficult to implement. This would be significant change from the authoritative expert driven approach of the 2016 NCSS, but the evidence gathered through this research suggests that it may be an option that requires serious consideration.

9.1 Areas for Further Study

As this project progressed it became clear that there were many areas that required further study outside the scope of this research.

First, an international comparative study based on the underlying theoretical analysis in this thesis would be an interesting approach to study cyberspace outside the UK. This could include the conceptual development of a layered governance model that could disconnect governance issues of one layer (e.g. the physical layer) from the logical and virtual layers and whether this offers any realistic advantages in determining optimal governance systems for cyberspace. Adopting a layered principle for Internet regulation has been proposed in the past (Solum and Chung, 2003) but there has been no development of regulation that could be applied from the principles outlined.

Studies could also be usefully be undertaken to evaluate the possible implications of Internet Balkanisation and understand how such a model could be applied to UK cyberspace if the international environment becomes such that this model is appropriate for the UK.

There are a number of technologies that may fundamentally change the architecture and design of cyberspace to such an extent that it may also fundamentally change the governance systems that operate in that technological environment. The development of high bandwidth satellite to satellite optical communications, for example, has potential implications for sovereignty debates given the limits to national sovereignty in outer space (so removing the physical territoriality argument concerning sovereignty over virtual environments) and whether the development of a cyberspace backbone infrastructure in space has implications for the outer space treaty of 1967.

Artificial intelligence in cyber security is one area that may significantly change the dynamics of the security environment, as well as a blockchain based internet development.

There are other softer considerations that may also benefit from further work. One of the most striking elements of this research project was the similarity in thinking of many of the interviewees, and how consistent that was with much of the official narrative on cyber security. In conjunction with other indicators, such as the number of interviewees who self-identified as former military, intelligence agency, or defence industry, the consistency in the

'thought leaders' speaking at multiple conferences and events, and reviewing social media posts, there is enough reason to think that there may be an interesting avenue of research to evaluate indicators of Groupthink in the Information Security Community. This is potentially exacerbated by the consolidation of government thought leadership in GCHQ.

Alongside issues of thought leadership there is scope for more work to be done to understand the effectiveness of oversight mechanisms in cyberspace. There are a number of areas during the research where oversight appears to have some difficulties in the UK, especially around the consolidation of capability in GCHQ, vulnerability hoarding by GCHQ, vulnerability sharing with the NSA, and the apparent lack of engagement of the ISC in cyber-issues. A comparative analysis focusing on oversight of state cyber security activities may be an interesting project for the future, perhaps also alongside an equivalent analysis of the oversight of private sector cyber security, which remains a market driven activity in which solutions such as cyber-insurance are as valid as implementing effective security.

Appendix A: Key Securitisation Speech Acts 2012 - 2017

This appendix provides a securitisation analysis of the speeches identified as part of a process of securitisation between 2012 and 2017 as identified in *Table 30* below.

Table 30 Securitisation Speeches 2012 - 2017

Date	Speaker	Position	Audience
26 June 2012	Jonathan Evans (Evans, 2012)	DG MI5	City of London
12 Oct 2012	Iain Lobban (Lobban, 2012)	Director GCHQ	IISS
17 June 2014	Ciaran Martin (Martin, 2014)	DG Cyber Security GCHQ	IA14 Conference
2 June 2015	Ciaran Martin (Martin, 2015)	DG Cyber Security GCHQ	Infosec 2015
24 Sept 2015	Michael Fallon (Fallon 2015)	Defence Secretary	RUSI Symposium
10 Nov 2015	Robert Hannigan (Hannigan, 2015)	Director GCHQ	IA15 Conference
17 Nov. 2015	George Osborne (Osborne, 2015)	Chancellor of the Exchequer	GCHQ
13 Sept 2016	Ciaran Martin (Martin, 2016b)	Head of NCSC	Billington Conference
20 Oct 2016	Michael Fallon (Fallon, 2016)	Defence Secretary	RUSI Cyber Symposium
1 Nov 2016	Philip Hammond (Hammond, 2016)	Chancellor of the Exchequer	Microsoft Conference
20 Oct 2016	Michael Fallon (Fallon, 2016)	Defence Secretary	RUSI Cyber Symposium
14 Feb 2017	Philip Hammond (Hammond, 2017)	Chancellor of the Exchequer	NCSC
27 March 2017	Matt Hancock (Hancock, 2017)	Minister of Digital and Culture	IoD
13 Sept 2017	Ciaran Martin (Martin, 2017b)	CEO NCSC	CBI
15 Nov 2017	Ciaran Martin (Martin, 2017d)	CEO NCSC	Times Tech Summit

This appendix should be seen as additional underlying information in relation to the analysis included in *The Securitisation of UK Cyberspace* on page 161. The commentary sections for each speech is intended only to highlight some specific

aspects of the speech that add to the previous analysis and is not intended as a full analysis in its own right.

Table 31 Jonathan Evans Speech 26th June 2012

Date	Event	Audience	Securitising Actor
26th June 2012	Lord Mayor's Annual Defence and Security Lecture	City of London	Jonathan Evans DG MI5

Speech Act	Referent Objects	Identified Threats	Exceptional Means Demanded	Securitization Categories
"….cyber security ranks alongside terrorism as one of the four key security challenges facing the UK." "…industrial scale processes involving many thousands of people lying behind both state sponsored espionage and organised cyber-crime." "…risks of real world damage as well as information loss"	Government information Infrastructure Intellectual property Future prosperity Companies and corporations	Criminals States Terrorist groups	Engagement with private sector Investment in world class capabilities, technologies and skills Increased levels of international cooperation Balance between regulation and flexibility	Political Economic

This was a wide ranging speech that was not specifically about cyber security. Given in the run-up to the 2012 Olympic Games, and titled "The Olympics and Beyond" it was a future looking scan of the security horizon that, along with cyber, encompassed the euro-zone economic crisis, terrorism and Iranian nuclear ambitions. However, as the first security service speech that specifically references cyber in a securitisation rhetorical structure, it can be seen as a starting point for future developments.

There is some indication of inter-service rivalry between MI5 and GCHQ regarding cyber. In what seems to be trying to establish MI5's cyber credentials, Evans emphasises the collaborative work of MI5 and refers to the CPNI as having "*encouraged the development of information exchanges*" and "*investigating cyber-compromises in over a dozen companies*".

Table 32 Iain Lobban Speech 12th October 2012

Date	Event	Audience	Securitising Actor
12th Oct 2012	Institute for Strategic Studies	ISS Members	Sir Iain Lobban, Director GCHQ

Speech Act	Referent Objects	Identified Threats	Exceptional Means Demanded	Securitization Categories
"…significant disruption to Government systems…" "...theft of intellectual property on a massive scale….of national security concern…" "…seriously disrupt the Critical National Infrastructure…" "…goes to the heart of our economic well-being and national interest" "…a knowledge economy needs to protect from exploitation the intellectual property at the heart of the creative and high tech industry sectors….maintain the integrity of its financial and commercial services."	Economy Government CNI	States e-crime insiders botnets personal data theft fraud	Prioritisation of cyber in SDSR. Direct feed of information from CNI operators Change in relationship between national security agencies and key industry players International coordination of counter measures Different approach to government/industry partnership	Economic Societal Political

This speech can be seen, in part at least, as a response to the Evans speech in June 2012, and represents a very clear statement of the Information Assurance mission of GCHQ, and the relevance of GCHQ's skill-set in that "*…mastery of high-end communications technology is hugely relevant to the problems of cyber security...*" and the combination of the IA mission with the intelligence mission allows insights into the

capabilities and motivations of cyber adversaries, as well as knowledge of our own vulnerabilities in government and the CNI. This can be interpreted as an overt 'pitch' for the cyber mission to be given to GCHQ. The threat analysis is fundamentally the same as we see today, with hostile states and criminals in particular as threat actors with the CNI, economy and government systems as the referent objects. Other similarities are also noticeable in that there is the call for improved working with the private sector (not only defensively, but also in relation to the business opportunity of cyber security), a first public reference to "active defensive techniques", and a focus on the underlying long term impact of cyber on economic prosperity.

Table 33 Ciaran Martin Speech 17th June 2014

Date	Event	Audience	Securitising Actor
17th June 2014	Information Assurance 2014 Conference	InfoSec Professionals	Ciaran Martin, DG Cyber, GCHQ

Speech Act	Referent Objects	Identified Threats	Exceptional Means Demanded	Securitization Categories
"…sophisticated, state-sponsored cyber espionage against UK government and industry networks is industrial in scale." "Cybercrime continues to pose a significant threat to the UK economy…" "…hostile activity against the networks of companies that own and operate critical infrastructure…" "Destructive cyber terrorism remains a potential threat."	Government networks Industry networks UK economy CNI	Supply chain threat. State sponsored attackers	"….applied our world-class technical expertise to assess some of the most critical IT systems in the country…increase capacity to deliver these reviews and advice" "…develop our partnership with CSPs by deepening our sharing of threat information…" "…focus on how we maximise the impact of our unique visibility and understanding of high end threats."	Economic Political

This was Ciaran Martin's first public speech as DG Cyber Security for GCHQ, and very much echoed the messages in Lobban's speech earlier in 2014. The focus was on defining the role of GCHQ in cyber security, emphasising the need for partnerships (the theme for the whole conference was "*Meeting the cyber security challenge in partnership*") and Martin refers to partnership with the business community, the NCA, CSPs, the Cabinet Office, Research Councils, and the CPNI.

Much of the emphasis, as is often seen, was also on distinguishing between the day-to-day threats and the frameworks that had been put in place to allow companies to deal with those threats for themselves (for example, CiSP, 10 Steps to Cyber Security, Cyber-Essentials, CESG Certified Professionals) while the focus of GCHQ was to be on government systems, the CNI, working with the NCA on major cyber issues

(online sexual exploitation of children was cited) and dealing with state-level threats. It is notable that at this point there is no reference to the UK wide automated protections that become a theme of the cyber-discourse in 2015 in preparation for the 2016 NCSS and the introduction of the NCSC.

Table 34 Ciaran Martin Speech 2nd June 2015

Date	Event	Audience	Securitising Actor
2nd June 2015	InfoSec 2015 Conference	InfoSec Professionals	Ciaran Martin, DG Cyber, GCHQ

Speech Act	Referent Objects	Identified Threats	Exceptional Means Demanded	Securitization Categories
Quoting Evans 2012: "What is at stake is not just our government secrets but also the safety and security of our infrastructure, the intellectual property that underpins our future prosperity…" "…pre-positioned capabilities on our infrastructure for future destructive use…."	UK Industry CNI Economic Success Public Services	Criminals State sponsored attacks Rogue States States Terrorists Hacktivists	New approaches – working internationally with FBI Acceptance of GCHQ advice Acknowledgment of position of GCHQ dealing with cyber security in the economy as a whole Ability to draw on intelligence capabilities	Political Economic

This speech in June 2015 is closely related to Hannigan's speech at IA15 in November and is focused on positioning GCHQ as the lead agency for cyber security. The speech is constructed in three parts of defining the threat, suggesting strategies for dealing with the threat, and finally emphasising the role of GCHQ in cyber security as "*not just the high end cyber defender of last resort, but as a body charged with promoting better information security in the economy as a whole.*" It is this positing of the wider authority of GCHQ in cyber security that is expanded upon in the Hannigan 2015 speech.

Table 35 Michael Fallon Speech 24th September 2015

Date	Event	Audience	Securitising Actor
24th Sept 2015	RUSI Cyber Symposium	Defence Analysts	Michael Fallon, Defence Secretary

Speech Act	Referent Objects	Identified Threats	Exceptional Means Demanded	Securitization Categories
"…today we stand on the front line of a virtual war." "…radicalise individuals and spread misinformation…" "…we have never been so digitally dependent." "…nor is it only our defence networks already under daily attack that are at risk…but our civilian infrastructure. Our transport networks. Our energy networks. Our banking systems. Our economy as a whole" "The Internet account for 8 per cent of the UK's GDP advantage. Over the last 10 years the ICT sector has grown three times as fast as the whole economy. And that could be worth hundreds of billions of pounds to us in the years ahead."	Economy State Critical National Infrastructure	Russia ISIL	Cyber 'hardwired into UK defence's DNA.' Upgrade of military capabilities. Creation of Joint Forces Cyber Group Improving Public Sector network resilience Building new Public Sector Network Testing private sector capacity to withstand cyber attack CiSP creation	Military Economic Societal Political

Public statements from the military and the Defence Secretary regarding cyber security appear to be less common than those from the Intelligence Agencies or the key Government Departments such as DCMS, and this speech from Michael Fallon had as much to say about civilian aspects of cyber security as they did about any military initiatives which were limited to talking about the creation of the Joint Forces Cyber Group (more than a year old at this point) and generic statements regarding cyber being "*hardwired in to UK defence's DNA*" and military capabilities being upgraded.

However, within the context of an ongoing securitisation process, this speech reinforces the same messages regarding threat and the need for action that is seen in civilian speeches but is reaching a different audience in the military community.

Table 36 Robert Hannigan Speech 10th November 2015

Date	Event	Audience	Securitising Actor
10th Nov 2015	Information Assurance 2015 Conference	Infosec Professionals	Robert Hannigan, Director GCHQ

Speech Act	Referent Objects	Identified Threats	Exceptional Means Demanded	Securitization Categories
"…the cyber threat – one of the greatest challenges of our age…" "…data loss...corrosive to trust in public services…" "…risk both of the highest end destructive attack, and the constant death-by-a-thousand-cuts set of lower level attacks." "…major destructive attacks on media networks…" "…the bulk theft of personal data in the US…" "…cumulative pernicious impact of smaller scale attacks…" "…public confidence in our digital world…" "…standards are not as high as they need to be. Take up of the schemes is not as high as it should be." "…terrorist groups seeking to harness the internet for the most brutal and manipulative propaganda." "….organised crime syndicates trying to disrupt our economy…"	Economy Government Critical National Infrastructure	Hostile States Major organised crime syndicates Terrorist groups	The capability to access information for national security purposes. More capability for automatic defence. Structural features to allow for more automatic protections. Changes to make the market work better Changes to promote cyber security and skills required	Economic Societal Political

This is a key speech in the development of the cyber security discourse over the period as it represents a pivot point from the previous approach of relying on the private sector to deliver cyber security with the encouragement of the Government to the more assertive and interventionist approach that follows.

Many of the key points are posed as questions, in particular the "*two big questions about our cyber security future*" of whether there is more that could be done automatically with built in structural features (a guarded reference to DNS filters), and whether the "*international market for cyber security is working sufficiently well*" making the clear case for a more interventionist approach with references to the failure of the take up rate of cyber security schemes and the failure to reach the standards of security required.

The speech is also noticeable for the extent to which it promotes GCHQ as the solution to cyber security, describing it as their "*security mission*" and claiming that it is "*every bit as much a part of GCHQ's DNA as intelligence gathering*." The speech goes on to emphasis the expertise within GCHQ, the work done with Universal Credit and smart meters, their partnerships with law enforcement in the UK and the US, and to declare as myths, vulnerability hoarding by GCHQ, a desire to ban encryption, or a requirement for backdoors in security products.

Table 37 George Osborne Speech 17th November 2015

Date	Event	Audience	Securitising Actor
17th Nov 2015	Announcement of NCSC	GCHQ	George Osborne (Chancellor)

Speech Act	Referent Objects	Identified Threats	Exceptional Means Demanded	Securitization Categories
"...risk of cyber-attack harming our economy and undermining the confidence on which it rests." "…there will be no economic security for our country without national security. Nowhere is that more true than when it comes to cyber." "For our country, defending our citizens from hostile powers, criminals or terrorists, the Internet represents a critical axis of potential vulnerability." "The stakes could hardly be higher – if our electricity supply, or our air traffic control, or our hospitals were successfully attacked online the impact could be measured not just in terms of economic damage but of lives lost." "ISIL are already using the Internet for hideous propaganda purposes; for radicalisation, for operational planning too. They have not been able to use it to kill people yet by attacking our infrastructure through cyber-attack. They do not yet have that capability but we know they want it and are doing their best to build it." "Imagine the cumulative impact of repeated catastrophic breaches, eroding that basic faith in the Internet that we need for our online economy and social life to function.	Economy Society Critical National Infrastructure	Criminals Hostile Powers Terrorists	Exceptional funding for cyber security Investigatory Powers Act ISPs to provide national level malware detection service Programmes for digital start ups Institute of coding Innovation Centres Defence & Cyber Innovation Fund Regulatory initiatives	Societal Economic

This speech by George Osborne was the announcement of the creation of the NCSC and can be seen as the public affirmation of the change in approach from the 2011 cyber security strategy to the more interventionist 2016 strategy. It is noticeable for the exaggerated threat language and the absolute affirmation that cyber security was a state national security issue with economic security and societal damage of CNI attacks prominent in the threat description, accompanied by reference to the potential for fatalities from terrorist cyber-attacks, and lives lost through CNI attacks. The threat actors were limited to those of realspace national security interest, i.e. terrorists, hostile states, and criminals, again placing cyber security firmly in the same context as realspace security issues.

Table 38 Ciaran Martin Speech 13th September 2016

Date	Event	Audience	Securitising Actor
13th Sept 2016	Billington Cyber Security Conference	US Cyber Security & Government	Ciaran Martin, Chief Executive, NCSC

Speech Act	Referent Objects	Identified Threats	Exceptional Means Demanded	Securitization Categories
"…a highly digitalised economy, which by some measures is the most digitally advanced and therefore, dependant in the world." "We've got hostile states." "They include criminal gangs. Some of these operate under the protection or tolerance of uncooperative states…" "…terrorists, hacktivists and lone operators…the world's major terrorist groups have the intent but not the capability to launch a destructive cyber-attack." "...painful stories of small businesses, lovingly built up, struggling to survive…after a ransomware attack." "...advanced persistent threats, or APTs. They threaten our public services…infrastructure…research…innovation, and much else." "…serious and persistent threat which puts at risk national security and national well-being."	Economy State Society Public Services Small Businesses Infrastructure Innovation Research	Ransomware SQL Injection Hostile States Criminal Gangs Terrorists Hacktivists Lone Operators APTs	BGP & SS7 Protocol Changes DNS Filtering Implementation	Economic Societal Political

Martin's Billington speech is important as his first speech after the formation of the NCSC and his appointment as Chief Executive, but also in that it was delivered in the United States to an audience that included not-only the cyber security industry but also significant figures from the US intelligence community. The speech made a point of emphasising the strength of the relationship with the US, equating GCHQ and the NSA as having both an IA and intelligence function, and emphasising the strength of the relationship. The speech provided a restatement of the threat, and is notable for the specification of the NCSC DNS filtering, BGP and SS7 initiatives.

Table 39 Michael Fallon Speech 21st October 2016

Date	Event	Audience	Securitising Actor
21st Oct 2016	RUSI Cyber Symposium 2016	Defence Analysts	Michael Fallon, Defence Secretary

Speech Act	Referent Objects	Identified Threats	Exceptional Means Demanded	Securitization Categories
"…the more reliant we are on electronic networks the more vulnerable we are to cyber-attack." "…target us anywhere on the planet...not only stealing our information, but exploiting, coercing or gaining psychological advantage over us, but potentially dealing a sucker punch to our systems, potentially disrupting our armaments or our energy supplies, even our governmental systems…"…" "Any threat we face…state sponsored aggression…global terror…attacks on elections…electoral machinery…media and other key features of democracy…lone wolf attacks….any of these can have a cyber dimension. What's more, these threats are growing." "…we must be clear that cyber could constitute an armed attack…while preparing our full spectrum response….and considering what sort of political or public support will be required by such a response."	Military State Critical National Infrastructure	State sponsored aggression Global Terror Attacks on elections Lone wolf attacks	£265 M to 'root out' vulnerabilities in defence systems. Integration of offensive cyber into military capabilities. 77 Brigade and 1st Reconnaissance Brigade. Influence operations, counter hybrid warfare, battlefield intelligence. New Defence Cyber School. Full spectrum response	Military Societal Political

This speech was much more focused than the 2015 speech to the same event a year previously. In particular it was much more specific regarding initiatives in the military sector, in particular the development of 77th Brigade (traditionally responsible for PsyOps, and perhaps typical of the continued conflation of Cyber-Warfare with Information Warfare). As a result it did make clear the military aspects of cyber security and the reference of the integration of offensive cyber into military capabilities is interesting as the majority of offensive cyber capabilities are generally thought to lie with GCHQ.

Table 40 Philip Hammond Speech 1st October 2016

Date	Event	Audience	Securitising Actor
1st Oct 2016	Microsoft Decoded Conference	Information Technology Leadership	Philip Hammond, Foreign Secretary

Speech Act	Referent Objects	Identified Threats	Exceptional Means Demanded	Securitization Categories
"Trust in the Internet and the infrastructure on which it relies is fundamental to our economic future" "…significant consequences including loss of customer data, significant financial costs, disruption of services, reputational damage, indeed threats to the infrastructure of the state itself." "…the precursor to any future state-on-state conflict would be a campaign of escalating cyber-attacks to break down our defences and test our resolve before the first shot is fired." "…these capabilities threaten the security of the UK's critical national infrastructure and our industrial control systems."	Economy State	IoT Botnets Spear Phishing Hostile Foreign Actors	Active Cyber Defence Strengthening Law Enforcement Offensive Cyber Capability Creation of NCSC	Economic Societal Political

This speech was the launch of the 2016 National Cyber Security Strategy, replacing the 2011 – 2015 strategy. It was made to a private sector technology event (the Microsoft Future Decoded Conference) and much of the speech focused on the economic benefits of technology and the transformative effects of technological change before focusing on the need for Britain to be "*a safe place to do digital business.*"

This speech also very clearly conforms to the rhetorical structure of securitisation with articulation of the threats and the effect of not doing anything, specification of exceptional measures and ending with statements of the potential future benefits of a secure digital Britain. Interestingly, there was also specific mention of the Chancellor's political agency in relation to cyber security as the Chair of the permanent Cabinet Cyber Committee, and in his prior role as Foreign Secretary with responsibility for GCHQ.

Table 41 Philip Hammond Speech 14th February 2017

1st Oct 2016	NCSC Opening	NCSC	Philip Hammond, Foreign Secretary

Speech Act	Referent Objects	Identified Threats	Exceptional Means Demanded	Securitization Categories
"…connectivity that will enable the development or the digital economy. Is also a source of vulnerability." "The cyber attacks we are seeing are increasing in their frequency, their severity and their sophistication." "…major attacks on critical national infrastructure…" "Most dramatic threats are the high-end sophisticated State sponsored attacks." "…less sophisticated mass targeted attacks…"	CNI Digital Economy	Electronic data theft Online ransom Phishing Viruses	Business secondments to the NCSC Partnership with business Bringing together intelligence and security agencies with the public and business community.	Economic Societal

This was the launch event for the opening of the NCSC. Previous launch events such as those held for CERT-UK and CiSP for example had included speeches from the Cabinet Office which did not meet the rhetorical structure of a securitising speech act. This speech was different in that it continued the securitisation discourse. However, the focus of the speech was on the potential that the new NCSC offered; emphasising its role in both high-end attacks, but also in raising a general level of capability against day-to-day low-level malicious activity and once again emphasising the need for partnership.

This speech was also notable for including a link between cyber security and the potential of the 'fourth industrial revolution' and the disruption to "*existing patterns of work, life, and society*" that are anticipated results of Artificial Intelligence developments. While not explicitly

stated, it seemed to be implied that getting cyber security right would be fundamental to addressing the challenges of this revolution and ensuring future economic success.

Table 42 Matt Hancock Speech 27th March 2017

27th Mar 2017	IoD Conference	Institute of Directors	Matt Hancock, Minister of Digital & Culture

Speech Act	Referent Objects	Identified Threats	Exceptional Means Demanded	Securitization Categories
"Cyber security is such a crucial part of our modern economy." "The scale of the threat is significant: one in three small firms, and 65% of large businesses are known to have, experienced a cyber breach in the past year." "…a quarter were known to have been attacked once a month" "It is absolutely crucial UK industry is protected against this threat because our economy is a digital economy." "...the costs of a successful attack can be huge…"	UK Industry Digital Economy	Cyber breach Basic known vulnerabilities	"…created the new National Cyber Security Centre…" "...new role in protecting 'the wider economy and society'…" "...all our suppliers which handle sensitive data to hold a Cyber Essentials certificate." "…range of interventions to support the UK's cyber security ecosystem…" "...cyber security skills strategy…"	Economic Societal

This speech was significant as the first cyber security specific speech aimed at the business community and the contents are very much tailored to that audience. There is little technical detail, and references to cyber threats are limited to generic "breach" or "attack". In line with the audience, the emphasis is on business adopting the Cyber Essentials scheme to 'get the basics right', and the costs of cyber attacks to business within the context of UK industry and the digital economy as referent objects.

Exceptional measures include a restatement of the creation of the NCSC, but with an emphasis on its expanded role to address the wider economy and society. There are a number of spending priorities mentioned, including the skills strategy and the various cyber security business incentives. There are also indications of pressure being brought bear on the business community with mention of the mandatory

nature of Cyber Essentials for some government suppliers, the expansion of that into the supply chain of large organisations, and the introduction of GDPR.

Table 43 Ciaran Martin Speech 13th September 2017

13th Sept 2017	Confederation of British Businesses Conference	British Business	Ciaran Martin, CEO, NCSC

Speech Act	Referent Objects	Identified Threats	Exceptional Means Demanded	Securitization Categories
"…the big state threat, traditional espionage with a modern twist that can now affect our democracy, our critical national infrastructure and the lens through which we view the world." "...the threat to prosperity from an aggregation of cyber-attacks that would damage consumer confidence." "…if trust in online services is lost, or if hundreds of thousands of data breaches become commonplace, that confidence is undermined permanently and fatally."	CNI Democracy Digital Economy	State attacks Small scale cyber attacks Data breaches Ransomware (wannacry)	"…secret intelligence capabilities combined with partnerships with law enforcement, other governments and global industry…" Compliance with new regulation. GDPR Active Cyber Defence partnerships Re-evaluation of corporate security policies Boardroom conversations on cyber Education of individual employees Acceptance of NCSC framework	Economic Societal Political

This was an interesting speech in several ways. First it was heavily tailored to the audience in that it was focused on the business community in terms of the types of threats that would resonate with that community and was asking for corporate leaders to engage with GDPR, user-driven security policies and the NCSC frameworks. Second, the language was clearly adjusted to that community and there was significantly less 'technospeak' and Martin goes out of the way to position himself as a non-technical person dependant on the people who work for him, asking the type of questions he wants his audience to ask their own cyber security staff. This reflects some of the concerns among the cyber security community that they are unable to get their message across to the 'C suite'.

Third, it contained clear messages concerning where the corporate community was failing to deliver its part of the national security imperative of cyber security, in particular focusing on the need for boardroom level discussions on cyber security and the need for businesses to educate the individuals within their organisation.

Table 44 Ciaran Martin Speech 14th September 2017

14th Sept 2017	EU Cyber Security Conference	European Cyber Organisations	Ciaran Martin, CEO, NCSC

Speech Act	Referent Objects	Identified Threats	Exceptional Means Demanded	Securitization Categories
"…common threat to our shared values of freedom, democracy, and prosperity through free enterprise, all underpinned by the rule of law." "….the threat to prosperity from the large scale theft of intellectual property from other states." "…threat to our citizens from the constant, unsophisticated but prolific attacks from criminals that threaten confidence in the digital economy."	freedom democracy prosperity rule of law democracies critical services prosperity citizens confidence in the digital economy	Unsophisticated cyber attacks (Wannacry) Cloudhopper Mirai botnet Global threats	"…to use what capabilities we have, to help cyber security not just of the UK but also of our European friends." To continue to work with the EU on strategic frameworks, legislation and standards, encourage cross border R&D collaboration and industry development. To continue to collaborate through the CSIRT network.	Economic Societal Political

This speech was delivered in the context of Brexit and was given just two days after the release of the UK Government's paper setting out the UKs Defence and Security Relationship with the EU post Brexit and is notable for a number of reasons.

First, it is based on an appeal to common shared values with the other EU member nation states and emphasises the shared threat and the global nature of the cyber security challenge using the Cloudhopper and Mirai botnet attacks as evidence that a global response is required. Second, the strength of the UK's relationships outside the UK is offered as part of the partnership with the EU along with specific UK developments that could aid a Europe wide solution along with direct reference to the disparity in spend between the USA and Europe on cyber security. Third, many of the exceptional means demanded are, in effect, an appeal to continue with the status quo, in that they are based

on a desire to continue current EU cooperation after Brexit. Finally, the speech emphasises the successes of the UK from the "radically different and more interventionist approach" and the suggestion that this could lead to more being done together with the EU.

Table 45 Ciaran Martin Speech 15th November 2017

14th Sept 2017	Times Technology Summit	British Business	Ciaran Martin, CEO, NCSC

Speech Act	Referent Objects	Identified Threats	Exceptional Means Demanded	Securitization Categories
"…Russian interference, seen by the NCSC, has included attacks on the UK media, telecommunications and energy sectors." "Russia is seeking to undermine the international system.....international order as we know it is in danger of being eroded." "Attacks that do damage to individual corporations and people's confidence in the digital economy."	CNI Democracy Digital Economy	Hostile states Rampant criminality	Acquiring information from corporations on plans and actions Acceptance of NCSC frameworks Technical defences at scale DMARC Corporations to focus on reducing vulnerabilities, leaving NCSC free to deal with state attacks	Economic Societal Political

This speech was similar in audience, style, and content to the CBI speech in September, and as such can be seen as a reaffirmation of the messages from that earlier CBI speech. The main messages were that businesses needed to "*get the basic right*" in order to allow the NCSC to focus on the issues that could only be addressed by the state. It was also stated that the NCSC required greater input from the business community to ensure that the advice it was providing was useful.

Appendix B: Bibliography

Aberdach, J. D. and Rockman, B. A. (2002) 'Conducting and Coding Elite Interviews', *Political Science and Politics*, 35(4), pp. 673–676.

Ablon, L. and Bogart, A. (2017) *Zero Days , Thousands of Nights The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. doi: 10.7249/RR1751.

Ackerman, S. (2013) *Cyber-attacks eclipsing terrorism as gravest domestic threat – FBI*, *The Guardian*. Available at: https://www.theguardian.com/world/2013/nov/14/cyber-attacks-terrorism-domestic-threat-fbi.

Adams, J. and Albakajai, M. (2016) 'Cyberspace: A New Threat to the Sovereignty of the State', *Management Studies*, 4(6), pp. 256–265. doi: 10.17265/2328-2185/2016.06.003.

Afifi-Sabat, K. (2018) *Companies "over-reporting" data breaches as ICO takes 500 calls per week*, *IT Pro*. Available at: https://www.itpro.co.uk/information-commissioner/31912/companies-over-reporting-data-breaches-as-ico-takes-500-calls-per (Accessed: 28 January 2019).

Agari (2017) *Agari Global DMARC Adoption Report: Open Season for Phishers*, *Agari Web Site*. Available at: https://www.agari.com/wp-content/uploads/2017/08/Agari_DMARC_Adoption_Report_PR1.pdf.

Aguilar, L. A. (2015) *The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses*, *U.S. Securities and Exchange Commission Web Site*. Available at: https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html#_edn6 (Accessed: 20 September 2018).

Aiken, M. (2016) *The Cyber Effect*. London: John Murray.

Alexander, K., Kupreev, O. and Badovskaya, E. (2018) *DDOS attacks in Q1 2018*, *SecureList, Kapersky Lab*. Available at: https://securelist.com/ddos-attacks-in-q1-2017/78285/ (Accessed: 28 June 2018).

Allcott, H. and Gentzkow, M. (2017) 'Social Media and Fake News in the 2016 Election', *Journal of Economic Perspectives*, 31(2), pp. 211–236. doi: 10.1257/jep.31.2.211.

Amazon Web Services Inc. (2017) *AWS: Global Infrastructure*. Available at: http://aws.amazon.com/about-aws/globalinfrastructure/ (Accessed: 15 November 2017).

Ammous, S. (2017) *Bitcoin and the Disintermediation of the State*, *American Institute for Economic Research: Research Briefs*. Available at: https://www.aier.org/research/bitcoin-and-disintermediation-state (Accessed: 17 October 2017).

Arbour Security Engineering and Response Team (2018) *OMG – Mirai Minions are Wicked*, *Netscout Web Site*. Available at: https://asert.arbornetworks.com/omg-mirai-minions-are-wicked/ (Accessed: 20 June 2018).

Armstrong, S. (2017) *Catalonia plots digital government in exile in bid for independence*, *Wired*. Available at: http://www.wired.co.uk/article/catalan-government-independence-internet-

spain.

Arthur, W. B. (1989) 'Competing Technologies, Increasing Returns, and Lock-In by Historical Events', *The Economic Journal*, 99(March), pp. 116–131. Available at: http://www.haas.berkeley.edu/Courses/Spring2000/BA269D/Arthur89.pdf.

Ashford, W. (2016) *RSAC16: UK government to change tack on cyber security*, *Computer Weekly*. Available at: http://www.computerweekly.com/news/4500277866/RSAC16-UK-government-to-change-tack-on-cyber-security (Accessed: 9 January 2017).

Ashford, W. (2017) *EternalRocks worm combines seven leaked NSA attack tools*, *Computer Weekly*. Available at: https://www.computerweekly.com/news/450419337/EternalRocks-worm-combines-seven-leaked-NSA-attack-tools (Accessed: 20 June 2018).

Assange, J. (2012) *Cypherpunks: Freedom and the Future of the Internet*. Paperback. London & New York: OR Books.

Australian Public Service Commission (2007) *Tackling wicked problems: A public policy perspective*, *Commonwealth of Australia*. doi: 10.4324/9781849776530.

Bain, W. (2017) *Medieval Foundations of International Relations*. Abingdon: Routledge.

Balzacq, T. (2005) 'The Three Faces of Securitization: Political Agency, Audience and Context', *European Journal of International Relations*, 11(2), pp. 171–201. doi: 10.1177/1354066105052960.

Barakso, M., Sabet, D. M. and Schaffner, B. (2014) *Understanding Political Science Research Methods: The Challenge of Inference*. Abingdon: Routledge.

Barlow, J. P. (1996) *A Declaration of the Independence of Cyberspace.*, *Humanist*. doi: 10.5860/CHOICE.48-1189.

Baron, J. *et al.* (2015) *National Security Implications of Virtual Currency*. doi: 10.7249/RR1231.

Bartholomew, B. and Guerrero-Saade, J. . (2016) *Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks*. Available at: https://fortunascorner.com/wp-content/uploads/2016/10/Bartholomew-GuerreroSaade-VB2016.pdf (Accessed: 1 October 2018).

Bartlett, J. (2014) *The Dark Net: Inside the Digital Underworld*. London: William Heinemann.

Barysevich, A. (2016) *Inside the Mind of Cybercriminals*, *Recorded Future Blog*. Available at: https://www.recordedfuture.com/cyber-criminal-profiling/ (Accessed: 28 December 2017).

Baylon, C., Brunt, R. and Livingstone, D. (2015) 'Cyber Security at Civil Nuclear Facilities Understanding the Risks', *Chatham House*, p. 53. doi: ISBN 978 1 78413 079 4 A.

BBC (2016) *Boy, 17, admits TalkTalk hacking offences - BBC News*, *BBC Online*. Available at: http://www.bbc.co.uk/news/uk-37990246 (Accessed: 23 May 2018).

BBC (2017) *Privacy regulator warns MPs over shared passwords Left unlocked*, *BBC News*. Available at: http://www.bbc.co.uk/news/technology-42225214 (Accessed: 25 May 2018).

BBC News (2000) *Napster shut down*, *BBC News OnlineNews Online*. Available at:

http://news.bbc.co.uk/1/hi/852283.stm (Accessed: 23 January 2018).

BBC News (2018) *Facebook: No new evidence of Russian meddling in Brexit vote*, *BBC News*. Available at: https://www.bbc.co.uk/news/uk-politics-43229969 (Accessed: 3 July 2018).

Beard, M. (2016) 'Beyond Tallinn: The Code of the Cyber Warrior', in Allhoff, F., Henschke, A., and Strawser, B. J. (eds) *Binary Bullets: The Ethics of Cyber Warfare*. Oxford: Oxford University Press, pp. 139–156.

Beaumont, K. (2017) *Regarding Marcus Hutchins aka MalwareTech*, *Double PUlsar BLog*. Available at: https://doublepulsar.com/regarding-marcus-hutchins-aka-malwaretech-650c99e96594 (Accessed: 21 September 2018).

Belk, R. and Noyes, M. (2012) *On the Use of Offensive Cyber Capabilities*. Harvard. Available at: http://live.belfercenter.org/files/cybersecurity-pae-belk-noyes.pdf.

Bencsáth, B. *et al.* (2012) 'The cousins of Stuxnet: Duqu, Flame, and Gauss', *Future Internet*, 4(4), pp. 971–1003. doi: 10.3390/fi4040971.

Bendrath, R. (2007) 'The Return of the State in Cyberspace', in Dunn, M., Krishna-Hensel, S. F., and Mauer, V. (eds) *The Resurgence of the State: Trends and Processes in Cyberspace Governance*. Aldershot: Ashgate, pp. 111–152.

Berry, J. M. (2002) 'Validity and Reliability Issues in Elite Interviewing', *Politic Science and Politics*, 35(4), pp. 679–682.

Betts, R. (2013) 'The Lost Logic of Deterrence', *Foreign Affairs*. Available at: https://www.foreignaffairs.com/articles/united-states/2013-02-11/lost-logic-deterrence.

Betz, D. (2012) 'Cyberpower in Strategic Affairs: Neither Unthinkable or Blessed', *Journal of Strategic Studies*, 35(5), pp. 689–711. doi: 10.1080/01402390.2012.706970.

Betz, D. and Stevens, T. (2011) *Cyberspace and the State: Toward a Strategy for Cyber Power*. Kindle. Abingdon: Routledge.

Bhutani, A. and Wadhwani, P. (2019) *Global Cyber Security Market Size to surpass $300bn by 2024*, *Global Market Insights*. Available at: https://www.gminsights.com/pressrelease/cyber-security-market (Accessed: 28 March 2019).

Bienkov, A. (2018) *Theresa May accuses Facebook of helping terrorists, child abusers, and slave traders*. Available at: http://uk.businessinsider.com/theresa-may-davos-speech-facebook-terrorism-child-abuse-slavery-2018-1 (Accessed: 9 February 2018).

Birch, S. (2015) *IBM's CEO on hackers: "Cyber crime is the greatest threat to every company in the world"*, *IBM Web Site*. Available at: https://www.ibm.com/blogs/nordic-msp/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/ (Accessed: 13 March 2019).

Blitz, J. (2013) *UK becomes first state to admit to offensive cyber attack capability*, *Financial Times*. London. Available at: https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de?mhq5j=e7 (Accessed: 2 October 2017).

Bodmer, S. *et al.* (2012) *Reverse Deception: Organised Cyber Threat Counter-Exploitation*. New

York: McGraw Hill.

Bohannon, J. (2016) *Who's downloading pirated papers? Everyone*, *Science*. Available at: http://www.sciencemag.org/news/2016/04/whos-downloading-pirated-papers-everyone.

Booth, K. (1991) 'Security and Emancipation', *Review of International Studies*, 117, pp. 313–326.

Booz Allen Hamilton (2011) 'Cyber Power Index', pp. 1–36. Available at: papers3://publication/uuid/567637EE-E478-4634-908E-72E08A1EF0B8.

Botsman, R. (2017) *Who Can You Trust? How Technology Brought Us Together - and Why It Could Drive Us Apart*. London: Penguin Random House.

Boyatzis, R. (1998) *Transforming Qualitative Information: Thematic Analysis and Code Development*. London: SAGE Publications.

Brantly, A. F. (2018) 'The cyber deterrence problem', *International Conference on Cyber Conflict, CYCON*, 2018-May, pp. 31–53. doi: 10.23919/CYCON.2018.8405009.

Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative Research in Psychology*, 3(2), pp. 77–101. doi: 10.1191/1478088706qp063oa.

BRC (2018) *BRC Cyber Security Toolkit: A Guide for Retailers*, *BRC Web Site*. Available at: https://brc.org.uk/media/382900/brc-cyber-security-toolkit-final.pdf (Accessed: 1 April 2019).

Brenner, J. (2011) *America the Vulnerable*. New York: Penguin.

Brenner, S. W. (2006) *Cybercrime jurisdiction*, *Crime, Law and Social Change*. doi: 10.1007/s10611-007-9063-7.

Brenner, S. W. (2007a) '" At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare', *The Journal of Criminal Law and Criminology*, 97(2), pp. 379–476. doi: 0091-4169/07/9702-0379.

Brenner, S. W. (2007b) 'Private-public sector cooperation in combating cybercrime: In search of a model', *Journal of International Commercial Law and Technology*, 2(2), pp. 58–67.

Brenner, S. W. (2013) 'Cyber-threats and the Limits of Bureaucratic Control', *Minnesota Journal of Law, Science & Technology*, 14(2009), pp. 137–258.

Brenner, S. W. (2014) *Cyberthreats and the Decline of the Nation State*. Abingdon: Routledge.

Brenner, S. W. and Clarke, L. (2005) 'Distributed security: A new model of law enforcement', *John Marshall Journal of Computer & Information Law, Forthcoming*, (June).

Brenner, S. W. and Clarke, L. (2010) *Civilians in Cyberwarfare: Casualties*. Available at: https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/BrennerClarke.pdf.

Brenner, S. W. and Clarke, L. (2014) 'Civilians in cyberwarfare: Conscripts', *Vanderbilt Journal of Transitional Law*, 43(4), pp. 1–54.

Brown, C. S. D. (2015) 'Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice', *International Journal of Cyber Criminology*, 9(1), pp. 55–119. doi: 10.5281/zenodo.22387.

Bryman, A. (2016) *Social Research Methods*. Fifth Edit. Oxford: Oxford University Press.

Buchanan, B. (2016) *The Cyber Security Dilemma*. London: Hurst & Company.

Buchanan, B. (2017) 'The Legend of Sophistication in Cyber Operations', *Belfer Centre for Science and International Affairs, Harvard Kennedy School*. Available at: https://www.belfercenter.org/sites/default/files/files/publication/Legend Sophistication - web.pdf.

Bull, H. (1977) *The Anarchical Society: A Study of Order in World Politics*. Fourth Edi. Basingstoke: Palgrave Macmillan.

Burgess, M. (2017) *What is the Petya ransomware spreading across Europe? WIRED explains*, *Wired*. Available at: http://www.wired.co.uk/article/petya-malware-ransomware-attack-outbreak-june-2017 (Accessed: 20 June 2018).

Burgess, M. (2018) *Where the UK's investigations into Russia's Brexit meddling stand*, *Wired*. Available at: http://www.wired.co.uk/article/russia-brexit-influence-uk-twitter-facebook-google (Accessed: 3 July 2018).

Buzan, B., Waever, O. and de Wilde, J. (1998) *Security: A New Framework for Analysis*. London: Lynne Rienner Publishers.

Cabinet-Office (2011) 'The UK Cyber Security Strategy Protecting and promoting the UK in a digital world', *[Online] at: https://www.gov.uk/*, (November), pp. 1–42. doi: 10.1109/MC.2013.72.

Cabinet Office (2008) *The National Security Strategy of the United Kingdom - Security in an interdependent world*. London. Available at: https://www.gov.uk/government/publications/the-national-security-strategy-of-the-united-kingdom-security-in-an-interdependent-world.

Cabinet Office (2009) *Cyber Security Strategy of the United Kingdom*. Available at: http://webarchive.nationalarchives.gov.uk/+/http:/www.cabinetoffice.gov.uk/media/216620/css0906.pdf.

Cabinet Office (2012) 'Government Digital Strategy', (November), pp. 1–52. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/296336/Government_Digital_Stratetegy_-_November_2012.pdf.

Carr, M. (2016) 'Public – private partnerships in national cyber-security strategies', *International Affairs*, 1, pp. 190–209. doi: 10.1111/1468-2346.12504.

Carr, M. (2017) 'Cyberspace and International Order', in Sugunami, H., Carr, M., and Humphreys, A. (eds) *The Anarchical Society at 40*. Oxford University Press, pp. 162–178.

Castells, M. (2001) *The Internet Galaxy*. Oxford: Oxford University Press.

Castro, D. and Mcquinn, A. (2016) 'Unlocking Encryption : Information Security and the Rule of Law', *Information Technology and Innovation Foundation*, (March), pp. 1–50.

CCHS (2016) *Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats.*, *Center for Cyber & Homeland Security*. Washington, DC. Available at:

https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

Cerny, P. G. (1998) 'Neomedievalism, civil war and the new security dilemma: Globalisation as durable disorder', *Civil Wars*, 1(1), pp. 36–64. doi: 10.1080/13698249808402366.

CERT-EU (2017) *WannaCry Ransomware Campaign Exploiting SMB Vulnerability*. Available at: https://cert.europa.eu/static/SecurityAdvisories/2017/CERT-EU-SA2017-012.pdf (Accessed: 16 March 2018).

CESG (2012) *Cyber security guidance for business*, *Gov.UK Web Site*. Available at: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility (Accessed: 5 March 2018).

Chandler, M. (2012) *Huawei and Cisco's Source Code: Correcting the Record*, *Cisco Blog*. Available at: https://blogs.cisco.com/news/huawei-and-ciscos-source-code-correcting-the-record (Accessed: 2 October 2018).

Chang, L. Y. and Grabosky, P. (2017) 'The Governance of Cyberspace', in Drahos, P. (ed.) *Regulatory Theory*. Paperback. Acton, Australia: ANU Press, pp. 533–544.

Cheshire, T. (2017) *WhatsApp rejected Government request to access encrypted messages*, *Sky News Web Site*. Available at: https://news.sky.com/story/whatsapp-denies-government-access-to-encrypted-messages-11043069 (Accessed: 27 June 2018).

Chirgwin, R. (2018) *Microsoft Germany emerging from behind Deutsche Telekom cloud*, *The Register*. Available at: https://www.theregister.co.uk/2018/09/04/microsoft_germany_emerging_from_behind_deutsche_telekom_cloud/ (Accessed: 2 October 2018).

Choucri, N. (2012a) *Cyberpolitics in International Relations*. Cambridge, MA: MIT Press.

Choucri, N. (2012b) 'Emerging Trends in Cyberspace : Dimensions & Dilemmas', *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition*, pp. 1–19. Available at: hhttps://nchoucri.mit.edu/cyberspace-cyberpolitics.

Churchman, C. W. (1967) 'Wicked problems [Guest Editorial]', *Management Science*, 14(4), pp. B141–B142. doi: 10.1366/000370209787169876.

Clark, D. (1992) 'A Cloudy Crystal Ball - Visions of the Future', in *Proceedings of the Twenty-Fourth Internet Engineering Task Force*. Available at: http://www.ietf.org/proceedings/24.pdf%3E.

Clarke, R. (2005) *Ten Years Later*, *The Atlantic*. Available at: https://www.theatlantic.com/magazine/archive/2005/01/ten-years-later/303659/ (Accessed: 3 July 2018).

Clarke, R. and Knake, R. (2010) *Cyber War: The Next Threat to National Security and What to Do About it*. New York: Harper Collins.

Clemente, D. (2011) 'Cyber Security As A Wicked Problem', *The World Today*, 67(October), pp. 15–17.

Cobb, M. (2016) *Why signature-based detection isn't enough for enterprises*, *Tech Target*. Available at: http://searchsecurity.techtarget.com/tip/Why-signature-based-detection-isnt-enough-for-enterprises (Accessed: 29 December 2017).

Cohen, J. E. (2007) 'Cyberspace as/and Space', *Colombia Law Review*, 107(1), pp. 219–256. Available at: www.jstor.org/stable/40041711.

Collins, K. (2017) *UK's flip-flops on encryption don't help anyone*. Available at: https://www.cnet.com/uk/news/british-government-amber-rudd-flip-flops-on-encryption/ (Accessed: 12 June 2018).

Committee on the National Security Strategy, J. (2018) 'Cyber Security Skills and the UK's Critical National Infrastructure', (July). Available at: www.parliament.uk/jcnss.

Corera, G. (2015) *Intercept: The Secret History of Computers and Spies*. London: Weidenfeld and Nicolson.

Corera, G. (2016) *How France's TV5 was almost destroyed by 'Russian hackers'*, *BBC News*. Available at: http://www.bbc.co.uk/news/technology-37590375 (Accessed: 5 December 2016).

Corfield, G. (2017) *British snoops at GCHQ knew FBI was going to arrest Marcus Hutchins*, *The Register*. Available at: https://www.theregister.co.uk/2017/08/21/gchq_knew_marcus_hutchins_risked_arrest_fbi/ (Accessed: 1 January 2018).

Corfield, G. (2018) *Techies! Britain's defence secretary wants you – for cyber-sniping at Russia*, *The Register*. Available at: https://www.theregister.co.uk/2018/05/01/ukgov_wants_techies_join_the_army/ (Accessed: 3 July 2018).

Cornish, P. *et al.* (2011) *Cyber Security and the UK's Critical National Infrastructure*.

Cornish, P. (2015) 'Governing cyberspace through constructive ambiguity', *Survival*, 57(3), pp. 153–176. doi: 10.1080/00396338.2015.1046230.

Council of Europe (2018) *Chart of signatures and ratifications of Treaty 185*, *Council of Europe Web Site*. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?desktop=true (Accessed: 20 August 2018).

Cox, J. (2015) *Police Agencies Are Getting Cozy with Private Security Companies*, *Motherboard*. Available at: https://motherboard.vice.com/en_us/article/gvyzxy/police-agencies-are-getting-cozy-with-private-security-companies (Accessed: 16 March 2018).

Crowdstrike (2016) *Who is FANCY BEAR?*, *Crowdstrike.com*. Available at: https://www.crowdstrike.com/blog/who-is-fancy-bear/ (Accessed: 22 February 2018).

Crown Prosecution Service (2017) *Hacker sentenced for cyber-attacks on high-profile companies*, *CPS Web Site*. Available at: https://www.cps.gov.uk/west-midlands/news/hacker-sentenced-cyber-attacks-high-profile-companies (Accessed: 28 June 2018).

Crown Prosecution Service (2018) *Hacker admits international cyber attacks*, *CPS Web Site*. Available at: https://www.cps.gov.uk/cps/news/hacker-admits-international-cyber-attacks (Accessed: 28 June 2018).

Curtis, J. (2017) *Mirai : Trio confesses to creating the world's most powerful DDoS botnet*, *ITPRO*. Available at: http://www.itpro.co.uk/distributed-denial-of-service-ddos/30150/mirai-trio-confesses-to-creating-the-worlds-most-powerful (Accessed: 28 June 2018).

Cushman & Wakefield (2016) *Data Centre Risk Index 2016*. London. Available at: http://www.cushmanwakefield.com/en/research-and-insight/2016/data-centre-risk-index-2016/.

Daviter, F. (2017) 'Coping, taming or solving: alternative approaches to the governance of wicked problems', *Policy Studies*. Taylor & Francis, 38(6), pp. 571–588. doi: 10.1080/01442872.2017.1384543.

DeGrace, P. and Stahl, L. H. (1991) *Wicked Problems, Righteous Solutions: A Catalogue of Modern Software Engineering Paradigms*. Englewood Cliffs, NJ: Prentice-Hall (Yourdon Press).

Deibert, R. *et al.* (eds) (2010a) *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press.

Deibert, R. *et al.* (eds) (2010b) *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.

Deibert, R. J. (2013) *Black Code*. Toronto: McClelland and Stewart.

Demchak, C. and Dombrowski, P. (2014) 'Cyber Westphalia: Asserting State Prerogatives in Cyberspace', *Georgetown Journal of International Affairs*, pp. 29–38.

Demchak, C. and Dombrowski, P. J. (2011) 'Rise of a Cybered Westphalian Age: The Coming Decades', *Strategic Studies Quarterly*, 5(Spring), pp. 91–113. doi: 10.1007/978-3-642-55007-2_5.

DeNardis, L. (2014) *The Global War for Internet Governance*. London: Yale University Press.

Denardis, L. and Musiani, F. (2014) 'Governance by Infrastructure', *The Turn to Infrastructure in Internet Governance*, pp. 1–31. doi: 10.1057/9781137483591_1.

Denmark, A. M. and Mulvenon, J. (2010) *Contested Commons: The Future of American Power in a Multipolar World*, *Contested Commons : The Future of American Power in a Multipolar World*. Washington, DC.

Denning, D. E. (2015) 'Rethinking the Cyber Domain and Deterrence', *Joint Force Quarterly*, 77(April), pp. 8–15.

Denning, P. (2007) 'Mastering the mess', *Communications of the ACM*, 50(April), p. 21. doi: 10.1145/1232743.1232763.

Denning, P. (2009) 'Resolving Wicked Problems through Collaboration', in Whitworth, B. and Moor, A. de (eds) *Handbook of Research on Socio-Technical Design and Social Networking Systems*. Hersey, PA: IGI Global, pp. 715–730. doi: 10.4018/978-1-60566-264-0.

Denning, P. and Denning, D. (2016) 'Cybersecurity is harder than building bridges', *American Scientist*, 104(3), pp. 154–157.

Dexter, L. A. (1970) *Elite and Specialized Interviewinig*. Evanston, IL: Northwestern University Press.

DHS and FBI (2016) *GRIZZLY STEPPE – Russian Malicious Cyber Activity Summary*, *US CERT Web Site*. Available at: https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY STEPPE-2016-1229.pdf (Accessed: 3 July 2018).

Diez, T., Albert, M. and Stetter, S. (2006) *The European union and border conflicts: The power of integration and association*, *The European Union and Border Conflicts: The Power of Integration and Association*. Edited by T. Diez, M. Albert, and S. Stetter. Cambridge: Cambridge University Press. doi: 10.1017/CBO9780511491337.

DoD Press Operations (2002) 'DoD News Briefing Secretary Rumsfeld and Gen. Myers February 12, 2002 11.30 AM EDT', *Defense.gov*. Available at: http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636.

Donohoe, J. (2018) *Facebook opens €300m Clonee data centre*, *The Irish Times*. Available at: https://www.irishtimes.com/business/technology/facebook-opens-300m-clonee-data-centre-1.3628532 (Accessed: 15 April 2019).

Dunlap, C. J. (2013) 'Some reflections on the intersection of law and ethics in cyber war', *Air and Space Power Journal*, 27(1), pp. 22–43.

Dunn-Cavelty, M. and Mauer, V. (2007) 'The Role of the State in Securing the Information Age - Challenges and Prospects', in Dunn, M., Maue, V., and Krishna-Hensel, S. F. (eds) *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*. Aldershot: Ashgate.

Easterbrook, F. H. (1996) 'Cyberspace and the Law of the Horse', *University of Chicago Legal Forum*, 207, pp. 207–216. doi: 10.1525/sp.2007.54.1.23.

Edelman, B. G. and Luca, M. (2014) *Digital Discrimination: The Case of Airbnb.com*, *Harvard Business School*. doi: 10.2139/ssrn.2377353.

Edelman, B. G., Luca, M. and Svirsky, D. (2015) *Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment*, *Harvard Business School*. doi: 10.2139/ssrn.2701902.

Egloff, F. (2015) 'Cybersecurity and the Age of Privateering: A Historical Analogy.', *Cyber Studies programa - University of Oxford*, (1), p. 14.

Eichensehr, K. E. (2017) 'Public-Private Cybersecurity', *Texas Law Review*, 95(3), pp. 467–538.

Electronic Frontier Foundation (2014) *The Crypto Wars: Governments Working to Undermine Encryption*, *EFF Web Site*. Available at: https://www.eff.org/document/crypto-wars-governments-working-undermine-encryption (Accessed: 5 March 2019).

Elmer-Dewitt, P. (1993) 'First Nation in Cyberspace', *Time*, (49), pp. 23–24. Available at: http://content.time.com/time/magazine/article/0,9171,979768,00.html.

European Union (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da*, *Official Journal of the European Union*. doi: L:2016:119:TOC.

Evans, J. (2012) *The Olympics and Beyond*. Available at: https://www.mi5.gov.uk/news/the-olympics-and-beyond (Accessed: 13 October 2017).

Facebook (2017a) *Odense Data Centre*. Available at: https://www.facebook.com/OdenseDataCenter/ (Accessed: 15 November 2017).

Facebook (2017b) *Our Mission*, *Facebook Newsroom*. Available at: https://newsroom.fb.com/company-info/ (Accessed: 15 November 2017).

Fafinski, S., Dutton, W. H. and Margetts, H. (2010) 'Mapping and Measuring Cybercrime', (18), pp. 1–26.

Fakhreddine, A. (2018) *State of the Internet Summer 2018 Attack Spotlight: What you need to know*, *Akamai Blog*. Available at: https://blogs.akamai.com/sitr/2018/06/state-of-the-internet-summer-2018-attack-spotlight-what-you-need-to-know.html (Accessed: 28 June 2018).

Falk, R. (2002) 'The Post Westphalia Enigma', in Hettne, B. and Oden, B. (eds) *In Search od World Order*. Stockholm: Almquiest & Wiksell Intl, pp. 147–183.

Fallon, M. (2015) *Cyber Symposium 2015*, *Gov.UK Web Site*. Available at: https://www.gov.uk/government/speeches/cyber-symposium-2015 (Accessed: 18 May 2018).

Fallon, M. (2016) *Defence Secretary's speech at the second RUSI Cyber Symposium*. Available at: https://www.gov.uk/government/speeches/defence-secretarys-speech-at-the-second-rusi-cyber-symposium (Accessed: 13 October 2017).

Fallon, M. (2017) *Defence Secretary's speech at Cyber 2017 Chatham House Conference - GOV.UK*. Available at: https://www.gov.uk/government/speeches/defence-secretarys-speech-at-cyber-2017-chatham-house-conference (Accessed: 18 May 2018).

Farrell, S. (2016) *TalkTalk counts costs of cyber attack*, *The Guardian*. Available at: https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave (Accessed: 27 June 2018).

Fenton, J. (2013) '5 Myths of Two-Factor Authentication', *Wired*, April, pp. 2–7. Available at: https://www.wired.com/insights/2013/04/five-myths-of-two-factor-authentication-and-the-reality/.

Field, M. (2018) *WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled*, *The Telegraph*. Available at: https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/ (Accessed: 1 April 2019).

Fierke, K. M. (2013) 'Constructivism', in Dunne T., Kurki, M., Smith, S. (ed.) *International Relations Theories: Discipline & Diversity*. 4th edn. Oxford: Oxford University Press, pp. 161–178.

Financial Times (2018) *Online retail sales continue to soar*, *Financial Times Web Site*. Available at: https://www.ft.com/content/a8f5c780-f46d-11e7-a4c9-bbdefa4f210b (Accessed: 25 June 2018).

FinFisher (2017) *Cyber Solutions for the Fight Against Crime*. Available at: http://www.finfisher.com/FinFisher/index.html (Accessed: 12 September 2017).

FireEye (2018a) *2018 Mega Trends*, *FireEye Web Site*. Available at: https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf (Accessed: 20 June 2018).

FireEye (2018b) *Advanced persistent threat*, *FireEye Web Site*. Available at: https://www.fireeye.com/current-threats/apt-groups.html (Accessed: 22 February 2018).

Fleming, J. (2018a) *Director GCHQ speaks at Billington Cyber Security Summit*, *GCHQ Web Site*. Available at: https://www.gchq.gov.uk/news-article/director-gchq-speaks-billington-cyber-security-summit (Accessed: 28 September 2018).

Fleming, J. (2018b) *Director GCHQ Speech at CyberUK 18*, *GCHQ Web Site*. Available at: https://www.gchq.gov.uk/sites/default/files/Director CyberUK2018 As Delivered.pdf (Accessed: 14 February 2019).

Francis, R. (2016) *Hire a DDoS service to take down your enemies*, *CSO Online*. Available at: https://www.csoonline.com/article/3180246/data-protection/hire-a-ddos-service-to-take-down-your-enemies.html (Accessed: 28 June 2018).

Franzese, P. (2009) 'Sovereignty in Cyberspace: Can it exist?', *Air Force Law Review*, 64(1).

Friedrichs, J. (2001) 'The Meaning of New Mediaevalism', *European Journal of International Relations*, 7(4), pp. 475–502.

Friis, K. and Reichborn-Kennerud, E. (2016) 'From Cyber Threats to Cyber Risks', in Friis, K. and Ringsmose, J. (eds) *Conflict in Cyberspace: Theoretical ,Strategic and Legal Persepectives*. Abingdon: Routledge, pp. 27–44.

Friis, K. and Ringsmose, J. (eds) (2016) *Conflict in Cyberspace: Theoretical, strategic, and legal perspectives*. Abingdon: Routledge.

Fruhlinger, J. (2018a) *The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet*, *CSO Online*. Available at: https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html (Accessed: 25 June 2018).

Fruhlinger, J. (2018b) *What is WannaCry ransomware, how does it infect, and who was responsible?*, *CSO Online Web Site*. Available at: https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html (Accessed: 5 March 2019).

Gallagher, R. (2014) *OPERATION SOCIALIST: The Inside Story of How British Spies Hacked Belgium's Largest Telco*, *The Intercept*. Available at: https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/ (Accessed: 11 January 2017).

Gallagher, R. (2018) *How UK Spies Hacked a European Ally and Got Away With It*, *The Intercept*. Available at: https://theintercept.com/2018/02/17/gchq-belgacom-investigation-europe-hack/ (Accessed: 20 February 2018).

Gallagher, S. (2014) *Photos of an NSA "upgrade" factory show Cisco router getting implant*, *Ars Technica*. Available at: https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/ (Accessed: 27 September 2018).

Gambino, L., Siddiqui, S. and Walker, S. (2016) *Obama expels 35 Russian diplomats in retaliation for US election hacking | US news | The Guardian*, *The Guardian*. Available at:

https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack (Accessed: 19 March 2018).

Gartzke, E. and Lindsay, J. (2015) 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace', *Security Studies*, 24(2), pp. 316–348. doi: 10.1080/09636412.2015.1038188.

GCHQ (2014a) *IA14 : Minister for Cabinet Office speech on working together The threat*, *GCHQ Web Site*. Available at: https://webcache.googleusercontent.com/search?q=cache:-d_ZRVdmw-gJ:https://www.gchq.gov.uk/speech/ia14-minister-cabinet-office-speech-working-together (Accessed: 6 March 2018).

GCHQ (2014b) *IA14 Conference – Meeting the cyber security challenge in partnership*, *GCHQ Web Site*. Available at: https://webcache.googleusercontent.com/search?q=cache:t3nf7O03KooJ:https://www.gchq.gov.uk/press-release/ia14-conference-%25E2%2580%2593-meeting-cyber-security-challenge-partnership (Accessed: 6 March 2018).

GCHQ (2016) *The National Technical Assistance Centre*, *GCHQ Web Site*. Available at: https://www.gchq.gov.uk/features/national-technical-assistance-centre (Accessed: 31 October 2017).

GCHQ (2018a) *Director GCHQ writes about the importance of securing the next generation of technology*, *GCHQ Web Site*. Available at: https://www.gchq.gov.uk/news-article/jeremy-fleming-securing-next-generation-technology (Accessed: 14 February 2019).

GCHQ (2018b) *The Equities Process*, *GCHQ Web Site*. Available at: https://www.gchq.gov.uk/features/equities-process (Accessed: 2 January 2019).

Georgieva, M. (2015) *Contesting the State Securitization of Cyberspace : The Impact of Alternative Securitizing Actors*. Central European University. Available at: www.etd.ceu.hu/2015/georgieva_mariya.pdf.

Gerritz, C. (2016) *Breach Detection by the Numbers: Days, Weeks or Years?*, *Infocyte Blog*. Available at: https://www.infocyte.com/blog/2016/7/26/how-many-days-does-it-take-to-discover-a-breach-the-answer-may-shock-you (Accessed: 20 June 2018).

Gertz, B. (2017) *NSA : Cyber Attacks Are Becoming More Sophisticated , Aggressive , and Disruptive*, *Washington Free Beacon*. Available at: http://freebeacon.com/national-security/nsa-cyber-attacks-becoming-sophisticated-aggressive-disruptive/ (Accessed: 27 June 2018).

GFCE (2016) *Terms of Reference GFCE*, *GFCE Web Site*. Available at: https://www.thegfce.com/about/documents/publications/2016/02/25/tor-gfce (Accessed: 6 March 2020).

GFCE (2019) *GFCE CYBIL Portal*, *CYBIL Web Site*. Available at: https://cybilportal.org/ (Accessed: 6 March 2020).

Giacomello, G. (2004) 'Bangs for the buck: a cost-benefit analysis of cyberterrorism', *Studies in conflict and terrorism*, 27(5), pp. 387–408. doi: 10.1080/10576100490483660.

Gibbs, S. (2015) *Telegram messaging app will block Islamic State broadcasts*, *The Guardian*. Available at: https://www.theguardian.com/world/2015/nov/19/telegram-messaging-app-will-block-islamic-state-broadcasts (Accessed: 2 March 2018).

Gibson, W. (1984) *Neuromancer*. Paperback. London: Victor Gollanz.

Gilad, Y. *et al.* (2017) 'Are We There Yet ? On RPKI ' s Deployment and Security', *Ndss 2017*, (March).

Glaser, C. L. (2011) *Deterrence of Cyber Attacks and US National Security*, *GW-CSPRI-2011-5*. Washington DC.

Glen, C. M. (2018) *Controlling Cyberspace*. Santa Barbara, CA: Praeger.

Goble, G. (2012) *Top 10 bad tech predictions*, *Digital Trends*. Available at: https://www.digitaltrends.com/features/top-10-bad-tech-predictions/8/ (Accessed: 21 August 2018).

Goldsmith, J. (1998) 'The Internet and the Abiding Significance of Territorial Sovereignty', *Indiana Journal of Global Legal Studies*, 5(2), pp. 475–491. Available at: www.jstor.org/stable/25691116.

Goldsmith, J. and Russell, S. (2018) *Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations*. 1806. Stanford, CA.

Google Inc. (2017) *Data center locations – Data Centers – Google*, *Data Center Locations*. Available at: https://www.google.com/about/datacenters/inside/locations/index.html (Accessed: 15 November 2017).

Grabosky, P. (2001) 'Virtual Criminality: Old Wine in New Bottles', *Social and Legal Studies*, 10(2), pp. 243–249.

Graff, G. M. (2017) *How a Dorm Room Minecraft Scam Brought Down the Internet*, *Wired*. Available at: https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/ (Accessed: 30 May 2018).

Green, D. (2017) *First anniversary of the National Cyber Security Strategy*, *Gov.UK Web Site*. Available at: https://www.gov.uk/government/speeches/first-anniversary-of-the-national-cyber-security-strategy (Accessed: 5 March 2018).

Green, J. (2015) 'Introduction', in Green, J. (ed.) *Cyber Warfare: A multidisciplinary analysis*. South Asia. Abingdon: Routledge, pp. 1–5.

Greenberg, A. (2016) *It ' S Been 20 Years Since This Man Declared Cyberspace*, *Wired*. Available at: https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/ (Accessed: 10 January 2018).

Greenwald, G. (2014a) *How the NSA tampers with US-made internet routers*, *The Guardian*. Available at: https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden (Accessed: 27 September 2018).

Greenwald, G. (2014b) *No Place to Hide: Edward Snowden, the NSA & the Surveillance State*. London: Penguin Books.

Grint, K. (2010) 'Wicked problems and clumsy solutions: The role of leadership', *The New Public Leadership Challenge*, pp. 169–186. doi: 10.1057/9780230277953.

Grunwald, L. (2018) *Glauben statt wissen*, *Heise Online*. Available at:

https://www.heise.de/ix/heft/Glauben-statt-wissen-4140402.html (Accessed: 2 October 2018).

Guibourg, C. and Ehrenberg, B. (2015) *TalkTalk share price plunges twice as deep as Sony, Carphone Warehouse, Barclays and EBay after cyber attacks*, *City AM Web Site*. Available at: http://www.cityam.com/228714/talktalk-share-price-plunges-twice-as-deep-as-sony-carphone-warehouse-barclays-and-ebay-after-cyber-attacks (Accessed: 27 June 2018).

Gurr, T. R. (1980) *Handbook of Political Conflict*. New York: The Free Press.

Hackett, R. (2015) 'Let's get physical? United States weighs options when it comes to cyber attacks', *Fortune*, 12 May. Available at: http://fortune.com/2015/05/12/rogers-cyber-attacks-us-response/.

Hakim, S., Rengert, G. F. and Shachmurove, Y. (2000) *Knowing your odds: Home burglary and the odds ratio*. 00–14. Philadelphia, PA.

Hammond, P. (2016) *Chancellor speech: launching the National Cyber Security Strategy*, *UK Government Web Site*. Available at: https://www.gov.uk/government/speeches/chancellor-speech-launching-the-national-cyber-security-strategy (Accessed: 20 June 2017).

Hammond, P. (2017) *Chancellor's speech at the National Cyber Security Centre opening*. Available at: https://www.gov.uk/government/speeches/chancellors-speech-at-the-national-cyber-security-centre-opening (Accessed: 20 June 2017).

Hancock, M. (2016) *Keeping Britain safe from cyber attacks : Matt Hancock speech*, *Gov.UK Web Site*. Available at: https://www.gov.uk/government/speeches/keeping-britain-safe-from-cyber-attacks-matt-hancock-speech (Accessed: 5 March 2018).

Hancock, M. (2017) *Matt Hancock's cyber security speech at the Institute of Directors conference*. Available at: https://www.gov.uk/government/speeches/matt-hancocks-cyber-security-speech-at-the-institute-of-directors-conference (Accessed: 13 October 2017).

Hannigan, R. (2014) 'The web is a terrorist's command-and-control network of choice', *Financial Times*, pp. 5–6. Available at: https://www.ft.com/content/c89b6c58-6342-11e4-8a63-00144feabdc0.

Hannigan, R. (2015) 'IA15: Robert Hannigan's keynote speech - as delivered', pp. 1–6. Available at: https://www.gchq.gov.uk/speech/ia15-robert-hannigans-keynote-speech-delivered.

Hannigan, R. (2017) *How Britain's GCHQ Decides Which Secrets to Share with You*, *The Cipher Brief*. Available at: https://www.thecipherbrief.com/column_article/britains-gchq-decides-secrets-share (Accessed: 21 June 2018).

Hansen, L. and Nissenbaum, H. (2009) 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, (53), pp. 1155–1175. Available at: https://www.nyu.edu/projects/nissenbaum/papers/digital disaster.pdf.

Hardin, R. (2006) *Trust*. Cambridge: Polity Press.

Harris, S. (2014) *@War*. London: Headline.

Hayden, M. V (2016) *Playing to the Edge*. New York: Penguin Press.

HCSEC (2015) *Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board 1st Annual Report*. Banbury. Available at: https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2015.

HCSEC (2017) *Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board: Annual Report 2017*. Banbury. Available at: https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2017.

HCSEC (2018) *Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Anual Report 2018*. Banbury. Available at: https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2018.

Healey, J. (2011) 'The Five Futures of Cyber Conflict and Cooperation', *Georgetown. Journal of International Affairs*, 12(Special), pp. 110–118.

Healey, J. (2013) *A Fierce Domain: Conflict in Cyberspace 1986 - 2012*. Kindle. Washington DC: Cyber Conflict Studies Association.

Heickerö, R. (2014) 'Cyber Terrorism: Electronic Jihad', *Strategic Analysis*, 38(4), pp. 554–565. doi: 10.1080/09700161.2014.918435.

Herpig, S. (2014) *Anti-War and the Cyber Triangle: Strategic Implications of Cyber Operations and Security for the State*. University of Hull.

Herrera, G. (2008) 'Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space', in *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace.* London: Ashgate, pp. 67–93.

Hertz, R. and Imbert, J. (eds) (1995) *Studying Elites Using Qualitative Methods*. Thousand Oaks CA: SAGE Publications.

Herzberg, B., Bekerman, D. and Zeifman, I. (2016) *Breaking Down Mirai: An IoT DDoS Botnet Analysis*, *Imperva Incapsula Blog*. Available at: https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html (Accessed: 25 June 2018).

Herzog, M. and Schmid, J. (2016) 'Who pays for zero days?', in Friis, K. and Ringsmose, J. (eds) *Conflict in Cyberspace: Theoretical ,Strategic and Legal Persepectives*. Abingdon: Routledge, pp. 95–115.

Hettne, B. (2002) 'In Search of World Order', in Hettne, B. and Oden, B. (eds) *Global Governance in the 21st Century: Alternative Perspectives on World Order*. Stockholm: Almquiest & Wiksell Intl.

HMG (2010) *A Strong Britain in an Age of Uncertainty : The National Security Strategy*. doi: Cm 7953.

HMG (2013) *Oxford will host Cyber Security Capacity Building Centre*, *Gov.UK Web Site*. Available at: https://www.gov.uk/government/news/oxford-will-host-cyber-security-capacity-building-centre (Accessed: 5 March 2020).

HMG (2015a) *Chancellor opens book on more than £24 billion of Northern Powerhouse investment opportunities in China*, *Gov.UK Web Site*. Available at: https://www.gov.uk/government/news/chancellor-opens-book-on-more-than-24-billion-of-

northern-powerhouse-investment-opportunities-in-china (Accessed: 5 March 2018).

HMG (2015b) *National Security Strategy and Strategic Defence and Security Review 2015*. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf.

HMG (2016) *National Cyber Security Strategy*. Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021trategies-ncsss/NCSS_ESen.pdf.

HMG (2017a) *Government Transformation Strategy 2017 - 2020*, *UK Government Web Site*. Available at: https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020 (Accessed: 25 June 2018).

HMG (2017b) *Hate crime: abuse, hate and extremism online: The Government Response to the Fourteenth Report from the Home Affairs Select Committe Session 2016-17 HC609*, *Gov.UK Web Site*. Available at: https://www.publications.parliament.uk/pa/cm201617/cmselect/cmhaff/609/609.pdf (Accessed: 7 March 2018).

HMG (2018a) *Cyber Security capacity building: objectives 2017 to 2018*, *Gov.UK Web Site*. Available at: https://www.gov.uk/government/publications/official-development-assistance-oda-fco-programme-spend-objectives-2017-to-2018/cyber-security-capacity-building-objectives-2017-to-2018 (Accessed: 5 March 2020).

HMG (2018b) *FCO Cyber Security Capacity Building Programme 2018 to 2021*, *Gov.UK Web Site*. Available at: https://www.gov.uk/government/publications/fco-cyber-security-capacity-building-programme-2018-to-2021 (Accessed: 5 March 2020).

Hoffman, S. (1986) 'Hedley Bull and His Contribution to International Relations', *International Affairs*, 62(2), pp. 179–195. Available at: www.jstor.org/stable/2618360.

Hohmann, M. *et al.* (2017) 'Advancing Cybersecurity Capacity Building Implementing a Principle-Based Approach', *Global Public Policy Institute (GPPi)*. Available at: http://www.gppi.net/fileadmin/user_upload/media/pub/2017/Hohmann__Pirang__Benner__2017__Advancing_Cybersecurity_Capacity_Building.pdf.

Home Office Science Advisory Council (2018) *Understanding the costs of cyber crime A report of key findings from the Costs of Cyber Crime Working Group*. London. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674046/understanding-costs-of-cyber-crime-horr96.pdf.

Hunt, J. (2019) *Deterrence in the cyber age: Foreign Secretary's speech*, *Gov.UK Web Site*. Available at: https://www.gov.uk/government/speeches/deterrence-in-the-cyber-age-speech-by-the-foreign-secretary (Accessed: 6 January 2020).

Hunter, B. (2017) *Publishers vs ResearchGate: an academic's view*, *Times Higher Education*. Available at: https://www.timeshighereducation.com/blog/publishers-vs-researchgate-academics-view (Accessed: 23 January 2018).

Hurley, M. M. (2012) 'For and from cyberspace: Conceptualizing cyber intelligence,

surveillance, and reconnaissance', *Air and Space Power Journal*, 26(6), pp. 12–33.

Huysmans, J. (2002) 'Defining Social Constructivism in Security Studies: The Normative Dilemma of Writing Security', *Alternatives*, Special Is, pp. 41–62.

Ilves, T. H. (2014) *Remarks by the President of Estonia , Toomas Hendrik Ilves at the Freedom Online Coalition Conference in Swissotel , April 28 , 2014*. Available at: https://vp2006-2016.president.ee/en/official-duties/speeches/10101-remarks-by-the-president-of-estonia-toomas-hendrik-ilves-at-the-freedom-online-coalition-conference-in-swissotel-april-28-2014/index.html (Accessed: 21 November 2017).

Infosec Institute (2018) *Consequences of the Late Announcement of Cyber-security Incidents*, *Infosec Institute Web Site*. Available at: https://resources.infosecinstitute.com/consequences-late-announcement-cyber-security-incidents/#gref (Accessed: 27 June 2018).

Ingram, H. J. (2014) 'Three Traits of the Islamic State's Information Warfare', *RUSI Journal*, 159(6), pp. 4–11. doi: 10.1080/03071847.2014.990810.

Intelligence and Security Committee (2017) *Intelligence and Security Committee of Parliament Annual Report 2016 - 2017*. London. Available at: http://isc.independent.gov.uk/committee-reports/annual-reports.

International Security Advisory Board (2014) 'Report on A Framework for International Cyber Stability'.

International Telecommunications Union (2003) *Word Summit on the Information Society, Declaration of Principles*. Available at: http://www.itu.int/net/wsis/docs/geneva/official/dop.html (Accessed: 9 October 2017).

International Telecommunications Union (2008) *Recommendation X.1205: Overview of Cybersecurity*. Geneva: ITU-T. Available at: https://www.itu.int/rec/T-REC-X.1205-200804-I (Accessed: 15 January 2018).

International Telecommunications Union (2017) *Percentage of Individuals using the Internet*, *ITU Web Site*. Available at: https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2018/Individuals_Internet_2000-2017.xls (Accessed: 2 October 2018).

Internet Live Stats (2017) *Internet Live Stats*. Available at: http://www.internetlivestats.com/google-search-statistics/#share (Accessed: 11 September 2017).

Internet Society (2012a) *Internet Society Perspectives on Domain Name System (DNS) Filtering :* Geneva. Available at: http://www.isoc.org/internet/issues/dns-filtering.shtml.

Internet Society (2012b) *The Internet and the Public Switched Telephone Network*. Available at: https://www.internetsociety.org/sites/default/files/The Internet and the Public Switched Telephone Network.pdf.

ISC (2013) 'Foreign involvement in the Critical National Infrastructure : The implications for national security'. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/205680/ISC-Report-Foreign-Investment-in-the-Critical-National-Infrastructure.pdf.

ITU FG-Net-2030 (2020) *Network 2030*, *ITU Web Site*. Available at: https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/White_Paper.pdf (Accessed: 3 June 2020).

Jackson Higgins, K. (2016) *Hacking A Penetration Tester*, *Dark Reading*. Available at: https://www.darkreading.com/vulnerabilities---threats/hacking-a-penetration-tester/d/d-id/1326192 (Accessed: 12 August 2017).

Jarvis, L., Macdonald, S. and Nouri, L. (2014) 'The Cyberterrorism Threat: Findings from a Survey of Researchers.', *Studies in Conflict & Terrorism*, 37(1), pp. 68–90. doi: 10.1080/1057610X.2014.853603.

Jenkins, R. (2016) 'Cyberwar as Ideal War', in Allhoff, F., Henschke, A., and Strawser, B. J. (eds) *Binary Bullets: The Ethics of Cyber Warfare*. New York: Oxford University Press, pp. 89–114.

Jensen, B. M., Valeriano, B. and Maness, R. C. (2017) 'Cyber Compellence : Applying Coercion in the Information Age', pp. 1–27. Available at: http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/cyber_victory.pdf.

Jervis, R. (1978) 'Cooperation Under the Security Dilemma', *World Politics*, 30(12), pp. 167–214.

Johnson, D. R. and Post, D. (1996) 'Law and borders - The rise of law in cyberspace', *Stanford Law Review*, 48(5).

Jolley, J. (2017) *Attribution, state responsibility, and the duty to prevent malicious cyber-attacks in international law.* University of Glasgow. Available at: http://theses.gla.ac.uk/8452/.

Kahn, J. (2017) *U.K. Probes Russian Social Media Influence in Brexit Vote*, *Bloomberg*. Available at: https://www.bloomberg.com/news/articles/2017-11-02/u-k-probes-russian-social-media-influence-in-brexit-vote (Accessed: 27 September 2018).

Kaplan, R. D. (2000) *The Coming Anarchy*. Vintage. New York: Random House.

Keen, A. (2015) *The Internet is Not the Answer*. Paperback. London: Atlantic Books Ltd.

Kello, L. (2013) 'The Meaning of the Cyber Revolution', *International Security*, 38(2), pp. 7–40. Available at: https://www.belfercenter.org/sites/default/files/files/publication/IS3802_pp007-040.pdf.

Kello, L. (2018) *The Virtual Weapon and International Order*. Paperback. New Haven, CT: Yale University Press.

Keohane, R. and Nye, J. (1989) *Power and Interdependence*. Second. New York: Harper Collins.

Keough, M. (2015) *Twitter moves non-US data to server in Dublin*, *Irish Central*. Available at: https://www.irishcentral.com/business/technology/twitter-moves-non-us-data-to-server-in-dublin (Accessed: 15 November 2017).

Keppler, N., Freifeld, K. and Walcott, J. (2017) *Siemens , Trimble , Moody ' s breached by Chinese hackers , U . S . charges*, *Reuters*. Available at: https://www.reuters.com/article/us-usa-cyber-china-indictments/siemens-trimble-moodys-breached-by-chinese-hackers-u-s-charges-

idUSKBN1DR26D (Accessed: 22 February 2018).

Kimball, J. (2019) *7 of the best free network vulnerability scanners and how to use them*, *Comparitch Website*. Available at: https://www.comparitech.com/net-admin/free-network-vulnerability-scanners/ (Accessed: 5 March 2019).

Kimery, A. (2014) 'The Jester Speaks', *Homeland Security Today*. Available at: https://www.hstoday.us/subject-matter-areas/cybersecurity/the-jester-speaks-and-he-has-a-lot-to-say-too/.

Kincaid, H. V and Bright, M. (1957) 'Interviewing the Business Elite', *American Journal of Sociology*, 63(3), pp. 304–311.

Kirk, J. (2014) *Home Depot attackers broke in using a vendor's stolen credentials*, *Computer World Web Site*. Available at: https://www.computerworld.com/article/2844491/home-depot-attackers-broke-in-using-a-vendors-stolen-credentials.html (Accessed: 20 June 2018).

Kirk, T. (2018) *GCHQ mass surveillance breached human rights on privacy, European court rules*, *The Guardian*. Available at: https://www.standard.co.uk/news/world/gchq-mass-surveillance-breached-human-rights-on-privacy-european-court-rules-a3934996.html (Accessed: 27 September 2018).

Klimburg, A. (2011) 'Mobilising Cyber Power', *Survival*, 53(1), pp. 41–60. doi: 10.1080/00396338.2011.555595.

Klimburg, A. (2017a) *The Darkening Web: The War for Cyberspace*. Internatio. New York: Penguin Press.

Klimburg, A. (2017b) *The Darkening Web: The War for Cyberspace*. Internatio. New York: Penguin Press.

Knightly, P. (1987) *The Second Oldest Profession*. London: Pan.

Kobrin, S. (1999) 'Back to the Future: Neomedievalism and the Postmodern Digital World Economy', in Prakash, A. and Hart, J. A. (eds) *Globalization and Governance*. London: Routledge, pp. 165–187. doi: Article.

Kohl, U. and Rowland, D. (2017) 'Censorship and Cyberborders through EU Data Protection Law', in *The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance*, pp. 93–109.

Kolodny, L. (2018) *Former Google CEO predicts the internet will split in two — and one part will be led by China*, *CNBC Web Site*. Available at: https://www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html (Accessed: 11 October 2018).

Kramer, F., Starr, S. and Wentz, L. (eds) (2009) *Cybepower and National Security*. Washington DC: Centre for Technology & National Security Policy.

Krasner, S. D. (1999) *Sovereignty: Organised Hypocrisy*. Princeton, NJ: Princeton University Press.

Krebs, B. (2016) *Israeli Online Attack Service 'vDOS' Earned $600,000 in Two Years*, *Krebs on Security*.

Kuehl, D. T. (2009) 'From Cyberspace to Cyberpower', in Kramer, F. D., Starr, S. H., and Wentz, L. K. (eds) *Cyberpower and National Security*. Paperback. Dulles VA: Potomac Books, pp. 24–42.

Kugler, R. (2009) 'Deterrence of Cyber Attacks', in Kramer, F., Starr, S., and Wentz, L. (eds) *Cyberpower and National Security*. First. Dulles: Potomac Books, pp. 309–342.

Kuhn, J. (2015) *Dangers of the deep , dark web*. Somers, NY. Available at: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=SP&infotype=PM&htmlfid=SEL03035USEN&attachment=SEL03035USEN.PDF.

Kumar, M. (2017) *Process Doppelgänging : New Malware Evasion Technique Works On All Windows Versions*, *The Hacker News*. Available at: https://thehackernews.com/2017/12/malware-process-doppelganging.html (Accessed: 7 December 2017).

Kutner, M. (2016) 'Alleged Dam Hacking Raises Fears of Cyber Threats to Infrastructure', *Newsweek*. Available at: http://www.newsweek.com/cyber-attack-rye-dam-iran-441940.

Lachow, I. (2009) 'Cyberterrorism: Menace or Myth?', in Kramer, F., Starr, S., and Wentz, L. (eds) *Cyberpower and National Security*. Washington DC: Centre for Technology & National Security Policy.

Lachow, I. (2016) *The Private Sector Role in Offensive Cyber Operations : Benefits , Issues and Challenges*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836201 (Accessed: 16 March 2018).

Lachow, I. and Richardson, C. (2007) *Terrorist Use of the Internet The Real Story*, *Joint Forces Quarterly*. Available at: http://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-45.pdf (Accessed: 3 July 2018).

Lambach, D. (2016) 'The Territorialisation of Cyberspace', *Tagung der DVPW-Themengruppe Internet und Politik*. Heidelberg: Researchgate, pp. 25–27. Available at: https://www.researchgate.net/publication/308720083_The_Territorialization_of_Cyberspace.

Landau, S. (2017) *Listening In: Cyber Security in an Insecure Age*. New Haven, CT: Yale University Press.

Latiff, R. H. (2017) *Future War: Preparing for the New Global Battlefield*. New York: Albert Knopf.

Lee, R. M. and Rid, T. (2014) 'OMG Cyber!', *The RUSI Journal*, 159(5), pp. 4–12. doi: 10.1080/03071847.2014.969932.

Lemos, R. (2018) *Why the hack-back is still the worst idea in cybersecurity*, *Tech Beacon*. Available at: https://techbeacon.com/why-hack-back-still-worst-idea-cybersecurity (Accessed: 23 February 2018).

Leonard, J. (2016) *NAO report slates the Cabinet Office's cyber security efforts*, *Computing*. Available at: http://www.computing.co.uk/ctg/news/2470726/nao-report-slates-the-uk-governments-cyber-security-efforts (Accessed: 9 January 2017).

Lessig, L. (1999) *Code and Other Laws of Cyberspace*. New York: Basic Books.

Lessig, L. (2000) 'Code Is Law', *Harvard Magazine*, pp. 1–5. Available at: https://www.harvardmagazine.com/2000/01/code-is-law-html.

Lessig, L. (2006) *Code version 2.0*. Kindle Edi. New York: Basic Books.

Levin, K. *et al.* (2009) 'Playing it forward: Path dependency, progressive incrementalism, and the "Super Wicked" problem of global climate change', *IOP Conference Series: Earth and Environmental Science*, 6(50), p. 502002. doi: 10.1088/1755-1307/6/0/502002.

Levin, K. *et al.* (2012) 'Overcoming the tragedy of super wicked problems: Constraining our future selves to ameliorate global climate change', *Policy Sciences*, 45(2), pp. 123–152. doi: 10.1007/s11077-012-9151-0.

Levy, I. (2016a) *Active Cyber Defence - tackling cyber attacks on the UK*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk (Accessed: 9 October 2017).

Levy, I. (2016b) *Active Cyber Defence - tackling cyber attacks on the UK*, *NCSC Blog*. Available at: https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk (Accessed: 10 January 2017).

Levy, I. (2018) *Equities Process*, *NCSC Blog*. Available at: https://www.ncsc.gov.uk/blog-post/equities-process (Accessed: 2 January 2019).

Leydon, J. (2012) *Whistleblower : Decade-long Nortel hack 'traced to China'*, *The Register*. Available at: https://www.theregister.co.uk/2012/02/15/nortel_breach/ (Accessed: 22 February 2018).

Leydon, J. (2018) *Pwned with '4 lines of code': Researchers warn SCADA systems are still hopelessly insecure*, *The Register*. Available at: https://www.theregister.co.uk/2018/06/18/physically_hacking_scada_infosec/ (Accessed: 28 June 2018).

Liaropoulos, A. (2017) 'Cyberspace Governance and State Sovereignty', in Bitros, G. and Kyriazis, N. (eds) *Democracy and an Open-Economy World Order*. Cham, Switzerland: Springer International, pp. 25–36. doi: 10.1007/978-3-319-52168-8.

Libicki, M. (2007) *Conquest in Cyberspace*. New York: Cambridge University Press.

Libicki, M. (2009) *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation.

Libicki, M. C. (2012) 'Cyberspace Is Not a Warfighting Domain', *Journal of Law and Policy*, 8(2), pp. 325–336.

Limbago, A. L. (2017) *The 'Hacking Back' Bill isn't the Answer to Cyberattacks*, *War on the Rocks*. Available at: https://warontherocks.com/2017/10/the-hacking-back-bill-isnt-the-solution-to-cyberattacks/ (Accessed: 23 February 2018).

Lindsay, J. (2013) 'Stuxnet and the Limits of Cyber Warfare', *Security Studies*, 22(3), pp. 365–404. doi: 10.1080/09636412.2013.816122.

Lloyds of London (2017) *Counting the cost: cyber exposure decoded*, *Emerging Risks Report*.

London. Available at: https://www.lloyds.com/news-and-insight/risk-insight/library/technology/countingthecost.

LM Security (2016) *CIA Triad*, *Infosec Institute Web Site*. Available at: http://resources.infosecinstitute.com/cia-triad/ (Accessed: 15 January 2018).

Lobban, I. (2012) *Director GCHQ makes cyber speech at the International Institute of Strategic Studies*. Available at: https://www.gchq.gov.uk/speech/director-gchq-makes-cyber-speech-international-institute-strategic-studies (Accessed: 13 October 2017).

Lomas, N. (2016a) 'UK's new cyber security centre to debunk scare tactics and lead by example', *Tech Crunch*, pp. 1–5. Available at: https://techcrunch.com/2016/10/21/uks-new-cyber-security-centre-to-debunk-scare-tactics-and-lead-by-example/.

Lomas, N. (2016b) *UK's new cyber security centre to debunk scare tactics and lead by example*, *Tech Crunch*. Available at: https://techcrunch.com/2016/10/21/uks-new-cyber-security-centre-to-debunk-scare-tactics-and-lead-by-example/ (Accessed: 11 January 2017).

Maher, K. (2013) 'The New Westphalian Web', *Foreign Policy*. Available at: http://foreignpolicy.com/2013/02/25/the-new-westphalian-web/.

Makrushin, D. (2017) *The cost of launching a DDoS attack*, *Kaspersky Secure List Blog*. Available at: https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/ (Accessed: 28 June 2018).

Malcolmson, S. (2017) 'Welcome to the Splinternet', pp. 1–5.

Malewarebytes (2017) *The new mafia: Gangs and vigilantes*, *Malwarebytes Web Site*. Available at: https://www.malwarebytes.com/pdf/white-papers/Cybercrime_NewMafia.pdf (Accessed: 2 October 2018).

Malone, E. F. and Malone, M. J. (2013) 'The "wicked problem" of cybersecurity policy: analysis of United States and Canadian policy response', *Canadian Foreign Policy Journal*, 19(2), pp. 158–177. doi: 10.1080/11926422.2013.805152.

Manter, G. (2003) 'The Pending Determination of the Legality of Internet Gambling in the United States', *Duke Law and Technology Review*, 2(1). Available at: http://www.law.duke.edu/journals/dltr/articles/2003dltr0016.html.

Manville, B. (2016) 'Six Leadership Practices for Wicked Problem Solving', *Forbes*, May, pp. 1–7. Available at: https://www.forbes.com/pictures/56ead155e4b0c144a7f785a3/3-enthusiasm/#4bb04cf16c32.

Martin, C. (2014) *IA14 : Ciaran Martin ' s opening address*. Available at: https://www.gchq.gov.uk/speech/ia14-ciaran-martins-opening-address (Accessed: 15 October 2017).

Martin, C. (2015) 'Director General for Cyber Security speaks at Infosecurity Europe 2015', *Gchq*, pp. 1–7. Available at: https://www.gchq.gov.uk/speech/director-general-cyber-security-speaks-infosecurity-europe-2015.

Martin, C. (2016a) *A new approach for cyber security in the UK*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk (Accessed: 13 January

2017).

Martin, C. (2016b) 'A new approach for cyber security in the UK', *NCSC Web Site*, pp. 1–8. Available at: https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk.

Martin, C. (2017a) *Ciaran Martin's speech in Tallinn, Estonia*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/news/ciaran-martins-speech-tallinn-estonia (Accessed: 9 October 2017).

Martin, C. (2017b) *Ciaran Martin ' s speech to CBI*. Available at: https://www.ncsc.gov.uk/news/ciaran-martins-speech-cbi (Accessed: 13 October 2017).

Martin, C. (2017c) *Cyber security : fixing the present so we can worry about the future*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/news/cyber-security-fixing-present-so-we-can-worry-about-future (Accessed: 13 December 2017).

Martin, C. (2017d) *Cyber security : fixing the present so we can worry about the future*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/news/cyber-security-fixing-present-so-we-can-worry-about-future.

Martin, C. (2017e) 'Full speech : Ciaran Martin on the National Cyber Security Centre', 2017(September), pp. 1–7. Available at: http://www.cbi.org.uk/news/full-speech-ciaran-martin-on-the-national-cyber-security-centre/.

Maude, F. (2012) *Francis Maude speech at IA12 - Cyber Security Strategy one year on*, *Speeches - GOV.UK*. Available at: https://www.gov.uk/government/speeches/francis-maude-speech-at-ia12-cyber-security-strategy-one-year-on (Accessed: 12 July 2017).

Maude, F. (2013) *Cyber Security Information Sharing Partnership*, *Gov.uk*. Available at: https://www.gov.uk/government/speeches/cyber-security-information-sharing-programme (Accessed: 15 October 2017).

Maude, F. (2014a) *Francis Maude on the launch of CERT-UK*, *Speeches - GOV.UK*. Available at: https://www.gov.uk/government/speeches/francis-maude-on-the-launch-of-cert-uk (Accessed: 12 July 2017).

Maude, F. (2014b) *Francis Maude speech at IA14*, *Speeches - GOV.UK*. Available at: https://www.gov.uk/government/speeches/francis-maude-speech-at-ia14 (Accessed: 15 October 2017).

Maurer, T. (2018) *Cyber Mercenaries*. Cambridge: Cambridge University Press.

Maxey, L. (2017) 'How Britain's GCHQ Decides Which Secrets to Share with You', *The Cipher Brief*. Available at: https://www.thecipherbrief.com/column_article/britains-gchq-decides-secrets-share.

Maxey, L. (2018) *Terrorists Stalk Dark Web for Deadlier Weaponry*, *The Cipher Brief*. Available at: https://www.thecipherbrief.com/article/tech/terrorists-stalk-dark-web-deadlier-weaponry (Accessed: 23 January 2018).

McCarthy, K. (2016) *Critics hit out at 'black box' UN internet body*, *The Register*. Available at: https://www.theregister.co.uk/2016/03/31/black_box_un_internet_body/ (Accessed: 20 August 2018).

McFate, S. (2014) *The Modern Mercenary: Private Armies and What They Mean for World Order*. Paperback. New York: Oxford University Press.

McGoogan, C. (2016) 'GCHQ wants internet providers to rewrite systems to block hackers', *Daily Telegraph*, 5 November. Available at: http://www.telegraph.co.uk/technology/2016/11/05/gchq-wants-internet-providers-to-rewrite-systems-to-block-hacker/.

McGraw, G. (2013) 'Cyber War is Inevitable (Unless We Build Security In)', *Journal of Strategic Studies*, 36(1), pp. 109–119.

McGuire, M. and Dowling, S. (2013) *Cyber crime: A review of the evidence Research Report 75*. London. Available at: http://www.justiceacademy.org/iShare/Library-UK/horr75-chap1.pdf.

McKenzie, T. M. (2017) *Is cyber deterrence possible?* Available at: https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF.

Mey, J. (2001) *Pragmatics: An Introduction*. Oxford: Blackwell.

Microsoft (2016) *Microsoft Cloud Germany*, *Microsoft Azure Web Site*. Available at: download.microsoft.com/download/6/.../Microsoft_Cloud_Germany_Datasheet.pdf (Accessed: 2 March 2018).

Minarik, T. (2016) *NATO Recognises Cyberspace as a Somain of Operations at Warsaw Summit*. Available at: https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html (Accessed: 10 January 2018).

MoD (2020) *6th (United Kingdom) Division*, *MoD Web Site*. Available at: https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/ (Accessed: 20 February 2020).

Morgan, P. M. (2010) 'Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm', in *Proceedings of a Workshop on Deterring Cyberattacks*. Washington, DC: National Academies Press. doi: 10.17226/12997.

Morgan, S. (2017) *Cyber Security Market Report*, *Cyber Security Ventures*. Available at: https://cybersecurityventures.com/cybersecurity-market-report/ (Accessed: 1 January 2018).

Morozov, E. (2011) *The Net Delusion: How Not to Liberate the World*. Penguin. London: Penguin Books Ltd.

Mueller, M. (2013) *Networks and States*. Paperback. Cambridge MA: MIT Press.

Mueller, M., Mathiason, J. and Klein, H. (2007) 'The Internet and Global Governance: Principles and Norms for a New Regime', *Global Governance*, 13(2), pp. 237–254. Available at: www.jstor.org/stable/27800656.

Munk, T. H. (2015) *Cyber-security in the European Region : Anticipatory Governance and Practices*. University of Manchester. Available at: https://www.research.manchester.ac.uk/portal/files/54570851/FULL_TEXT.PDF.

Murdock, J. (2016) *GCHQ: Spy chief admits UK agency losing cyberwar despite £860m funding*

boost, *International Business Times*. Available at: http://www.ibtimes.co.uk/gchq-spy-chief-admits-uk-agency-losing-cyberwar-despite-860m-funding-boost-1547943 (Accessed: 9 January 2017).

Muresan, R. (2017) 'Cyber security spending to reach $90 billion in 2017, Gartner says', *Bitdefender*, pp. 2017–2018.

National Audit Office (2013) 'The UK cyber security strategy: Landscape review', *National Audit Office*, (February), pp. 1–42. Available at: http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf.

National Audit Office (2014) *Update on the National Cyber Security Programme*. Available at: https://www.nao.org.uk/wp-content/uploads/2015/09/Update-on-the-National-Cyber-Security-Programme-summary.pdf.

National Audit Office (2016) *Protecting Information Across Government*. Available at: https://www.nao.org.uk/wp-content/uploads/2016/09/Protecting-information-across-government.pdf.

National Audit Office (2019) *Progress of the 2016 – 2021 National Cyber Security Programme Key facts*. London.

National Crime Agency (2015) *GCHQ and NCA join forces to ensure no hiding place online for criminals*, *NCA Web Site*. Available at: http://www.nationalcrimeagency.gov.uk/news/736-gchq-and-nca-join-forces-to-ensure-no-hiding-place-online-for-criminals (Accessed: 31 October 2017).

National Crime Agency (2017a) *The cyber threat to UK business 2016/2017 Report*, *NCA Web Site*. London. Available at: http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file.

National Crime Agency (2017b) *Two of dark web's biggest criminal marketplaces shut down*, *NCA Web Site*. Available at: http://www.nationalcrimeagency.gov.uk/news/1154-two-of-dark-web-s-most-significant-criminal-marketplaces-shut-down (Accessed: 21 January 2019).

National Crime Agency (2018a) *Dark web drug dealers get 56 years in jail*, *NCA Web Site*. Available at: http://www.nationalcrimeagency.gov.uk/news/1310-dark-web-drug-dealers-get-56-years-in-jail (Accessed: 21 January 2019).

National Crime Agency (2018b) *Depraved 'hurt core' university academic jailed for 32 years*, *NCA Web Site*. Available at: http://www.nationalcrimeagency.gov.uk/news/1293-depraved-hurt-core-university-academic-jailed-for-38-years (Accessed: 21 January 2019).

National Institute of Standards and Technology (2012) 'NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments', *NIST Special Publication*, (September), p. 17. doi: 10.6028/NIST.SP.800-30r1.

NCSC (2015) 'Common Cyber Attacks: Reducing The Impact', *UK Government*, (January), p. 17. Available at: https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/common_cyber_attacks_ncsc.pdf.

NCSC (2016a) *Common Cyber attacks*. London. Available at: https://www.ncsc.gov.uk/white-

papers/common-cyber-attacks-reducing-impact.

NCSC (2016b) *Password Guidance: Simplifying Your Approach*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach (Accessed: 4 February 2019).

NCSC (2017a) *Certified products*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/index/certified-product (Accessed: 12 December 2017).

NCSC (2017b) 'Finding the Kill Switch to Stop the Spread of Ransomware', *National Cyber Security Center*, pp. 2–4. Available at: https://www.ncsc.gov.uk/blog-post/finding-kill-switch-stop-spread-ransomware-0.

NCSC (2017c) *Growing positive security cultures*, *NCSC Twitter Feed*. Available at: https://www.ncsc.gov.uk/blog-post/growing-positive-security-cultures (Accessed: 24 September 2018).

NCSC (2017d) *Have you signed up to be part of our Cyber Security Information Sharing Partnership (CiSP)?*, *NCSC Twitter Feed*. Available at: https://twitter.com/ncsc/status/946306989466046465 (Accessed: 29 December 2017).

NCSC (2017e) *NCSC 2017 Annual Review*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/news/national-cyber-security-centre-year-protecting-uk.

NCSC (2017f) *NCSC degree certification - Call for new applicants*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/information/ncsc-degree-certification-call-new-applicants-0 (Accessed: 12 December 2017).

NCSC (2017g) *The Secure by Default Partnership Programme*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/information/secure-default-partnership-programme (Accessed: 13 December 2017).

NCSC (2017h) *What is Industry 100 ?*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/information/industry-100 (Accessed: 12 December 2017).

NCSC (2018a) *Example supply chain attacks*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/guidance/example-supply-chain-attacks (Accessed: 20 June 2018).

NCSC (2018b) *GCHQ Certified Training*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/scheme/gchq-certified-training (Accessed: 24 September 2018).

NCSC (2018c) *General Data Protection Regulation (GDPR)*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/GDPR (Accessed: 26 September 2018).

NCSC (2018d) *Introduction to the NIS Directive*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/guidance/introduction-nis-directive (Accessed: 2 March 2018).

NCSC (2018e) *Joint report on publicly available hacking tools*, *NCSC Web Site*. Available at: https://www.ncsc.gov.uk/joint-report (Accessed: 11 October 2018).

NCSC (2018f) *NCSC UK Twitter 24th January 2018 09.54*, *Twitter*. Available at: https://twitter.com/ncsc/status/956221367057346560 (Accessed: 20 February 2018).

Neudorf, P. *et al.* (2016) 'Cyber War'. UK: VICE. Available at:

www.vice.com/en_us/topic/cyberwar.

New York Times (1995) 'International Briefs ; European Approval Seen On Atlas', *New York Times*, October. Available at: http://www.nytimes.com/1995/10/17/business/international-briefs-european-approval-seen-on-atlas-telecom-deal.html.

New York Times (2018) *Russian Hacking and Influence in the U.S. Election*, *New York Times*. Available at: https://www.nytimes.com/news-event/russian-election-hacking (Accessed: 27 September 2018).

NHS Digital (2017) *Fit for 2020: Report from the NHS Digital Capability Review*. Leeds. Available at: https://digital.nhs.uk/about-nhs-digital/our-work/transforming-health-and-care-through-technology/fit-for-2020-report-from-the-nhs-digital-capability-review (Accessed: 3 September 2018).

Nichols, S. (2016) *Great British Block-Off: GCHQ floats plan to share its DNS filters*, *The Register*. Available at: http://www.theregister.co.uk/2016/09/14/great_british_blockoff/ (Accessed: 11 January 2017).

NIST (2017) *New Network Security Standards Will Protect Internet's Routing*. Available at: https://www.nist.gov/news-events/news/2017/10/new-network-security-standards-will-protect-internets-routing (Accessed: 9 October 2017).

Norton-Taylor, R. (2009) 'British intelligence agencies to step up security over cyber-attack threats', pp. 1–3. Available at: https://www.theguardian.com/politics/2009/jun/25/cyber-crime-hacking-gchq-security.

Nugraha, Y., Kautsarina and Sastrosubroto, A. S. (2015) 'Towards data sovereignty in cyberspace', *2015 3rd International Conference on Information and Communication Technology, ICoICT 2015*, (2), pp. 465–471. doi: 10.1109/ICoICT.2015.7231469.

Number Resource Organization (2014) *Regional Internet Registries*. Available at: http://www.nro.net/about-the-nro/regional-internet-registries (Accessed: 12 March 2018).

Nye, J. (2004) *Power in the Global Information Age*. Abingdon: Routledge.

Nye, J. (2010) *Cyber Power*. Cambridge, MA. Available at: http://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf.

Nye, J. (2011) *The Future of Power*. New York: Public Affairs.

Nye, J. S. (2014) 'The Regime Complex for Managing Global Cyber Activities', *CIGI Publications*, (1), pp. 1–15.

Nye, J. S. and Welch, D. A. (2014) *Understanding Global Conflict & Cooperation: Intro to Theory & History*. Pearson Ne. Harlow: Pearson.

O'Connell, R. (2013) *Defining Conflict*, *VIACONFLICT Web Site*. Available at: https://viaconflict.wordpress.com/2013/12/15/definitions-of-conflict/ (Accessed: 17 January 2020).

O'Connor, T. (2011) *The Jester Dynamic : A Lesson in Asymmetric Unmanaged Cyber Warfare*. Available at: https://www.sans.org/reading-room/whitepapers/attacking/jester-dynamic-

lesson-asymmetric-unmanaged-cyber-warfare-33889.

O'Neill, P. H. (2017) *U.S. Air Force invests millions this month on cyberweapons projects*, *Cyber Scoop*. Available at: https://www.cyberscoop.com/us-air-force-invested-millions-on-new-cyber-weapons/ (Accessed: 12 September 2017).

OFCOM (2017) *The Communications Market: UK*, *OFCOM Web Site*. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0021/105438/uk-internet-online.pdf (Accessed: 25 June 2018).

ONS (2017a) *E-commerce and ICT activity*, *ONS Web Site*. Available at: https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/datasets/ictactivityofukbusinessesecommerceandictactivity (Accessed: 25 June 2018).

ONS (2017b) *Internet access – households and individuals: 2017*, *ONS Web Site*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2017#online-shopping-continues-to-grow (Accessed: 15 June 2018).

ONS (2018) *Internet Users Dataset*, *ONS Web Site*. Available at: https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/datasets/internetusers (Accessed: 25 June 2018).

Osborne, G. (2015) *Chancellor's speech to GCHQ on cyber security*, *Gov.Uk*. Available at: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security (Accessed: 13 October 2017).

Panda Security (2017) *PandaLabs Annual Report 2017*. Available at: http://www.pandasecurity.com/mediacenter/src/uploads/2015/02/Pandalabs2014-DEF2-en.pdf (Accessed: 18 June 2018).

Pariser, E. (2011) *The Filter Bubble: What the Internet is Hiding From You*. Kindle. London: Viking.

Parkin, S. (2017) *Keyboard warrior: the British hacker fighting for his life*, *The Guardian*. Available at: https://www.theguardian.com/news/2017/sep/08/lauri-love-british-hacker-anonymous-extradition-us (Accessed: 23 May 2018).

Pauli, D. (2016) *Hacker takes down CEO wire transfer scammers , sends their Win 10 creds to the cops*, *The Register*. Available at: http://www.theregister.co.uk/2016/09/06/hacker_hacks_ceo_wire_transfer_scammers_sends_win_10_creds_to_cops/ (Accessed: 22 February 2018).

Pauna, A. and Moulinos, K. (2013) *Window of exposure … a real problem for SCADA systems? - Recommendations for Europe on SCADA patching*. Heraklion, Greece. Available at: https://www.enisa.europa.eu/publications/window-of-exposure-a-real-problem-for-scada-systems.

Pemberton, A. (2015) *Talk Talk boss Dido Harding's utter ignorance is a lesson to us all*, *Campaign*. Available at: https://www.campaignlive.co.uk/article/talk-talk-boss-dido-hardings-utter-ignorance-lesson-us/1370062 (Accessed: 25 May 2018).

Penney, J. W. (2015) 'Code Is Law', *Slate*, (February 2000), pp. 1–5. Available at:

http://www.slate.com/articles/technology/future_tense/2015/01/cfaa_reform_how_laws_are_determining_the_ethics_of_code.html.

Peoples, C. and Vaughan-Williams, N. (2015) *Critical Security Studies: An Introduction*. Second. Abingdon: Routledge.

Perez, R. (2017) *A cyber-success story : HMRC's road to DMARC implementation*, *SC Magazine*. Available at: https://www.scmagazineuk.com/a-cyber-success-story-hmrcs-road-to-dmarc-implementation/article/639198/ (Accessed: 13 December 2017).

Perritt Jr., H. (1998) 'The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance', *Indiana Journal of Global Legal Studies*, 5(2), pp. 423–442. doi: 10.1525/sp.2007.54.1.23.

Peters, B. G. (2017) 'What is so wicked about wicked problems? A conceptual analysis and a research program', *Policy and Society*. Routledge, 36(3), pp. 385–396. doi: 10.1080/14494035.2017.1361633.

Peterson, D. (2013) 'Offensive Cyber Weapons: Construction, Development, and Employment', *Journal of Strategic Studies*, 36(1), pp. 120–124. doi: 10.1080/01402390.2012.742014.

PhishLabs (2016) '2016 Phishing Trends & Intelligence Report: Hacking the Human', pp. 1–40. Available at: https://pages.phishlabs.com/rs/130-BFB-942/images/2017 PhishLabs Phishing and Threat Intelligence Report.pdf%5Cnhttps://www.phishlabs.com/phishlabs-2016-phishing-trends-intelligence-report-hacking-the-human/.

Pia, E. and Diez, T. (2007) 'Conflict and Human Rights : A Theoretical Framework', pp. 1–31.

Pinsent Masons (2017) *ECB's cyber incident reporting requirements individualised for 121 banks*, *Out-Law.Com Web Site*. Available at: https://www.out-law.com/en/articles/2017/october/ecbs-cyber-incident-reporting-requirements-individualised-for-121-banks/ (Accessed: 24 September 2018).

Post, D. G. (1995) 'Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace', *Journal of Online Law*, 1, pp. 3–20. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=943456.

Prime Minister's Office (2017) *Prime Minister calls for automatic blocking of terrorist content*, *Gov.UK Web Site*. Available at: https://www.gov.uk/government/news/prime-minister-calls-for-automatic-blocking-of-terrorist-content (Accessed: 27 June 2018).

Prince, C. and Sullivan, J. (2019) 'The UK Cyber Strategy Challenges for the Next Phase', *Royal United Services Institute*, pp. 1–19.

Rawnsley, A., Woods, E. and Triebert, C. (2018) *The Messaging App Fueling Syria' s Insurgency*, *Foreign Policy*. Available at: http://foreignpolicy.com/2017/11/06/the-messaging-app-fueling-syrias-insurgency-telegram-arms-weapons/ (Accessed: 18 January 2018).

Raymond, M. and DeNardis, L. (2016) *Multi Stakeholderism: Anatomy of an Inchoate Global Institution*. 41. London. Available at: ourinternet.org.

Raywood, D. (2017) *Equifax Blames Breach on Apache Struts Flaw*, *Infosecurity Magazine*.

Available at: https://www.infosecurity-magazine.com/news/equifax-blame-breach-apache/ (Accessed: 21 June 2018).

Reeve, T. (2017) 'CyberUK 2017 : GCHQ director explains NCSC ethos in parting interview', *SC Magazine*, pp. 1–5. Available at: https://www.scmagazineuk.com/cyberuk-2017-gchq-director-explains-ncsc-ethos-in-parting-interview/article/644125/.

Rice, G. (2010) 'Reflections on interviewing elites', *Area*, 42(1), pp. 70–75. doi: 10.1111/j.1475-4762.2009.00898.x.

Richards, J. (2014) *Cyber-War: The Anatomy of the Global Security Threat*. Kindle. London: Palgrave Macmillan.

Rid, T. (2013) *Cyber War Will Not Take Place*. Kindle. New York: Oxford University Press.

Rid, T. and Buchanan, B. (2014) 'Attributing Cyber Attacks', *The Journal of Strategic Studies*, 00(00), pp. 1–34. doi: 10.1080/01402390.2014.977382.

Risk Based Security (2018) 'Data breach quickview report: Data breach trends - year end 2017', (January), pp. 1–19. Available at: https://pages.riskbasedsecurity.com/2017-ye-breach-quickview-report.

Rittel, H. and Webber, M. (1973) 'Dilemmas in a General Theory of Planning', *Policy Sciences*, 4, pp. 155–169.

Roberts, N. (2000) 'Wicked Problems and Network Approaches to Resolution', *International Public Management Review*, 1(1), pp. 1–19. doi: 10.1016/S0732-1317(01)11006-7.

Roberts, N. (2006) *Syllabus: COPING WITH WICKED PROBLEMS*. Monterey, CA. Available at: https://calhoun.nps.edu/bitstream/handle/10945/34445/roberts-fall2006-navalpostgradschool-da4302.pdf?sequence=1.

Robinson, T. (2018) *Revised ' Hack Back ' bill encourages ' active-defense ' techniques , sets parameters*, *SC Magazine*. Available at: https://www.scmagazine.com/revised-hack-back-bill-encourages-active-defense-techniques-sets-parameters/article/664391/ (Accessed: 19 March 2018).

Rosemont, H. (2016) *Public – Private Security Cooperation From Cyber to Financial Crime*. London. Available at: https://rusi.org/publication/occasional-papers/public–private-security-cooperation-cyber-financial-crime.

Rosenau, J. N. (2003) *Dynamics Beyond Globalisation*. Princeton, NJ: Princeton University Press.

Rowland, J., Rice, M. and Shenoi, S. (2014) 'The anatomy of a cyber power', *International Journal of Critical Infrastructure Protection*. Elsevier, 7(1), pp. 3–11. doi: 10.1016/j.ijcip.2014.01.001.

Ruddick, G. (2017) *UK government considers classifying Google and Facebook as publishers*, *The Guardian*. Available at: https://www.theguardian.com/technology/2017/oct/11/government-considers-classifying-google-facebook-publishers (Accessed: 27 June 2018).

Rudner, M. (2013) 'Cyber-Threats to Critical National Infrastructure: An Intelligence

Challenge', *International Journal of Intelligence and CounterIntelligence*, 26(3), pp. 453–481. doi: 10.1080/08850607.2013.780552.

Schmidt, E. and Cohen, J. (2013) *The New Digital Age*. Kindle. London: John Murray (Publishers). Available at: https://www.amazon.co.uk/New-Digital-Age-Reshaping-Business-ebook/dp/B00A7YYYE2/.

Schmitt, M. N. (2012a) '" Attack " as a Term of Art in International Law : The Cyber Operations Context', *International Conference on Cyber Conflict*, (2010), pp. 283–293.

Schmitt, M. N. (2012b) 'Tallinn Manual on the International Law Applicable to Cyber Warfare', pp. 1–215. doi: 10.1017/CBO9781139169288.

Schneier, B. (2000) *Secrets and Lies*. New York: Wiley and Sons.

Schneier, B. (2013) 'The Battle for Power on the Internet', *The Atlantic*, pp. 1–9.

Schneier, B. (2015) *Data and Goliath*. Paperback. New York, NY: W.W. Norton.

Schneier, B. (2017) *Hacking Back*, *Schneier on Security*. Available at: https://www.schneier.com/blog/archives/2017/10/hacking_back_1.html (Accessed: 23 February 2018).

Schonfeld, E. (2010) *Hillary Clinton Extends Foreign Policy To The Internet And Wants Your Help*, *Tech Crunch*. Available at: https://techcrunch.com/2010/01/21/internet-freedoms-clinton-foreign-policy/?guccounter=1 (Accessed: 13 August 2018).

Schreier, F. (2012) *On Cyberwarfare*, *DCAF Horizon Working Paper*. 7. Geneva. Available at: http://www.dcaf.ch/Publications/On-Cyberwarfare.

Segal, A. (2016) *The Hacked World Order*. First. New York: Public Affairs.

Sharp, H. and Kolkman, O. (2020) *Discussion Paper : An analysis of the " New IP " proposal to the ITU*, *Internet Society Web Site*. Available at: https://www.internetsociety.org/wp-content/uploads/2020/04/ISOC-Discussion-Paper-NewIP-analysis-29April2020.pdf (Accessed: 3 June 2020).

Sheldon, J. B. (2014) 'Geopolitics and Cyber Power: Why Geography Still Matters', *American Foreign Policy Interests*, 36(5), pp. 286–293. doi: 10.1080/10803920.2014.969174.

Singer, P. W. (2008) *Corporate Warriors*. New York: Cornell Univeristy Press.

Slaughter, A. (1997) 'The real new world order', *Foreign Affairs*, 76(5), pp. 183–197. doi: 10.2307/20048208.

Small, P. E. (2011) *Defense in Depth : An Impractical Strategy for a Cyber World*, *SANS Institute Infosec Reading Room*. Available at: https://www.sans.org/reading-room/whitepapers/warfare/defense-depth-impractical-strategy-cyber-world-33896 (Accessed: 20 June 2018).

Smith, B. (2017) *The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack*, *The Official Microsoft Blog*. Available at: https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.00001a3m6z19gf27ssv2d96m5gv2n (Accessed: 27 December 2017).

Solon, O. (2017) 'Marcus Hutchins : cybersecurity experts rally around arrested WannaCry ' hero '', *The Guardian*, 11 August. Available at: https://www.theguardian.com/technology/2017/aug/11/marcus-hutchins-arrested-wannacry-kronos-cybersecurity-experts-react.

Solum, L. B. (2009) 'Models of Internet Governance', in Bygrave, L. A. and Bing, J. (eds) *Internet Governance: Infrastructure and Institutions*. New York: Oxford University Press, pp. 48–91.

Solum, L. B. and Chung, M. (2003) 'The Layers Principle: Internet Architecture and the Law', *SSRN Electronic Journal*, 79(3). doi: 10.2139/ssrn.416263.

Stalder, F. (2006) *Manuel Castells: The Theory of the Network Society*. Cambridge: Polity Press.

Standage, T. (1998) *The Victorian Internet*. Paperback. London: Orion Books.

Starr, S. H. (2009a) 'Toward a Preliminary Theory of Cyberpower', in Kramer, F., Starr, S. H., and Wentz, L. K. (eds) *Cyberpower and National Security*. Paperback. Dulles VA: Potomac Books, pp. 43–88.

Starr, S. H. (2009b) 'Towards an evolving theory of cyberpower', *Cryptology and Information Security Series*, 3, pp. 18–52. doi: 10.3233/978-1-60750-060-5-18.

Stat Counter Global Stats (2017a) *Desktop Operating System Market Share Worldwide*. Available at: http://gs.statcounter.com/os-market-share/desktop/worldwide (Accessed: 11 September 2017).

Stat Counter Global Stats (2017b) *Mobile Operating System Market Share Worldwide*. Available at: http://gs.statcounter.com/os-market-share/mobile/worldwide (Accessed: 11 September 2017).

Statista (2017) *Most famous social network sites worldwide as of August 2017, ranked by number of active users (in millions)*. Available at: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (Accessed: 11 September 2017).

Statista (2019) *Size of the cyber security market worldwide, from 2017 to 2023 (in billion U.S. dollars), Statista Web Site*. Available at: https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/ (Accessed: 28 March 2019).

Steiner, P. (1993) 'On the Internet Nobody Knows You're a Dog', *New Yorker*, July.

Stille, A. (2001) 'Adding Up the Costs Of Cyberdemocracy', *New York Times*, pp. 2–4. Available at: http://www.nytimes.com/2001/06/02/arts/adding-up-the-costs-of-cyberdemocracy.html.

Stohl, M. (2006) 'Cyber Terrorism: A Clear and Present Danger, Sum of All Fears, Breaking Point or Patriot Games?', *Crime Law and Social Change*.

Stone, J. (2012) 'Cyber War Will Take Place!', *Journal of Strategic Studies*, 36(1), pp. 101–108.

Stoup, P. (2008) 'The Development and Failure of Social Norms in Second Life', *Duke Law Journal*, 58(2), pp. 311–344. Available at: http://www.jstor.org/stable/40040654.

Strange, S. (1983) 'Cave! hic dragones: a critique of regime analysis', in Krasner, S. D. (ed.)

International Regimes. New York: Cornell Univeristy Press, pp. 337–354.

Strayer, J. R. (1970) *On the Medieval Origins of the Modern State*. Princeton. Princetoon NJ: Princeton University Press.

Suler, J. (2016) *The Psychology of Cyberspace*, *True Center Publishing*. Available at: http://truecenterpublishing.com/psycyber/psycyber.html (Accessed: 15 January 2018).

Sweney, M. (2017) *TalkTalk chief executive Dido Harding to step down*, *The Guardian*. Available at: https://www.theguardian.com/business/2017/feb/01/talktalk-chief-executive-dido-harding-cyber-attack (Accessed: 27 June 2018).

Sweney, M. (2018) *Is Facebook for old people? Over-55s flock in as the young leav*, *The Guardian*. Available at: https://www.theguardian.com/technology/2018/feb/12/is-facebook-for-old-people-over-55s-flock-in-as-the-young-leave (Accessed: 25 June 2018).

Symantec Corporation (2017) *ISTR22: Internet Security Threat Report*, *Symantec Web Site*. Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (Accessed: 3 July 2018).

Symantec Corporation (2018) *ISTR23: Internet Security Threat Report*, *Symantec Web Site*. Available at: https://www.symantec.com/security-center/threat-report (Accessed: 23 May 2018).

Symantec Security Response Attack Investigation Team (2017) *Dragonfly: Western energy sector targeted by sophisticated attack group*, *Symantec Web Site*. Available at: https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks (Accessed: 28 June 2018).

Termeer, C., Dewulf, A. and Breeman, G. (2013) 'Governance of Wicked Climate Adaptation Problems', in Knieling, J. and Leal Filho, W. (eds) *Climate Change Governance (Climate Change Management)*. Berlin: Springer-Verlag. doi: 10.1007/978-3-642-29831-8.

Termeer, C. J. A. M. *et al.* (2015) *Governance Capabilities for Dealing Wisely With Wicked Problems*, *Administration and Society*. doi: 10.1177/0095399712469195.

The White House (2018) 'National Cyber Strategy of the United States of America', (September). Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Tilly, C. (1992) *Coercion, Capital and European States, AD 1990 - 1992*. Paperback. Oxford: Blackwell.

Timberg, C., Nakashima, E. and Douglas-Gabriel, D. (2014) 'Cyberattacks trigger talk of "hacking back"', *The Washington Post*. Available at: http://search.proquest.com/docview/1610488749?accountid=13360.

Townsend, K. (2017) *Russian Outsourcing Provides Plausible Deniability for State-Sponsored Hacking*, *Security Week*. Available at: https://www.securityweek.com/russian-outsourcing-provides-plausible-deniability-state-sponsored-hacking (Accessed: 2 October 2018).

Townsend, K. (2018) *UK Warns That Aggressive Cyberattack Could Trigger Kinetic Response*, *Security Week*. Available at: https://www.securityweek.com/uk-warns-aggressive-

cyberattack-could-trigger-kinetic-response (Accessed: 12 June 2018).

Tucker, E. (2017) *DMARC Email Validation - We're Doing It All Wrong*, *Computer Weekly*. Available at: http://www.computerweekly.com/opinion/Dmarc-email-validation-were-doing-it-all-wrong (Accessed: 13 December 2017).

US Department of Defense (2011) *DOD Strategy for Operating in Cyberspace*. Washington, DC. Available at: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

US Department of Justice (2014) *U . S . Charges Five Chinese Military Hackers for Cyber Espionage Against U . S . Corporations and a Labor Organization for Commercial Advantage*, *Department of Justice Web Site*. Available at: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor (Accessed: 22 February 2018).

USG (2017) *Vulnerabilities Equities Policy and Process for the United States Government*, *White House Web Site*. Available at: https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External - Unclassified VEP Charter FINAL.PDF (Accessed: 21 June 2018).

Vaas, L. (2017) *Hackers hired for year-long DDoS attack against man ' s former employer*, *Naked Security*. Available at: https://nakedsecurity.sophos.com/2017/11/09/hackers-hired-for-year-long-ddos-attack-against-former-employer/ (Accessed: 28 June 2018).

Vaas, L. (2018) *So long ! 'The internet's most inept criminal' goes to jail*, *Naked Security*. Available at: https://nakedsecurity.sophos.com/2018/06/21/so-long-the-internets-most-inept-criminal-goes-to-jail/ (Accessed: 28 June 2018).

Valeriano, B. and Craig, A. (2018) *Realism and Cyber Conflict: Security in the Digital Age*, *E-International Relations*. Available at: https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/ (Accessed: 15 January 2020).

Valeriano, B. and Maness, R. . (2015) *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press.

Varmazis, M. (2018) *The password to your IoT device is just a Google search away*, *Sophos Naked Security Web Site*. Available at: https://nakedsecurity.sophos.com/2018/03/22/the-password-to-your-iot-device-is-just-a-google-search-away/ (Accessed: 27 September 2018).

de Vaus, D. (2014) *Surveys in Social Research*. Sixth. Abingdon: Routledge.

Vincent, J. (2016) *The UK Now Wields Unprecedented Surveillance Powers — Here's What it Means*, *The Verge*. Available at: https://www.theverge.com/2016/11/23/13718768/uk-surveillance-laws-explained-investigatory-powers-bill (Accessed: 1 October 2018).

Vupen Security (2017) *VUPEN Security Twitter Feed*, *Twitter*. Available at: https://twitter.com/VUPEN (Accessed: 12 September 2017).

van Vuuren, J. *et al.* (2016) 'Building Blocks for National Cyberpower', in Zlateva, T. and Greiman, V. (eds) *11th International Conference on Cyber Warfare and Security*. Boston, MA: Academic Conferences and Publishing International Ltd.

Waqas (2017) *Lizard Squad & PoodleCorp Founder Pleads Guilty to DDoS Attacks*, *HackRead*. Available at: https://www.hackread.com/lizard-squad-poodlecorp-founder-guilty-to-ddos-attacks/ (Accessed: 28 June 2018).

Warman, M. (2013) *George Osborne trumpets Chinese investment in London*, *Daily Telegraph*. Available at: https://www.telegraph.co.uk/technology/news/10380821/George-Osborne-trumpets-Chinese-investment-in-London.html (Accessed: 5 March 2018).

Watts, J. (2017) *Watching terrorist propaganda online to become a criminal offence , says Tory Home*, *The Independent*. Available at: https://www.independent.co.uk/news/uk/politics/terrorist-propaganda-criminal-offence-new-law-amber-rudd-streaming-watching-extremist-material-isis-a7979986.html (Accessed: 27 June 2018).

Watts, S. (2012) 'The Notion of Combatancy in Cyber Warfare', in *4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications. Available at: https://ccdcoe.org/cycon/2012/proceedings/d2r1s10_watts.pdf.

Weimann, G. (2011) 'Cyber Fatwas and Terrorism', *Studies in Conflict & Terrorism*, 34(10), pp. 765–781. doi: 10.1080/1057610X.2011.604831.

Welch, C. *et al.* (2002) 'Corporate elites as informants in qualitative international business research', *International Business Review*, 11(5), pp. 611–628. doi: 10.1016/S0969-5931(02)00039-2.

WGIG (2005) *Report of the Working Group on Internet Governance*. Geneva. Available at: https://www.wgig.org/docs/WGIGREPORT.pdf.

Whittaker, Z. (2012) *Who owns your files on Google Drive?*, *CNET*. Available at: https://www.cnet.com/news/who-owns-your-files-on-google-drive/ (Accessed: 23 January 2018).

Wiedeman, R. (2017) *Gray Hat*, *New Yorker Magazine Web Site*. Available at: http://nymag.com/selectall/2018/03/marcus-hutchins-hacker.html (Accessed: 19 March 2018).

Williams, M. C. (2003) 'Word, Images, Enemies? Securitization and International Politics', *International Studies Quarterlyudies Quarterly*, 47(4), pp. 511–531. Available at: http://www.jstor.org/stable/3693634.

Winn, N. (ed.) (2004) *Neo-Medievalism and Civil Wars*. London: Frank Cass Publishing.

Wintour, P. (2018) *Russian bid to influence Brexit vote detailed in new US Senate report*, *The Guardian*. Available at: https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report (Accessed: 3 July 2018).

Wired (1997) *CATALONIA TRYING TO ESTABLISH ' VIRTUAL STATE '*, *Wired*. Available at: https://www.wired.com/1997/04/catalonia-trying-to-establish-virtual-state/ (Accessed: 17 October 2017).

Wittes, B. and Blum, G. (2016) *The Future of Violence: Robots and Germs, Hackers and Drones: Confronting the New Age of Threat*. Paperback. Stroud: Amberley.

Wu, T. (1998) 'Cyberspace Sovereignty? - The Internet and the International System',

Harvard Journal of Law & Technology, 10(3), pp. 647–666.

Wu, T. and Goldsmith, J. (2006) *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press.

Zerechak, J. (2012) *Code 2600*. USA: ZyPIX. Available at: www.code2600.com.

Zerodium (2018) *Our Exploit Acquisition Program*, *Zerodium Web Site*. Available at: https://www.zerodium.com/program.html (Accessed: 21 June 2018).

Zetter, K. (2016) *Apple's FBI Battleis Complicated. Here's What's Really Going On.*, *Wired*. Available at: https://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/ (Accessed: 20 February 2018).

Zuckerman, E. (2010) 'Intermediary Censorship', in Deibert, R. et al. (eds) *Access Controlled*. Paperback. Cambridge MA: MIT Press, pp. 71–85.

Appendix C: Participant F Meeting Notes

1. NCSC struggling for a role.
2. Not enough funding to set up a proper agency
3. Potentially falling back on looking after public sector rather than looking at private sector.
4. Less work being done with CNI than before NCSC
5. UK Government not getting to grips with cyber
6. Too many changes of personnel in government for consistent approach
7. Too many different departments – DCMS, Cabinet Office
8. Government lacking skills and suitable background – Cabinet Office
9. Government too slow to deal with cyber
10. Outdated government systems and data architectures. Public sector a mess in some areas
11. Maybe a possible approach to move all cyber into Military
12. Not sure whether being part of GCHQ is a help or a hindrance to NCSC
13. Partnership not defined
14. NCSC not clear what they want from private sector or what they want to do for the private sector
15. Partnership seems to involve providing people and skills for free. Not clear what the upside is.
16. Attacks becoming more targeted and less opportunistic
17. There is no long term government plan
18. Reactive rather than proactive
19. Government has a huge responsibility especially around offensive cyber and controls
20. NCSC in information gathering role – trying to discover what private sector does and where they can fit
21. Private sector push back from first NCSC initiatives may have changed approach
22. What we think we see as "criminal gangs" may well be state agencies
23. Concern over proliferation, blowback, control

24. Seeing same attacks coming back at same point - need for pattern recognition and predictive defence
25. State v state attack is 'war' – otherwise difficult to categorise it as such.
26. Difficult to distinguish war v crime
27. Difficult to distinguish public and private - infrastructure and responsibility/actors
28. There are malicious actors who just want to destroy things – e.g. Shamoon Saudi Aramco attack.
29. Difficult for private sector to defend against state level capabilities – e.g. Eternal Blue example
30. Legacy systems particularly difficult to identify all vulnerabilities - especially if old systems now being connected to Internet - ICS/SCADA examples
31. Cyber is now a part of all conversations with customers
32. Many organisations not aware of the scale of the problem they face
33. Data leakage via social media is becoming a major issue - reputational damage and accidental leakage of sensitive information

Appendix D: Example Edited Transcript

Oil and Gas sector, Critical National Infrastructure.

Thursday 27th April 2017

Start time: 11 a.m.

Duration: 58 minutes.

To what extent is cyber security a collaborative effort? Is it a sectoral approach that is most effective?

It is helpful to be able to speak with other organisations in the same sector but the issues transcend sectors. Attackers don't really care who it is they are attacking in whether it is out of malice, to make money, or to damage a country or an industry. Not bothered about who they are attacking as long as they are making money or getting what they want. While there are commonalities across the industry that are quite useful it is not the whole story.

Do you see targeted or opportunistic attacks?

Attacks are both opportunistic and targeted. There are a whole set of attackers who will just go for the easy target and does tend to be the ones with the lower skill level. We do see the more targeted attacks. There are attackers who have specialist skills related to an industry or a specific company. They we use that inside information that they think they have to craft a specific attack. We see it right across the spectrum there are targeted attacks and the more generic attacks.

How does the relationship with government help in the work you are trying to do?

Government is useful as a broker to bring together competitors as it can be a very sensitive issue speaking to a competitor especially when it can be construed as an anti-competitive activity under antitrust law so having a government bring together competitors can be very useful to allow discussions without concerns of accusations of anti-competitive behaviour.

Secondly, there are the introductions that can be made to bring the right people together, for example if I wanted to approach another company to discuss a specific issue I wouldn't necessarily know who to go to. I can approach advisers in government to find out who the right people are to speak to, for example, who has the same type of industrial control systems that we use who I could ask a question of. Also, in the past they have commissioned reports from consultants for example in records on how to protect industrial control systems that were given to all companies operating critical infrastructure in the UK. Commissioning these reports on our own would be very expensive for us.

How much of a role is there for the vendors in this?

Critical infrastructures groups and invited vendors to be able to understand their patching strategies and future development plans with all their potential customers in the room. Vendors can also work through this forum if they have any ideas they would like to test with their customers for a security improvement possibility. As a customer you can also hear all the other customers' responses to the ideas so we can quickly get an idea of whether particular ideas will fly.

We normally work with security specialist within ICS vendors rather than generic security providers. ICS systems have a very long life and changes are incremental and slow. Patching is a much slower cycle.

The development cycle for control systems is much slower than the development of new threats. It is a soft underbelly for attacks, so much stronger controls are put in place such as air gaps, controlled remote access, firewalls and the like. We have developed strategies to enable systems to catch up with the threat as we cannot just replace them as they are so integral to the process.

What areas are easier to work with other people – such as information sharing?

There is a common enemy here which is much easier to discuss without commercial issues. Security staff are generally not dealing with commercial issues – they are keeping systems safe which is a common concern for everyone.

There are commercial drivers for collaboration in terms of shared business interests and although we would not discuss commercial or contractual issues concerning common systems we would discuss techniques for protection, security infrastructure, incidents and threats.

Is there a state obligation to protect CNI rather than industry itself?

Private industry owns much of the infrastructure and so it has to be a partnership – there is no other option short of renationalisation. Government would rather see private industry deal with it, although they have a strong interest in ensuring that happens and keeping an eye on it and being aware of an area of infrastructure that is falling behind. Regularly have discussions with government who want to hear what is being done. Other mechanisms as well in terms of security assessment processes where a team will be sent in to a plant and carry out an assessment, collaboratively with you, to get reassurance that things are in hand. We are happy to cooperate with that but as government has little of the critical infrastructure it has to be a collaborative effort.

Conversations are normally constructive, and companies will generally try to satisfy government requirements. If any assessment is felt to be unreasonable or lead to unnecessary demand, then the relationship is mature enough to be able discuss that and develop a mutually acceptable plan. We can have a trusted conversation and know that any insights we give to them will not result in unwanted publicity or

unreasonable use of the information. There is a sensible and mature approach and everyone involved sees the benefits of keeping the conversation at the right level.

Nation state Attacks. Is that a government issue?

Government are most likely to be able to identify a specific attack and attacker. We will see the symptoms and indicators of compromise, but we may not know what it is, whereas government may have seen the same symptoms on other systems and know that it indicates a specific attacker and be able to propose mitigation strategies. There would be an exchange of information on future incidents. We place attack information on CiSP and government can provide responses to that.

Are there areas where government activity has a negative effect?

The amount of change and reorganisation in government and movement of people that makes it difficult. When you finally build a relationship with someone they are moved to another function. Unfortunately it is part and parcel of dealing with government.

Where they can really mess things up is when they have the potential to publish information without permission. You have to be sure you can trust the people you are dealing with and that they understand the issues involved. Have not personally had any issues but aware of others and have to be careful. One breach of trust and all this collapses.

Do state agencies have a clear understanding of your issues?

Not always. The most difficult agency to deal with is law enforcement. They see things so differently to everyone else. Their interests are different to everyone else working in this area. Their sole focus is arrest and conviction. If there is any collateral damage then just too bad. Their attention span is also very short. They are very busy, focused on particular targets and conversations that you have are largely forgotten the next week as a result of that focus. Trying to report anything is a fraught process – you want to help and report incidents but they make it very difficult. Portals like Action Fraud are aimed at the general public and don't make it easy to report incidents at a corporate level. The information they ask for is inappropriate and you lose complete control. There is no agreement with a law enforcement officer about things not going any further – as soon as you say something it can be used for anything and it can be attributable – your name will be attached to it. We have had attempts over the years to bring law enforcement into the conversation and that works for a few months until that officer gets moved on to another job or inquiry and then it's back to square one.

By its very nature they will not discuss anything with you.

Is 'hacking back' an operational option.

Hacking back is not an option. We don't have the time or the expertise to do that. As soon as we stop an attack we lose interest in it apart from what lessons can be learned. We're not interested in who the attackers are really. If we know who they are and there is information that may help attribution then we will report it via CiSP and they will do what they will with it – but that's as far as it goes. We don't have the staff or the interest in going after anybody. That's not our role.

Has there been any noticeable change out of the formation of the NCSC?

At the point it has distracted a lot of people. They are more inward looking for the time being while they find out their new role and what their job is. There is a bit of confusion. They do know how to engage with the private sector. We have been dealing with a group of people who even with different roles have often been the same people.

Is it helpful for the NCSC to be part of GCHQ?

In theory it should be, but the jury is out as it is early days.

Do you see a greater role for CSPs in terms of what they can do on the network?

One irritation with the ISPs is how difficult they make it to get fraudulent domains shut down. We could do better there between private industry and the CSP/ISPs. We do not have a very good relationship where they would be able to take trusted information from us. If I need domains taken down quickly that could be anything between 48 hours and never and there is no reason it needs to take weeks to remove an obviously fraudulently domain. Would like to see a better control and process on setting up domains, but it is too easy to set up a fraudulent domain. It seems as if people can set up the most ridiculous fraudulent domains.

Will GDPR make a big difference?

We are aware of it and it is a noticeable issues that is getting attention, but in an industry with no end user customers and not dealing with the general public, the extent of responsibility is mainly employees and ex-employees so compared to many others it is a relatively minor issue.

What are the big worries?

The attacks that have happened to other people such as Saudi Aramco attack targeted on one company that has affected almost their entire IT stock in one go. That could cripple us. We are aware of weaknesses such as a lack of diversity in client operating systems and an attack with a zero day that moves horizontally between PCs is the doomsday scenario. We know of ways that this could happen – people have to do their jobs and we have to walk a line between enough control to stop the bad guys but enough leeway to do their jobs.

Desk access to social media and webmail is an example of where it would make sense to block it but it may be a step too far. Segmented wireless networks with a 'dirty network' where people can access almost anything, but segments with much more control.

Risk of proliferation of personal devices with dubious security controls.

Worst case scenario of an attack that sits quietly while it spreads and then hits everything.

Future needs with the state

Don't do anything to destroy the trust that has been built up.

Improve the relationship with law enforcement and publish to industry thetype of information that would be helpful to them. Give us a hint as to what yo0u;re interested in and the provide a mechanism for that to be provided. We cannot pass information on every attack and get no feedback. We have limited resources and will help when we can with intelligence and have to trust that the information will not be misused or used in a reckless way that breaks trust.

An equal collaboration is essential.

End.

Appendix E: Documentation Sent to Research Participants in Advance of the Interview

The main document sent to the participants in advance of the interview was a summary document outlining the themes that would form the basis of the semi-structured interview.[45]

This was useful in ensuring that participants were able to make an informed agreement to participate in the interview, and to enable them to consider the subject beforehand, although it was also the reason why at least two potential participants declined to be interviewed, after originally agreeing to the interview before receiving the documentation.

Interview Themes

The interview is designed to look at a number of themes, including:

- Relationships external to the organisation that are key to cyber security.
- Cyber-threats and threat actors
- Threat responses
- Private sector cyber security providers
- Engagement with state organisations
- State activity in cyberspace
- Law enforcement in cyberspace
- International issues

The interview will be treated as anonymous and any reference to the participant will be in a way that prevents direct attribution.

The interview is being recorded and a transcript will be provided if it has been requested.

Context and Relationships

Firstly, to what extent is cyber security an issue that is internal due to commercial sensitivity and to what extent is it a shared community activity?

[45] Note that the formatting of this has been edited to more closely match that of the thesis document, but the content remains the same.

Do these sensitivities have a material effect on the ability to work with others?

In what ways do you work with other organisations?

Is there a clear shared understanding of the issues, in particular with government sponsored organisations?

Cyber Risks/Threat

Can you tell me what you see as the most significant risks for organisations in cyber security at the moment for you?

Are these risks different from what you would have seen say two years ago?

In terms of types "cyber-attacks", what type of attacks do you see as the main concerns?

And in terms of attack vectors, what gives you the most concern?

Can you tell me something about the types of assets you see as being under the most threat from cyber-attack – either in terms of your own organisation or in general?

In terms of "cyber attacks", to what extent do you see attacks as being targeted as opposed to opportunistic?

What would improve the understanding of the risks of the cyber-threat?

Is the cyber security threat accurately reflected by the cyber security industry?

Threat Actors

Who do you see as the main 'threat actors'?

Are the threat actors significantly different by sector?

What are the key motivations of threat actors?

Are there any threat actors that are of particular concern above others?

Are there specific threats from attacks directly by nation states (or sponsored by nation states)?

Which threats would most benefit from state engagement?

Threat Response

What are the major challenges in responding to cyber threats?

How effective are the products available from the cyber security industry to defend against cyber-threats - in terms of products and services available in the market?

Does the state have a role to encourage solutions to be developed, or to approve existing products and services?

How does the changing nature of the threats effect the capability to defend itself?

Can the private sector react as quickly as the threat adapts?

And the state?

How could the effectiveness of the defensive elements be improved?

Government Engagement

What obligations do you feel government has to the private sector in cyber?

Is there an obligation on the government to defend the CNI – either in terms of protection or detection?

Is there a place for greater cyber regulation?

How do you think GDPR will impact cyber in the UK?

Has the private sector been guilty of not taking cyber security seriously enough in the past?

Has the state been guilty of not taking cyber security seriously enough in the past?

Does the potential role of the state change depending on cyber security function? (So for example within the NIST framework core functions of Identify, Protect, Detect, Respond, Recover?)

Are there areas where state engagement with the private sector has been more successful?

Are there areas where state engagement with the private sector has been distinctly unsuccessful?

How do you view the role of law enforcement agencies in cyber security?

Norms of Behaviour

To what extent are there state activities which are detrimental to a secure cyberspace?

What limits are there on state activities in cyberspace? Where do impacts on privacy and civil liberties start to limit cyber security?

What limits are there on defensive activity by private organisations? Where is the line between defence and offence?

Where would you place 'electric fences' or 'hacking back' for example? Are these even realistic concepts?

Should the state be in a position to use offensive cyber capabilities?

Do offensive capabilities create an unacceptable risk for civilians?

Does the state have a role to play in recovery from cyber-attacks on private organisations? Is there potential for government backed 'reconstruction' funds or government insurance?

Is the state right to insist on the need to respond in kind to state cyber-attacks?

Does the concept of cyber-deterrence make sense?

Cyber and National Security

How do you view the recent introduction of the NCSC and its activities?

Is it helpful for the NCSC to be a part of GCHQ?

To what extent should private organisations be expected to take national security issues into account in their cyber strategies?

What is your view of the state's current effectiveness in terms of responding to cyber-attacks?

Other Organisations

What other organisations should be engaged in cyber security?

What role do ISPs and CSPs have to play as communications infrastructure providers?

What is the role of the Internet Governance organisations? Are they effective?

Final Questions

If you were in charge of Government cyber security activity what would you prioritise?

What cyber security concerns are there that keep you awake at night?

Appendix F: Speech Act Thematic Coding Example (Osborne)

This appendix includes the example of the text analysis for the derivation of key themes. This particular example shows the speech by George Osborne at GCHQ in 2016 where the creation of the NCSC was announced. This is a useful example as it represents a significant moment in the development of the UK cyber security capability.

1. Thank you. Before I start my speech, I want to say a few words about the heart-breaking events that unfolded in Paris on Friday evening. This was an assault not just on the people of France, but on all of us who value freedom and democracy. We stand with the people of France. We know that we must act as one, just as our enemies see us as one. As David Cameron has said, we will do everything we possibly can to help the French at this moment of national trauma. That includes making available to them the sharpest of our own national capability, which includes the skills and capabilities of GCHQ.
2. Before the dreadful events of the weekend we had already indicated that we would be increasing substantially the resources we dedicate to countering the terrorist threat posed by ISIL. The Prime Minister has made clear that across the agencies a further 1,900 staff will be recruited to keep Britain safe from terrorist attack.This was going to be an important outcome of the Spending Review. What has unfolded in Paris has reminded us all that it is a vital one too.
3. As the threat develops, we will need to make sure that our capabilities develop to match it. Following what happened to the Metrojet flight from Sharm, the Prime Minister announced that we would be doubling the amount we spent on aviation security. The answer is not just in more resources, but in ensuring those who keep us safe have the right legal framework, that allows them to do their job while preserving the values and freedoms which we are so determined to defend. Through the Investigatory Powers Bill, HM Government will make sure that they have the powers they need to access vital intelligence about the intentions and activities of those who wish us harm.
4. This determination to confront threats against our country is at the heart of what you do here at GCHQ. To the men and women of GCHQ in this audience – the TV cameras today will not show your faces, and the public will never know your names, but let me

say this: you are the unsung heroes who never get the recognition you deserve by dint of the sort of work you do, but who day and night keep us safe. One of the ways you keep us safe is by tracking terrorist groups and collecting the information we need to stop those attacks. Our intelligence agencies historically disrupt one terrorist plot a year; this year you have prevented seven. Let me thank you on behalf of the British people.

5. I also want to thank those of you in the audience who are here because you are our partners in keeping Britain safe in cyberspace – not just those from GCHQ, but across government, the armed forces, industry, and academia. For this is a shared effort between us. Earlier this year the Prime Minister asked me to chair the government's committee on cyber, and through that I see the huge collective effort required to keep our country safe from cyber attack; the range of threats we face; and how this will be one of the great challenges of our lifetimes.
6. As Chancellor I know about the enormous potential for the internet to drive economic growth, but I am also acutely aware of the risk of cyber attack harming our economy and undermining the confidence on which it rests. And I also know that we can't afford to build strong cyber defences unless they rest on the solid foundations of sound public finances.
7. Next week I will present the conclusions of the Spending Review that will deliver those solid foundations. We have already reached provisional agreement with four departments, and today I can confirm we have provisionally settled a further seven Whitehall departments: the Department for Energy and Climate Change; the Department for Work and Pensions; HM Revenue and Customs; the Cabinet Office and the Scotland, Wales and Northern Ireland offices
8. This means that over half of the Whitehall departments have now reached provisional agreements on their resource budgets. Combined, these departments will on average see a reduction in real terms spending of 24% by 2019-20, contributing to our economic security and enabling us to spend more on key priorities like national security. I've been very clear that we cannot afford national security without economic security. But as we have seen in recent months and weeks, there will be no economic security for

our country without national security. Nowhere is that more true than when it comes to cyber.

9. When I was born the internet was barely two years old. It was the preserve of academics, used to connect dozens rather than billions of users. There weren't many who predicted it would transform our world. Today, the internet has changed our lives in countless ways, and continues to evolve at a pace that would have stunned even its own pioneers. Every part of the way we live is being touched and reshaped by it. Britain helped create the internet – Tim Berners Lee created the World Wide Web, one of a long line of British scientists who have given us an outsized role in shaping our own digital future.
10. Britain is enriched by the internet. And Britain has embraced the internet – a far higher proportion of British retail is done online than in any other country in the world. That's an enormous economic and commercial opportunity for our country. But when the internet was first created, it was built on trust. That trust, appropriate inside a community of scholars, is not merited in a world with hostile powers, criminals and terrorists.
11. The internet has made us richer, freer, connected and informed in ways its founders could not have dreamt of. It has also become a vector of attack, espionage, crime and harm. And that's what I want to talk to you about this morning. For government has a duty to protect the country from cyber attack, and to ensure that the UK can defend itself in cyberspace.
12. Today I want to set out how we are fulfilling that duty. I will explain how we have invested in Britain's cyber security in the past five years, and to set out our plan for the next five. The national cyber plan I am announcing means investing in defending Britain in a cyber-age. It is a key part the Spending Review I will deliver next week. For the Review is all about security: economic security, national security and the opportunity that comes to a country that provides that security. It is right that we choose to invest in our cyber defences even at a time when we must cut other budgets.
13. For our country, defending our citizens from hostile powers, criminals or terrorists, the internet represents a critical axis of potential vulnerability. From our banks to our cars, our military to our schools, whatever is online is also a target. We see from this

place every day the malign scope of our adversaries' goals, their warped sophistication and their frenetic activity. The stakes could hardly be higher – if our electricity supply, or our air traffic control, or our hospitals were successfully attacked online, the impact could be measured not just in terms of economic damage but of lives lost.

14. ISIL's murderous brutality has a strong digital element. At a time when so many others are using the internet to enhance freedom and give expression to liberal values and creativity, they are using it for evil. Let's be clear ISIL are already using the internet for hideous propaganda purposes; for radicalisation, for operational planning too. They have not been able to use it to kill people yet by attacking our infrastructure through cyber attack They do not yet have that capability. But we know they want it, and are doing their best to build it.
15. So when we talk about tackling ISIL, that means tackling their cyber threat as well as the threat of their guns, bombs and knives. It is one of the many cyber threats we are working to defeat. Getting cyber security right requires new thinking. But certain principles remain true in cyberspace as they are true about security in the physical world. Citizens need to follow basic rules of keeping themselves safe – installing security software, downloading software updates, using strong passwords. Companies need to protect their own networks, and harden themselves against cyber attack.
16. The starting point must be that every British company is a target, that every British network will be attacked, and that cyber crime is not something that happens to other people. And government cannot duck its responsibilities. There are certain things that only government can do, in cyberspace just as in the physical world. Government has a unique ability to aggregate and educate. Only government can legislate and regulate. Only government can collect secret intelligence.
17. Government has a duty to protect the country from hostile attack. Government has a duty to protect its citizens and companies from crime. Only government can defend against the most sophisticated threats, using its sovereign capability. And that's exactly what we will do. And it is this sovereign capability that brings me here, to GCHQ. Through my time in office, I have seen for myself the extraordinary quality of

this institution; the dedication, integrity and ingenuity of its staff; and the difference it makes protecting our nation.

18. Coming here, as the first Chancellor to give a speech in GCHQ, I am acutely conscious of the rich history of this still relatively young institution in our island's story. The father of GCHQ was Winston Churchill. It was as First Lord of the Admiralty that he established Room 40, and gave it its charter. Room 40 was an operation to decrypt German communications during the First World War, a secret held on extraordinarily close hold even within government.
19. By 1924 Winston Churchill had become Chancellor of the Exchequer, and wrote to Prime Minister Stanley Baldwin saying: In the years I have been in office since Room 40 began in the Autumn of 1914, I have read every one of its flimsies, and I attach more importance to them as a means of forming a true judgement of public policy in these spheres than to any other source of knowledge at the disposal of the state. Churchill went on to complain that other ministers in the government had access to this information but that as Chancellor he did not, and that they therefore might have been pulling the wool over his eyes.
20. Some things have changed since those days. As a member of the National Security Council I see the crucial role that information produced by GCHQ can play in the conduct of government and war. Other things haven't changed – like the continuing attempts by spending departments to pull the wool over the eyes of the Chancellor. A hundred years on, they still haven't learnt that it never, ever works. GCHQ is rightly known as equal to the best in the world. And I am clear that the answer to the question 'who does cyber?' for the British government is – to very large degree – 'GCHQ'.
21. Of course there are others involved – the other intelligence agencies; the National Crime Agency; the Ministry of Defence; DCMS; the FCO. Often in partnership with our Allies overseas, like the US and France. It's very good to see Matthew Barzun the American ambassador here this morning. But GCHQ has a unique role. It is the point of deep expertise for the UK government. It has an unmatched understanding of the internet and of how to keep information safe.
22. It is a centre of capability that we cannot duplicate, which must sit at the heart of our cyber security. Over the past 18 months, for example, GCHQ has helped UK law

enforcement tackle a number of high-profile operations against pernicious cybercrime malware threats, like Dridex, Shylock and GameOver Zeus. These have cost UK citizens and companies and government departments millions of pounds in the form of fraud, theft and damage; this figure would have been much higher had it not been for law enforcement disrupting these operations with GCHQ's help.

23. I can tell you today that right now GCHQ is monitoring cyber threats from high end adversaries against 450 companies across the aerospace, defence, energy, water, finance, transport and telecoms sectors. In protecting the UK from cyber attack, we are not starting from zero. In 2010, at a time when we as a new government were taking the most difficult decisions on spending in other areas, we took a deliberate decision to increase spending on cyber. We set up the National Cyber Security Programme and funded it with £860 million.
24. And for the past five years we have been creating and enhancing the structures and capabilities that Britain needs to defend itself in cyberspace. We have invested in building our sovereign capability here at GCHQ. We have ensured that our military systems are properly secured from cyber attack. We have built the National Cyber Crime Unit so cyber criminals are brought to justice. We established the Computer Emergency Response Team for the UK, and the Cyber Information Sharing Partnership so companies could share what they knew.
25. We developed clear guidance for businesses, including the Cyber Essentials scheme, which already has over a thousand companies accredited. We launched a series of cyber risk reviews for companies in the Critical National Infrastructure, to identify vulnerabilities that could then be addressed. We built cyber security into every stage of the education process. We established Cyber First and cyber apprentices to make sure that we got the talent we needed coming into the field.
26. And we undertake exercises so we know what to do when there is a serious cyber incident. One such exercise took place last week – Resilient Shield, a joint UK/US exercise across the financial sector. So I want to thank all those who, over the last five years, have brought us to where we are today. We have built a world-class range of tools and capabilities that Britain needs to stay safe from cyber attack. We are widely regarded as top or near top in the world.

27. But nice though it would be to sit on our laurels, the truth is that we are not where we need to be. We are not winning as often as we need to against those who would hurt us in cyberspace. The truth is that we have to run simply to stand still. The pace of innovation of cyber attack is breathtakingly fast, and defending Britain means that we have to keep up.
28. At the heart of cyber security is a painful asymmetry between attack and defence. It is easier and cheaper to attack a network than it is to defend it. And the truth is that this asymmetry is growing. A few years ago, mounting a sophisticated cyber attack meant having all the skills that each stage of the attack required, from gaining access to the network to designing the payload that was to go into it.
29. But in the past few years, an on-line market-place has developed, which means all the elements of an attack can now be bought and assembled from the computer of anyone with the money to pay for it. The barriers to entry are coming right down, and so the task of the defenders is becoming harder. All of this is reflected in the cyber breaches that we see reported with increasing frequency and severity.
30. Last summer GCHQ dealt with 100 cyber national security incidents per month. This summer, the figure was 200 a month. Each of these attacks damages companies, their customers, and the public's trust in our collective ability to keep their data and privacy safe. Imagine the cumulative impact of repeated catastrophic breaches, eroding that basic faith in the internet that we need for our online economy and social life to function. As a nation determined to live within our means, we are facing painful choices, and the hardest of decisions.
31. You will see that next week. But the Prime Minister, my colleagues at the top of government and I have decided that we have to make a top priority of cyber security, if Britain is to be able to defend itself, now and in the future. Today I am announcing a plan to do precisely that. It is a bold, comprehensive programme that will give Britain the next generation of cyber security, and make Britain one of the safest places to do business online.
32. It will give our companies and our citizens confidence that their cyber-safety is being properly protected. It will ensure that Britain remains at the cutting edge of the global cyber economy. In the Spending Review, I have made a provision to almost double

our investment to protect Britain from cyber attack and develop our sovereign capabilities in cyberspace, totalling £1.9 billion over five years. If you add together the spending on core cyber security capabilities, protecting our own networks and ensuring safe and secure online services, the government's total cyber spending will be more than £3.2 billion.

33. That money by itself is not enough. It supports a national cyber plan. The plan consists of five major steps forward in the nation's cyber defence. The most fundamental thing we need to do is defend ourselves online, and we are developing a series of measures to do so more actively. We will be stepping up our efforts to disrupt the criminal marketplace, and making sure that anyone committing cyber crime against our citizens and companies will be brought to justice. We will be boosting the capabilities of the National Cyber Crime Unit, so that – in partnership with their counterparts around the world - they attack the assumption among too many that cyber crime is risk free, and comes with little risk of consequences.
34. We will introduce stronger defences for government systems. We will aggressively defend our public services from cyber attack by installing capabilities that can detect attacks, find where our services are vulnerable to attack, and fix them. We will introduce a cross-government IP Reputation Service – warning government websites when they try to do business with known bad addresses. We have done this already with HMRC, and saved £40 million on fraud on a £1 million investment. But we can go further.
35. Internet service providers already divert their customers from known bad addresses, to prevent them from being infected with malware. We will explore whether they can work together – with our help – to provide this protection on a national level. We cannot create a hermetic seal around the country – indeed it wouldn't be in our interests to have one – but with the right systems and tools our private internet service providers could kick out a high proportion of the malware in the UK internet, and block the addresses which we know are doing nothing but scamming, tricking and attacking British internet users
36. Let us try to get to the point where all the internet service providers will as a matter of routine divert known bad addresses. By doing so, we could fundamentally alter the

economics of cyber crime against UK citizens and businesses. Second, we need to address the alphabet soup of agencies involved in protecting Britain in cyberspace. As the threat has emerged, so have they. Now we need to bring more coherence to our efforts, so that businesses know there is a single place they can go for advice and help.

37. Today I can announce that in 2016 we will establish a single National Cyber Centre, which will report to the Director of GCHQ. The Centre will be a unified source of advice and support for the economy, replacing the current array of bodies with a single point of contact. The Centre will make it easier for industry to get the support it needs from government. And make it easier for government and industry to share information on the cyber threat to protect the UK. Reporting to GCHQ will mean the Centre can draw on the necessarily secret world-class expertise within this organisation.
38. But the Centre will also have a strong public face and will work hand in hand with industry, academia and international partners to keep the UK protected against cyber attacks. And over time, we will build several important capabilities in the new Centre. It will give us a unified platform to handle incidents as they arise, ensuring a faster and more effective response to major attacks. And we will build in the National Cyber Centre a series of teams, expert in the cyber security of their own sectors, from banking to aviation, but able to draw on the deep expertise here, and advise companies, regulators, and government departments.
39. Building the National Cyber Centre will be a hugely ambitious and important undertaking that reflects this government's commitment to making the UK secure in cyberspace. The third part of the plan is about the most important raw material. We will never succeed in keeping Britain safe in cyberspace unless we have more people with the cyber skills that we need. This year's Global Information Security Workforce Study estimates that the global cyber security workforce shortage will widen to 1.5 million by 2020.
40. If we do not act decisively, the skills gap will grow, and limit everything we want to achieve in cyberspace. So we will launch an ambitious programme to build the cyber skills our country needs, identifying young people with cyber talent, training them, and giving them a diversity of routes into cyber careers. Training the next generation

of coders is vital – both for our economy and our security. Today I can announce that, as part of the Spending Review we will be running a £20 million competition to open a new Institute of Coding to fill the current gap in higher education and train the next generation in the high level digital and computer science skills that we need.

41. We will invite bids – including joint bids – from our universities, businesses and others who have the innovative ideas to bring these proposals to life. As all of you who work in the sector know, what is needed are specific cyber security skills, building on particular talents. And we need to tackle this problem on a number of fronts including in our universities. But we need to make sure there are other routes into the cyber workforce. So we will build higher and degree level apprenticeships in key sectors, starting with the finance and energy sectors. We will create a retraining programme for highly skilled workers who want to move into cyber.
42. And most ambitiously, we will be rolling out a major programme for the most talented 14 to 17 year olds, involving after-school sessions with expert mentors, challenging projects, and summer schools where those on the scheme can see where their cyber skills can take them. Modelled on a hugely successful Israeli programme, this scheme will help us draw on the great hidden talents in our classrooms and bring on our nation's cyber potential.
43. Of course, we need not just great skills but great British companies as well. If Britain is to be a world leader in cyber, and stay at the cutting edge of cyber technology, we need the innovation and vigour that only these companies can offer. We need to create a commercial ecosystem in which cyber start-ups proliferate, get the investment and support they need, and are helped to win business around the world. We need an ecosystem in which our best people move in and out of institutions like this one, bringing the best minds and deepest expertise into the private sector, and the latest innovation back into government.
44. We need an ecosystem in which great ideas get translated into great companies. So the fourth element of the plan is to set up programmes to support the best cyber start-ups – excellent British companies like GlassWall, Garrison, Digital Shadows and Titania, who I am glad to see here with us. I am glad that there is already so much happening in this space; I am happy we have the founders of Cyber London with us today.

45. And I am delighted that Paladin Capital has just announced it is establishing a dedicated cyber fund in the UK; we can be proud that they have chosen London as its base. We will build on this energy. We will help commercialise the extraordinary innovation in our universities. We will provide training and mentoring for our cyber entrepreneurs. We will be establishing two cyber innovation centres - places where cyber start-ups can base themselves in their crucial early months, and which can become platforms for giving those start-ups the best possible support.
46. I have talked before about an arc of cyber excellence – stretching from this building, through Bristol and Bath to Exeter – to make the South West a world leader in Cyber Security. Today I can announce that one of the two innovation centres will be here in the South West of England, in Cheltenham, reflecting the extraordinary talent in this place, and our aspiration that this talent should help drive our cyber sector. Government can itself provide a huge boost for British cyber start-ups, if it can be smart enough to marshal its procurement in a coherent way. This should be a win-win – our cyber start-ups need endorsement, investment and first customers.
47. And government, from our military and GCHQ to the Government Digital Service and the NHS, need to be able to procure excellent cyber security hardware and services. So I can announce today that we will create a £165 million Defence and Cyber Innovation Fund, to support innovative procurement across both defence and cyber security. It will mean that we support our cyber sector at the same time as investing in solutions to the hardest cyber problems that government faces.
48. Of course, our involvement with industry on cyber goes well beyond the cyber sector. We need to make sure that Britain has the regulatory framework it needs, particularly in the sectors we define as the Critical National Infrastructure. If the lights go out, the banks stop working, the hospitals stop functioning or government itself can no longer operate, the impact on society could be catastrophic. So government has a responsibility towards these sectors, and the companies in those sectors have a responsibility to ensure their own resilience.
49. Any new regulation will need to be carefully done – light enough and supple enough that it can keep up with the threat, so it encourages growth and innovation rather than suffocates it. Our vulnerability as a nation in cyberspace goes well beyond the critical

national infrastructure. The impact of last year's attack on Sony should be a warning to anyone who thinks that such attacks are just a matter for the companies concerned. We have a collective interest in the cyber defences of individual companies across the British economy.

50. The experience in the last month of TalkTalk shows how cyber attack can suddenly go from a theoretical risk to a massive business cost. We will work with businesses across the economy to ensure that they have the right defences in place. All of this sets out what we will do to establish the strongest possible defences for Britain. Strong defences are necessary for our long-term security. But the capacity to attack is also a form of defence. If we are to tackle the asymmetry between attack and defence, then we need to establish deterrence in cyberspace.
51. We need not just to defend ourselves against attacks, but rather to dissuade people and states from targeting us in the first place. Part of establishing deterrence will be making ourselves a difficult target, so that doing us damage in cyberspace is neither cheap nor easy. Part of establishing deterrence will be building global norms, so that those who do not follow them can be called out, and shown to be acting outside the boundaries of acceptable behaviour.
52. And part of establishing deterrence will be making sure that whoever attacks us knows we are able to hit back. We need to destroy the idea that there is impunity in cyberspace. We need those who would harm us to know that we will defend ourselves robustly. And that we have the means to do so. This is the fifth element of the plan. Thanks to the investment that we have made during the last Parliament, just as our adversaries can use a range of actions against us, from the virtual to the physical, so we are making sure that we can employ a full spectrum of actions in response.
53. We reserve the right to respond to a cyber attack in any way that we choose. And we are ensuring that we have at our disposal the tools and capabilities we need to respond as we need to protect this nation, in cyberspace just as in the physical realm. We are building our own offensive cyber capability – a dedicated ability to counter-attack in cyberspace. We have built this capability through investing in a National Offensive Cyber Programme. The Programme is a partnership between the Ministry of Defence

and GCHQ, harnessing the skills and talents of both organisations to deliver the tools, techniques and tradecraft required for the UK to establish a world class capability.

54. And we will now commit the resources to develop and improve this capability over the next five years. The threats to our country in cyber space come from a range of places – from individual hackers, criminal gangs, terrorist groups and hostile powers. To all of them I have a clear message. We will defend ourselves. But we will also take the fight to you too. We are increasingly confident in our ability to determine from where attacks come. We are stepping up not just the means of defence, but also the means to ensure that attacks on Britain are not cost-free. To those who believe that cyber attack can be done with impunity I say this: that impunity no longer exists.
55. And at the sharpest end, we need to ensure that our military are equipped to fight the wars of the 21st Century. That means they need to be prepared for hybrid conflicts, played out in cyberspace as well as on the battlefield. A 21st Century military has to operate as effectively in cyberspace as it does on land and sea, in the air and space. Our commitment to spending 2% GDP on defence means we can invest in a military that is cyber trained, cyber secure, and cyber enabled, with the ability to fight in every domain of future conflicts. The PM will set out more details in the Security and Defence Strategic Review.
56. Of course the internet is global, and so must our approach be. We need to keep fighting to preserve a free, open, peaceful and secure cyberspace. Agreement that international law applies in cyberspace has been an essential first step. And we need international norms of behaviour in cyberspace, so that freedom is matched by responsibility. Norms like working together to prosecute those who commit illegal acts online; like not deliberately allowing their territory to be used for internationally wrongful acts; like not illegally preventing critical infrastructure from delivering essential services to the public.
57. We do all this by creating the strongest possible alliance of like-minded states that share our vision. We will do this by showing to those that have a different view of the internet that our approach can bring all of us benefits – just as we have done by encouraging Huawei to invest safely in the UK though partnership with GCHQ. We need our police forces to work together to ensure that less and less of the world is a

hiding place for cyber criminals. And we need to help our partners develop their own cyber-security – as we share a single cyberspace, we collectively become stronger when each country improves its own defences.

58. For the past five years we have been investing in the cyber security of our partners as well as our own. We have helped establish the outstanding Global Cyber Security Capacity Centre in Oxford. In the coming years we will step up these efforts, mindful that we are bound together in cyberspace. The national cyber plan that I have announced today is bold, far-reaching and transformative in numerous ways. It will provide the next generation of cyber security for our country. It will ensure that we have the skills, the structures, the tools, the companies and the partners we need. It will not be enough to stop Britain being attacked every minute of every day. It will not prevent breaches, or provide hermetic protection for the country or any part of it.

59. But it will make Britain one of the best protected countries in the world; it will give our companies and citizens the tools they need to stay safe from cyber attack; and it will create jobs and prosperity. With the ability and dedication of GCHQ's staff, our new National Cyber Centre, and the ideas and skills across our country, our plan will make sure that Britain remains a world leader in cyber, and give Britain an important edge in the global race.

60. And just as we build our resilience to cyber attack, so too we will keep building our resilience to terrorist attacks – in all their evil and murderous forms. This requires effort by all of us – government and industry, start-ups and universities, agencies and allies.

Table 46 Thematic Coding Codeable Event Table for George Osborne 2016 Speech

Code	Paragraphs	Text Samples
Threat	11, 13, 14, 16, 22, 23, 54	
Scale of the Threat	5, 13, 16, 23, 27, 28, 29, 30, 58	
Exceptional Measures	15, 16, 31, 32, 33, 34, 35, 36, 48	
Referent Object	6, 8, 13, 16	
Action Effect	32, 37, 39, 42, 43, 58, 59	
Inaction Effect	40, 48, 50	
Partnership	24, 37, 38, 48, 49, 58, 60	

Appendix G: Interview Thematic Coding Example

This appendix includes the example of the text analysis for the derivation of key themes from the practitioner interviews. The appendix includes the interview data 'blocked'[46] into paragraphs from Participant A (as an example) and the thematic codeable events from all interviews, with the exception of Participant K[47]. Participant A's 'blocked' transcript is below:

1. It is helpful to be able to speak with other organisations in the same sector but the issues transcend sectors. Attackers don't really care who it is they are attacking in whether it is out of malice, to make money, or to damage a country or an industry. Not bothered about who they are attacking as long as they are making money or getting what they want. While there are commonalities across the industry that are quite useful it is not the whole story.
2. Attacks are both opportunistic and targeted. There are a whole set of attackers who will just go for the easy target and does tend to be the ones with the lower skill level. We do see the more targeted attacks. There are attackers who have specialist skills related to an industry or a specific company. They we use that inside information that they think they have to craft a specific attack. We see it right across the spectrum there are targeted attacks and the more generic attacks.
3. Government is useful as a broker to bring together competitors as it can be a very sensitive issue speaking to a competitor especially when it can be construed as an anti-competitive activity under antitrust law so having a government bring together competitors can be very useful to allow discussions without concerns of accusations of anti-competitive behaviour.
4. Secondly, there are the introductions that can be made to bring the right people together, for example if I wanted to approach another company to discuss a specific issue I wouldn't necessarily know who to go to. I can approach advisers in

[46] Blocking refers to placing the texts into manageable sized groupings. The thematic analysis process is more fully described in the Methodology chapter.

[47] Participant K was interviewed on multiple occasions and the resulting notes are very different to any other interviews in terms of the subjects discussed. While participant K was a valuable inclusion in the research project in terms of validation and verification of information, they did not add any significant new information to the data collected.

government to find out who the right people are to speak to, for example, who has the same type of industrial control systems that we use who I could ask a question of. Also, in the past they have commissioned reports from consultants for example in records on how to protect industrial control systems that were given to all companies operating critical infrastructure in the UK. Commissioning these reports on our own would be very expensive for us.

5. Critical infrastructures groups and invited vendors to be able to understand their patching strategies and future development plans with all their potential customers in the room. Vendors can also work through this forum if they have any ideas they would like to test with their customers for a security improvement possibility. As a customer you can also hear all the other customers' responses to the ideas so we can quickly get an idea of whether particular ideas will fly.
6. We normally work with security specialist within ICS vendors rather than generic security providers. ICS systems have a very long life and changes are incremental and slow. Patching is a much slower cycle.
7. The development cycle for control systems is much slower than the development of new threats. It is a soft underbelly for attacks, so much stronger controls are put in place such as air gaps, controlled remote access, firewalls and the like. We have developed strategies to enable systems to catch up with the threat as we cannot just replace them as they are so integral to the process.
8. There is a common enemy here which is much easier to discuss without commercial issues. Security staff are generally not dealing with commercial issues – they are keeping systems safe which is a common concern for everyone.
9. There are commercial drivers for collaboration in terms of shared business interests and although we would not discuss commercial or contractual issues concerning common systems we would discuss techniques for protection, security infrastructure, incidents and threats.
10. Private industry owns much of the infrastructure and so it has to be a partnership – there is no other option short of renationalisation. Government would rather see private industry deal with it, although they have a strong interest in ensuring that happens and keeping an eye on it and being aware of an area of infrastructure that is

falling behind. Regularly have discussions with government who want to hear what is being done. Other mechanisms as well in terms of security assessment processes where a team will be sent in to a plant and carry out an assessment, collaboratively with you, to get reassurance that things are in hand. We are happy to cooperate with that but as government has little of the critical infrastructure it has to be a collaborative effort.

11. Conversations are normally constructive, and companies will generally try to satisfy government requirements. If any assessment is felt to be unreasonable or lead to unnecessary demand, then the relationship is mature enough to be able discuss that and develop a mutually acceptable plan. We can have a trusted conversation and know that any insights we give to them will not result in unwanted publicity or unreasonable use of the information. There is a sensible and mature approach and everyone involved sees the benefits of keeping the conversation at the right level.
12. Government are most likely to be able to identify a specific attack and attacker. We will see the symptoms and indicators of compromise, but we may not know what it is, whereas government may have seen the same symptoms on other systems and know that it indicates a specific attacker and be able to propose mitigation strategies. There would be an exchange of information on future incidents. We place attack information on CiSP and government can provide responses to that.
13. The amount of change and reorganisation in government and movement of people that makes it difficult. When you finally build a relationship with someone they are moved to another function. Unfortunately it is part and parcel of dealing with government.
14. Where they can really mess things up is when they have the potential to publish information without permission. You have to be sure you can trust the people you are dealing with and that they understand the issues involved. Have not personally had any issues but aware of others and have to be careful. One breach of trust and all this collapses.
15. Not always. The most difficult agency to deal with is law enforcement. They see things so differently to everyone else. Their interests are different to everyone else working in this area. Their sole focus is arrest and conviction. If there is any

collateral damage then just too bad. Their attention span is also very short. They are very busy, focused on particular targets and conversations that you have are largely forgotten the next week as a result of that focus. Trying to report anything is a fraught process – you want to help and report incidents but they make it very difficult. Portals like Action Fraud are aimed at the general public and don't make it easy to report incidents at a corporate level. The information they ask for is inappropriate and you lose complete control. There is no agreement with a law enforcement officer about things not going any further – as soon as you say something it can be used for anything and it can be attributable – your name will be attached to it. We have had attempts over the years to bring law enforcement into the conversation and that works for a few months until that officer gets moved on to another job or inquiry and then it's back to square one.

16. By its very nature they will not discuss anything with you.
17. Hacking back is not an option. We don't have the time or the expertise to do that. As soon as we stop an attack we lose interest in it apart from what lessons can be learned. We're not interested in who the attackers are really. If we know who they are and there is information that may help attribution then we will report it via CiSP and they will do what they will with it – but that's as far as it goes. We don't have the staff or the interest in going after anybody. That's not our role.
18. At the point it has distracted a lot of people. They are more inward looking for the time being while they find out their new role and what their job is. There is a bit of confusion. They do know how to engage with the private sector. We have been dealing with a group of people who even with different roles have often been the same people.
19. In theory it should be, but the jury is out as it is early days.
20. One irritation with the ISPs is how difficult they make it to get fraudulent domains shut down. We could do better there between private industry and the CSP/ISPs. We do not have a very good relationship where they would be able to take trusted information from us. If I need domains taken down quickly that could be anything between 48 hours and never and there is no reason it needs to take weeks to remove an obviously fraudulently domain. Would like to see a better control and process on

setting up domains, but it is too easy to set up a fraudulent domain. It seems as if people can set up the most ridiculous fraudulent domains.

21. We are aware of it and it is a noticeable issues that is getting attention, but in an industry with no end user customers and not dealing with the general public, the extent of responsibility is mainly employees and ex-employees so compared to many others it is a relatively minor issue.
22. The attacks that have happened to other people such as Saudi Aramco attack targeted on one company that has affected almost their entire IT stock in one go. That could cripple us. We are aware of weaknesses such as a lack of diversity in client operating systems and an attack with a zero day that moves horizontally between PCs is the doomsday scenario. We know of ways that this could happen – people have to do their jobs and we have to walk a line between enough control to stop the bad guys but enough leeway to do their jobs.
23. Desk access to social media and webmail is an example of where it would make sense to block it but it may be a step too far. Segmented wireless networks with a 'dirty network' where people can access almost anything, but segments with much more control.
24. Risk of proliferation of personal devices with dubious security controls. Worst case scenario of an attack that sits quietly while it spreads and then hits everything.
25. Don't do anything to destroy the trust that has been built up. Improve the relationship with law enforcement and publish to industry the type of information that would be helpful to them. Give us a hint as to what you're interested in and then provide a mechanism for that to be provided. We cannot pass information on every attack and get no feedback. We have limited resources and will help when we can with intelligence and have to trust that the information will not be misused or used in a reckless way that breaks trust. An equal collaboration is essential.

The remainder of this Appendix shows the results of coding all the blocked interview data against the themes that were identified of:

- The complexity of the cyber security environment.
- The failure of the market to address cyber security and the potential need for regulation as a result

- The limitations on the role and capabilities of the private sector
- The need for collaboration and the difficulties inherent in collaborative approaches
- The difficulties in working with government and state agencies
- The changing and adaptive nature of the cyber security environment
- The need for better education and understanding

Appendix H: Interview Themes Codeable Events

Table 47 Participant A Codeable Events

Label	Paragraphs	Text
Complexity	2, 7	"attacks are opportunistic and targeted"
		"attackers with specialist skills"
		"Strategies to enable systems to catch up with the threat as we cannot just replace them"
Regulation	20	"would like to see better control and process on setting up domains"
Limitations	17, 25	"we don't have the time of the expertise to do that [hack back]"
		"we have limited resources"
Collaboration	1, 6,9, 20. 25	"it is helpful to be able to speak with other organisations in the same sector"
		"work with security specialists within ICS vendors"
		"commercial drivers for collaboration in terms of shared business interests"
		"we could do better between industry and CSPs/ISPs"
		"an equal collaboration is essential"
Difficulty	10, 13, 14, 15	"government would rather see private industry deal with it"
		"the amount of change and reorganisation in government and movement of people makes it difficult"
		"where they really mess things up is when they have the potential to publish information without permission"
		"The most difficult agency to deal with is law enforcement. They see everything differently to everyone else"
Change	7	"development cycle for control systems much slower than the development of new threats"
Understanding	25	"give us a hint of what you're interested in"

Table 48 Participant B Codeable Events

Label	Paragraphs	Text
Complexity	2, 9, 11	"organisational and industry differences determine where the boundary for cyber-security is"
		"different security focus depending on the system"
		"there is no one size fits all approach to cyber security"
		"real problem is understanding the business model of adversaries"
Regulation	1, 14	"less successful organisations will be prompted by regulatory intervention"
		"it [more regulation] could help but it could also cause more problems than it solves"
Limitations	4	"it makes no difference unless there is funding available"
Collaboration	4, 14	"lot of agencies that provide best practice information"
		"the key will be collaboration between industry and the regulators"
		"there is a need for industry to work hand in hand with regulators so they understand the issues"
Difficulty	5, 6, 15	"there is still a long journey to go for organisations to trust government"
		"scepticism about what government can offer"
		"intelligence sharing seen as something that can draw on rather than share with government"
		"regulators are not the best qualified people in the room"
		"concern that the agencies are not being given the space and time to develop the relationships"
		"NCA announcements in the press leading to senior management fallout"

Participant B Codeable Events (continued)

Change	3, 10	"inter-organisation communications and expansion of technical capability has pushed out the boundary"
		"threat is always changing and very adaptive"
		"[understanding adversaries] should steer the investments and change programme"
Understanding	4, 12, 13, 18	"need recognition from the top that this is a business issue"
		"vendors do not understand the nuance [of cyber-security risk]"
		"the business model is what matters and none of the vendors understand this sufficiently"
		"work on the boards of organisations to help them understand the risks"
		"threat intelligence needs to understand how bad guys would use the information specific to your organisation"
		"it is down to organisations to understand their own business model"

Table 49 Participant C Codeable Events

Label	Paragraphs	Text
Complexity	1, 7	"there isn't a consistent 'private sector' and it depends on philosophy as to where public sector and private sector begin"
		"possible false flag and attribution issues"
Regulation	9	"Regulation would be nice, but it is almost impossible"
		"drifts into prescription"
Limitations	8	"An organisation that struggles to do things like patching infrastructure or securing networks will not have the budget or capability to be able to hack back effectively"
Collaboration	1, 4	"If it is a critical industry then it needs to be a community led activity"
		"partner with organisations to bring complementary solutions or scale"
		"One area where we do see partnership with government is in threat investigation"
Difficulty	12, 10	"vulnerability that he NSA discovered but did not tell anyone" "once it is in a legislative framework it gets difficult to change [good practice]"
Change	5, 10	"new threats are starting to materialise"
		"good practice can change"
Understanding	10, 11	"we do not understand today what we will need to do tomorrow"
		" we just don't know what the flaws look like or have a way of being sure we find those flaws"

Table 50 Participant D Codeable Events

Label	Paragraphs	Text
Complexity	2, 3	"no one size fits all process"
		"Amount of data and ever changing data gives problems with organisational processes"
		"velocity, veracity, volume and value of data"
		"Too much information for one organisation or one platform to process"
Regulation		
Limitations	5	"not bothered with future activity after a breach"
		"commercial cyber-security industry has a snake-oil element in it"
Collaboration	1	"Different levels of collaboration at commercial, national, and international levels."
Difficulty	2	"law enforcement not getting threat sharing right yet"
		"world would not have had wannacry if US government has not spent large amounts of money finding vulnerabilities and not reporting them"
Change	2, 3, 16	"sharing concepts are not working any more"
		"ever changing data gives problems with organisational processes"
		"islands of security are emerging"
		"buy the time regulation is in place, everything has changed"
Understanding	17	"priority is education"

Table 51 Participant E Codeable Events

Label	Paragraphs	Text
Complexity	2, 5	"don't want to scare people with the technology"
		"need to reduce complexity for analysts"
		"need to do simple things well the get more complex and advanced"
Regulation	2, 8	"the bigger players in cyber have a responsibility to drive the market"
		"government needs to set the bat and get everyone up to a similar standard"
		"if [the market] does not want to pay for certain elements of service then they won't be provided"
Limitations	3	"cannot compete with the technology the state can deploy"
Collaboration	1	"people in the doing space need to have the community"
		"in some aspects of cyber community and sharing information is everything"
		"wannacry was a good example of peers sharing"
Difficulty	10,11, 13	"statements on SS7 and BGP were cage rattling"
		"lead organisation such as the IoT forum should work to ensure IoT is secure – government should support these things"
		"Their skills are different and they have to deal with so many different types of crime and evidence that it will always be difficult"
Change	3, 11	"need a psychology of being fast moving and prepared to fail"
		"threat picture does change"
		"commercial organisations can drive security change because they recognise the commercial risk"
Understanding	1, 17	"getting that maturity [of understanding] is a challenge"
		"need to create an intelligent digital consumer who knows where their data goes"

Table 52 Participant F Codeable Events

Label	Paragraphs	Text
Complexity	22, 27	What we see as criminal gangs may well be state agencies"
		"difficult to distinguish public and private in terms of infrastructure responsibility"
Regulation		
Limitations	29	"difficult for the private sector to defend against state level capabilities"
Collaboration		
Difficulty	3, 5,6,7,8,9, 17	"government potentially falling back on looking after public sector rather than looking at the private sector"
		"government not getting to grips with cyber"
		"too many different departments, DCMS, Cabinet Office etc"
		"too many changes of personnel in government for a consistent approach"
		"government lacking skills and suitable background"
		"outdates government systems and data architectures"
		"there is no long term government plan"
Change	16	"attacks are becoming more targeted and less opportunistic"
Understanding	32	"many organisations are not aware of the scale of the problem that they face"

Table 53 Participant G Codeable Events

Label	Paragraphs	Text
Complexity	5, 6	"responsibility between private sector and the state is not clear"
		"there is no one model. Different threat actors have different motivations"
		"an organisation may not know enough about the attack to be able to act"
Regulation		
Limitations	14	"have to stop before hacking back"
Collaboration	3, 4	"NCSC has been able to engage with the community"
		"big change in tone to have a two way conversation"
Difficulty	5, 9, 10	"all a bit of a muddle about who takes responsibility for all the bits of cyber security"
		"private sector feels the state could be doing more to support them"
		"it is a challenge for law enforcement due to resource and people shortage"
		"only option is Action Fraud and then not a lot happens"
		"there is a lack of joined up thinking"
Change	1	"cyber security focus is changing away from a purely technical focus"
		"attacks now at such a large scale"
Understanding	13	"needs more of government to develop an understanding"
		"ridiculous statements about encryption and WhatsApp"

Table 54 Participant H Codeable Events

Label	Paragraphs	Text
Complexity	10	"there are no rules on where public ends and private begins"
Regulation	11,12,13	"Difficult decision on where you put regulatory intervention"
		"How do you stop people buying a cheap device and putting it on the internet?"
		"global regulation is required"
		"One answer is to let the market decide, but costs are externalised"
		"Relying on GDPR to make companies take security more seriously"
		"cyber issues are not reflected in the spend of large companies"
Limitations	4	"there is a massive skills shortage with inflated wages"
Collaboration	5, 8	"NCSC is a good example of outreach"
		"good initiatives out of their industry engagement team"
		"Wannacry example – instant sharing of information"
Difficulty	3, 10	"private sector is being asked for secondees a lot, but no clear benefit"
		"initial reluctance to engage with NCSC. Worry that it would just be GCHQ gobbling up intelligence and data from the private sector"
		"government procurement can be a long and difficult process"
Change	13	"Lots of companies are quite complacent. How can government change that thinking?"
Understanding	11	"relying on consumer to be aware of the security risks"
		"some devices have strong security settings but consumers don't switch them on"

Table 55 Participant I Codeable Events

Label	Paragraphs	Text
Complexity	8, 16	"increase in speed and automation of methods to monetise exploited systems"
		"hacktivists have different methodologies and motivations"
Regulation	12, 13, 28	"there is a role for the state to regulate – this will be the case with IoT"
		"devices with computers embedded will only last as long as the manufacturer keeps them up to date and that can be enforced by government"
		"state needs to start to act as a mechanism to make data available to underlying CSPs so there are more automatic opt-ins that ISPs could operate"
		"small companies looking for the government to lay down what is safe or not safe in the UK"
Limitations	3, 22, 31	"information may not be shared if it has commercial value"
		"lots of people have valuable information but it is not being shared"
		"Nation state attack can be stopped but banks [for example] may not have the capability to stop them"
		"hacking back has the potential to get out of hand"
		"market is horrendous – profit driven vulture like activity"
Collaboration	1	"only useful collaborative networks are those that have a high level of trust"
		"most consumer security is provided by corporations e.g. windows update, and the Apple app store"
		"government needs to work through the CSPs to provide security"
Difficulty	2	"difficulty of sharing information does not match the benefit"

Participant I Codeable Events (continued)

Label	Paragraphs	Text
Change	6, 7	"threats are constantly changing"
		"underlying attack methodologies change much more slowly"
		"ransomware changing from an untargeted to targeted attack"
		"introducing automation into ransomware means it is virtually no effort"
Understanding	11, 13	"people should worry about privacy rather than security"
		"people do not understand what they are buying so market forces will not come into effect"
		"companies do not appreciate that this is not going to go away"

Table 56 Participant J Codeable Events

Label	Paragraphs	Text
Complexity	10, 22	"more technology increases the threat landscape"
Regulation	18, 19	"Do you want to hand control to the government to be more secure?"
		""the consumer doesn't care if their IoT device has a security tested watermark"
Limitations	3, 10, 22	"no company can defend against a government sponsored state attack"
		"industry does not understand the technology it is trying to sell"
		"would hopefully see a market response and [IoT] products that are security tested"
		"if you do not have the technical capability to defend your company then you do not have the capability to attack another"
Collaboration	1, 4, 24	"all security is shared – can't ask one group to be responsible"
		"massive companies that hold a lot of data are a part of the CNI which means they work with the government"
		"sharing platforms are a really good idea – very good in the finance sector"

Participant J Codeable Events (continued)

Label	Paragraphs	Text
Difficulty	15, 17, 23	"it would not surprise me if there was not at least one government agent in most hacking groups"
		"seen a lot of infiltration by law enforcement and government"
		"governments are struggling with basis things – don't have the money, resources, or expertise"
		"they sometimes annoy the industry as a whole"
		"they take good ideas from companies that have been doing it for some time and pass them off as their own"
Change	19, 20, 27	"until the consumer is forced to take responsibility for the home network then they are never going to care"
		"possible there will be a generational change due to greater experience with equipment"
		"base line of competence is required – industry needs to develop certifications"
		"we need to create a new internet"
Understanding	4, 8, 9, 10, 13, 16, 29	"biggest risk is not doing the basics and people still don't understand that"
		"A cost of being a big company is that you have to understand that [you are a part of the CNI]"
		"reactive nature [to a breach] is just a lack of understanding"
		"industry does not understand the technology it is trying to sell"
		"educating the C-suite is what is necessary"
		"there will always be businesses that don't understand that [business risk]"
		"they do not understand that they need to know about security"
		"most organisations don't understand [how to respond to a breach]"
		"home user needs to be aware of the issues attached to these devices"
		"start a consumer education programme - needs a long term approach – educating young people"

Table 57 Participant L Codeable Events

Label	Paragraphs	Text
Complexity	14	"it does not take too much to create a lot of havoc"
Regulation	4	"State needs to provide a strong regulatory framework"
		"[corporates] now have access to such large amounts of personal data that they cannot be treated as if they are in a vacuum"
		"the legal requirement to inform the state of breaches and ensure minimum security standards is a stage in the ground to tell the private sector they need to make changes"
		"concerted action needed on IoT"
Limitations	9, 11	"[Hacking back] is a stupid idea for governments. No words to describe hoe bas it is if corporations do it. Private sector will create more chaos"
		"if the NSA can't keep them [exploits] under control then unlikely anyone else will"
Collaboration	1,	"Definitely collaborative. Inter-sectoral, state, private sector, and civil society"
		"skills shortage driving development of public and private partnerships"
		"threat information sharing, specific schemes to exchange staff between public and private sector"
Difficulty	9, 10	"the state environment is potentially damaging cyber-security"
		"oversight if very important"
		"there are law enforcement actions that can create insecurity in other areas."

Participant L Codeable Events (continued)

Label	Paragraphs	Text
Change	15	"law enforcement have to adapt to a role in the cyber domain which is significantly different to the realspace domain"
Understanding	9, 12, 16	"need elected officials to understand the implications of the intelligence agencies hanging on to zero days"
		"lack of understanding about what hack back really means"
		"important job to educate policy makers about cyber and educate cyber people about the policy world"
		"not enough people who can link [the technical world and the policy world] which leaves policy makers with intelligence agencies and lobbyists which is distorting the debate"
		"not enough technical skills available"

Table 58 Participant M Codeable Events

Label	Paragraphs	Text
Complexity	1	"difficult to protect from every angle"
		"massive data pool of threat information"
		"sleeper threats are almost undetectable. We believe mediated data and believe instruments and tools above our own senses"
Regulation	4, 6	"normalisation of behaviour ….government has a role to play in this [determining acceptability]"
		"problems with companies driving understanding with marketing dollars to drive sales"
		"data standards are essential"
		"compliance and audit"
		"threat of regulation will induce self-regulation in some areas"
Limitations	4	"technology industry not always helpful"
Collaboration	1, 2	"depends on level of trust"
		"community itself can be self-policing"
Difficulty		
Change	1, 10	"traditional methods of protection don't apply and something different is needed"
		"expectation that anonymity will disappear over time"
Understanding	1	"learn the norms and patterns"
		"understanding the system and traffic"

Appendix I: Interview Wicked Problem Codeable Events

Table 59 Participant A Wicked Problem Codeable Events

Label	Paragraphs	Text
No definitive formulation	1, 2, 12	"attackers don't really care who it is they are attacking or whether it is out of malice, to make money, or to damage a country or industry"
		"attacks are both opportunistic and targeted"
		"we will see the symptoms and indicators of compromise, but we may not know what it is"
Stopping Rule	6	"changes are incremental and slow"
No True or False	7, 10	"we have developed strategies to enable systems to catch up with the threats"
		"other mechanisms as well in terms of security assessment processes"
		"if an assessment is felt to be unreasonable or lead to unnecessary demand"
No solution test	5, 15	"ideas they would like to test with their customers for a security improvement possibility"
		"If there is any collateral damage then just too bad"
One shot operation	14	"one breach of trust and all this collapses"
Potential	5	"ideas they would like to test with their customers for a security improvement possibility"
Solutions		"stronger controls are put in place such as air gaps, controlled remote access, firewalls, and the like"
Unique	6	"ICS systems have a very long life and changes are incremental and slow"
Symptom	22	"…we are aware of weaknesses such as a lack of diversity in client operating systems"

Table 59 Participant A Wicked Problem Codeable Events (continued)

Label	Paragraphs	Text
Explanation	1, 6, 17, 20, 22	"…malice, to make money, or to damage a country or an industry. Not bothered about who they are attacking as long as they are making money or getting what they want."
		"patching is a much slower cycle"
		"we don't have the time or expertise"
		"difficult to get fraudulent domains shut down….too easy to set up a fraudulent domain"
		"lack of diversity in client operating system"
No right to be wrong	14	"you have to be sure you can trust the people you are dealing with"
		"one breach of trust and all this collapses"
		"desk access to social media and webmail is one example of where it would make sense to block it, but that may be a step too far"
		"we have to walk a line between enough controls to stop the bad guys and enough leeway [for staff] to do their jobs"
Social Complexity	1, 4, 5	"it can be a very sensitive issue speaking to a competitor especially when it can be construed as an anti-competitive activity"
		"there are introductions that can be made to bring the right people together"
		"critical infrastructure groups and invited vendors to be able to understand their patching strategies and future development plans"

Table 60 Participant B Wicked Problem Codeable Events

Label	Paragraphs	Text
No definitive formulation	4, 8, 10, 11	"need to remain aware of the risks involved with extending the boundary"
		"[key threats] depends very much on the industry"
		"…systems such as NATS would be focused on availability. For other organisations focus will be on the security of customer data"
		"threat is always changing and very adaptive"
		"there is not a one size fits all approach to cyber-security"
Stopping Rule	3, 11	"has pushed the security boundary out to a point where the boundary is almost irrelevant"
		"worry about how the threat is going to change and who is next to come at the organisation"
		"IoT is just another example of an old problem of badly configured devices"
No True or False	4	"agencies that provide best practice information but it make no difference unless there is funding available from the top"
		"Most will say that "CiSP is a good thing……something they will draw on rather than share with the government"
No solution test	18	"look at what's there and already works"
One shot operation	14, 17	"yes it [regulation] could help, but it could cause more problems than it solves"
		"Once they have figured out what you are doing then they by-pass it"
		"good hackers recognise when they are in a sand pit and how to defeat it"
Potential	12	"have to look at risk in context….understanding risk for each element of the business"
Solutions		"down to organisations to understand their own business model and understand use cases where things apply"
		"it's an arms' race"

Table 60 Participant B Wicked Problem Codeable Events (continued)

Label	Paragraphs	Text
Unique	11	"even within organisations the concerns are different"
		"if the cyber-security capability is configured for the wrong type of attack then that is a problem"
Symptom	15	"ill-informed press cause problems in dealing with senior management fall-out"
Explanation	4	"needs recognition from the top that this is a business issue and not just a technical plumbing issue"
No right to be wrong	12	"The business model is what matters and none of the vendors understand this sufficiently"
Social Complexity	1	"what is best for the organisation and its customers and other stakeholders"
		"organisational and industry differences determine where the boundary for cyber-security is"
		"where the boundary is, depends on to what extent the other stakeholders play a part in the security system"

Table 61 Participant C Wicked Problem Codeable Events

Label	Paragraphs	Text
No definitive formulation	5	"ransomware as a major future problem"
		"we don't know whether a piece of software has a flaw in it"
		"new threats are starting to materialise"
Stopping Rule	5, 10, 11	"kill-switch and sand-box evasion techniques pre-used"
		"we do not understand today what we will need to do tomorrow"
		"it isn't like a car safety program where you can drive dummy cars into a wall"
No True or False	3	"security is not as good in cheaper products"
No solution test	10	"good practice can change"
One shot operation	8, 9	"potential for side effects is huge"
		"regulation drifts into prescription"
		"…people do things whether they are appropriate or not and people drive down cost by doing as little as possible.
Potential	5	"Possible false flag and false attribution situation"
Solutions		"Microsoft produced the vulnerability which the NSA discovered and did not choose to tell anyone"
Unique	1	"if it is a critical industry then it needs to be a community led activity but otherwise it is up to the organisation"
Symptom		
Explanation	3	"if you choose the cheapest thing you have to accept there are compromises"
		"it is about ethical purchasing rather than an ethical requirement on a supplier"
No right to be wrong	12	"understand the real risks and what the problems are we need to fix"

Table 61 Participant C Wicked Problem Codeable Events (continued)

Label	Paragraphs	Text
Social Complexity	1, 4, 7	"if it is a critical industry then it is a community activity"
		"there isn't a consistent private sector and it depends on philosophy as to where the public sector and private sector begin and end"
		"partner with organisations like BT, partner around the world with different specialisations bringing complementary solutions"
		"different agencies and states have different objectives and end-games"
		"difficult to take action due to a myriad of different agreements and different laws"

Table 62 Participant D Wicked Problem Codeable Events

Label	Paragraphs	Text
No definitive formulation	3, 10, 14	"no one size fits all process"
		"worry at the moment is the hybrid nature of what is happening in Eastern Europe and Ukraine – high grade organised crime"
		"negligence will allow criminal activity to be perpetrated from your machine in a bot net"
		"lack of anti-virus and unpatched system or illegal copies of windows"
Stopping Rule	2, 3	"an increasing challenge"
		"by the time you have written it down on a sharing platform it has probably changed at a tactical and operational level"
		"by the time regulation is in place, everything has changed"
No True or False		
No solution test	11	"as soon as the Shadow Broker was made public that authors of wannacry modified it to use a different exploit"
One shot operation	10	"huge threat of blowback with state research being used"
Potential Solutions Unique	16	"difference between active defence and hacking back (macho crap) – but a trace back and forensics is fine."
Symptom	9	"world would not have had wannacry if US had not spent large amounts of money in finding vulnerabilities and not reporting them"
Explanation	14	"lack of anti-virus and unpatched system or illegal copies of windows"
No right to be wrong	7	"People need to focus on doing some of the simple things – patching and getting a decent firewall."
Social Complexity	1	"different levels of collaboration at practitioner, commercial, national and international levels"

Table 63 Participant E Wicked Problem Codeable Events

Label	Paragraphs	Text
No definitive formulation	3, 19	"Threat picture does change"
		"Script kiddies are getting more sophisticated as the tools that can be taken off the internet are more sophisticated."
		"cyber is a human problem more than a technical problem"
Stopping Rule	5, 6, 10, 13	"if [a telecommunications] operator has mitigated risk then why should they change"
		"there is more that can be done but the issue is how"
		"key point about cyber is it is about the journey and not the destination"
No True or False	6	"moving forward and being better is the best way to defend"
No solution test	6	"[cyber criminals] diversified into state sponsorship"
One shot operation	7	"the psychology of a fast moving and prepared to fail attitude"
Potential Solutions	4, 6, 7,11	"know where your critical data, systems and technology is. Know your own systems and do simple things well."
		"change to making security enable your business"
		"flexibility and innovation is also emerging"
		"bringing good tools to the marketplace that would not have been thought of"
		"if it is malicious traffic that impacts service then they should stop it and that is a core part of the service"
Unique	3	"cannot compete with the technology that the state will deploy"
Symptom	3	"script kiddies getting more sophisticated as tools off the internet become more sophisticated"
Explanation	4, 9	"[criminals] have a high level of anonymity that allows them to be fast moving"
		"SS7 is an inherently insecure protocol and needs changing. But it needs to be paid for"
No right to be wrong		

Table 63 Participant E Wicked Problem Codeable Events (continued)

Label	Paragraphs	Text
Social Complexity	1, 2	"in some aspects of cyber, community is everything" "bigger players in cyber have a responsibility to drive the market"

Table 64 Participant F Wicked Problem Codeable Events

Label	Paragraphs	Text
No definitive formulation	10, 16, 17, 22, 33	"outdated government systems and data architecture"
		"the Public Sector is a mess in some areas"
		"attacks becoming more targeted and less opportunistic"
		"there is no long-term government plan"
		"what we see as criminal gangs may be state agencies"
		"data leakage via social media is becoming a major issue"
Stopping Rule	15, 18, 22, 32	"Partnership seems to involve providing people and skills for free. Not clear what the upside is"
		"reactive rather than proactive"
		"seeing the same attacks coming back at some point"
		"many organisations are not aware of the scale of the problem they face"
No True or False	12	"Not sure whether being part of GCHQ is a help or hinderance to the NCSC"
No solution test	4	"there is less work being done with CNI than before the NCSC"
One shot operation	21	"private sector push back from first NCSC initiative may have changed approach"
Potential Solutions	31	"cyber is now a part of all conversations with customers"
Unique	28, 29,30	"there are malicious actors who just want to destroy things"
		"difficult for private sector to defend against state level capabilities"
		"legacy systems are particularly difficult to identify all vulnerabilities"
Symptom	23	"concern over proliferation, blowback and control"
Explanation	26	"difficult to distinguish war and crime"

Table 64 Participant F Wicked Problem Codeable Events (continued)

Label	Paragraphs	Text
No right to be wrong	1, 2, 5, 16	"NCSC is struggling for a role"
		"There is not enough money to set up a proper agency"
		"Government is not getting to grips with cyber"
		"there is no long term government plan"
Social Complexity	7, 12, 27	"Too many different departments, DCMS, Cabinet Office"
		"Not sure whether being part of GCHQ is a help or hinderance to the NCSC"
		"difficult to distinguish public and private – infrastructure and responsibility"

Table 65 Participant G Wicked Problem Codeable Events

Label	Paragraphs	Text
No definitive formulation	1, 2, 5, 6	"Private sector focus has been that cyber security is a technical issue and the solutions must be technical. Changing in the last few years – security being more people centric"
		"people talk about AI when what they mean is machine learning or not even that"
		"all a bit of a muddle as to who takes responsibility for all the bits of cyber security"
		"there is no one model. Different threat actors have different motivations and different" methodologies and different resource and targets therefore differ"
Stopping Rule		
No True or False	4	"need to engage the wider conversation and for it to be a two-way conversation rather than just saying what people should do"
No solution test	7	"Reliability of the conclusion of the analysis is also debatable"
One shot operation	14	"If you hack back on incomplete evidence and are wrong then there can be a far more damaging chain of events initiated"
		"[Hacking back] is a fundamentally flawed idea that could cause of lot of collateral damage"
Potential	9, 6	"…talking about hacking back. But also look at defences – mitigate risk – look ahead"
Solutions		"how to disrupt, delay and confuse any attackers"
		"what targets can do to defend themselves is also varied"
Unique	6	"…organisation may not know enough about the attack for it to be possible to act on that kind of varied model"

Table 65 Participant G Wicked Problem Codeable Events (continued)

Label	Paragraphs	Text
Symptom	5, 13	"nobody providing guidance, and nobody knows who should"
		"ridiculous statements [about encryption] shows a lack of understanding. Row over encryption causes a disconnect"
		"How can government want to make the UK the safest place to do business and talk about banning encryption at the same time?"
Explanation	7, 12	"Attacks that look as if they are criminal attacks may be a state"
		"A lot of being successful in cyber security comes down to having the right mindset"
No right to be wrong	15	"Potentially attacking innocent bystanders"
Social Complexity	3, 13	"[NCSC] has been a really positive influence. They have reached out to the community"
		"events engaging academia and industry"
		"Depends on which part of the government and which part of the cyber security industry. Some are more privacy focused than others."

Table 66 Participant H Wicked Problem Codeable Events

Label	Paragraphs	Text
No definitive formulation	7, 10	"not every incident is the same"
		"no rules on where public ends and private begins"
Stopping Rule	11, 12	"…and then how do you stop people buying cheap devices on the Internet"
		"global regulation required – but how do you enforce that"
No True or False	12	"In an ideal world that is how it would work, but costs are externalised"
No solution test	11	"Relying on consumer being aware of the security risk"
One shot operation	11	"Some devices have strong security settings, but customers do not switch them on. Tomorrow's threats will come from the connected devices."
Potential Solutions	11	"Difficult decision as to where to put the regulatory intervention"
		"could require cyber security in annual audit, but relying on GDPR as a driver for making companies take cyber more seriously"
Unique	5	"sectors working with NCSC – retail cyber toolkit"
Symptom	4	"Massive skills problem, inflated wages…government see best people being poached"
Explanation	13	"Lot of companies are quite complacent"
No right to be wrong	13	"How can government change that thinking?"
Social Complexity	1, 2, 6	"Cyber Growth Partnership modelled on other industry government partnerships…been through several iterations"
		"Revolving door between industry and government which shared skills and insights"
		"some companies have had difficulties working with GCHQ as an organisation"

Table 67 Participant I Wicked Problem Codeable Events

Label	Paragraphs	Text
No definitive formulation	4, 6, 7	"Intelligence led defence will not deal with untargeted attacks"
		"Intelligence led models work well against campaign level attacks"
		"Top of the pool is constantly churning or moving around and threats are constantly changing"
		"Ransomware removed the time element from an attack"
		"When a new methodology comes along it may bypass more levels of controls or multiple layers simultaneously."
Stopping Rule	8	"speed and automation...ransomware automatically sending bitcoin…then there is no effort"
No True or False	8	"Still routes to sell data and different ways to monetise an exploited system [after closing dark markets]"
No solution test		
One shot operation	22	"[hacking back] has the potential to get out of hand but could also be very useful"
Potential		
Solutions		
Unique		
Symptom	4	"Lot of people have valuable information, but as it is valuable it is not being shared"
Explanation		
No right to be wrong		
Social Complexity	1	"Useful [networks] are those that have a high level of trust – typically quite closed networks where you know everyone in the room."
		"Some do not want to share as it can give away that they are not as good as they should be."

Table 68 Participant J Wicked Problem Codeable Events

Label	Paragraphs	Text
No definitive formulation	3, 16, 19	"The bigger you are the easier it is for outside agents to infiltrate the company"
		"A management issue and not just a security issue."
		"won't make any difference as the consumer doesn't care if their IoT device has a security tested watermark. Until the consumer is forced to take responsibility for the home network then they are never going to care"
Stopping Rule	1, 10	"Need to layer security"
		"It's an arms race between defence and attack and it always will be"
		"…everything is getting worse and at some point, it will be so insecure that it becomes secure. So tainted that nobody wants to use it and people won't connect to the internet."
No True or False	8, 10	"If you've done the basis like network segmentation then you massively reduce the risk of high-level impact"
		"It is an unwinnable war but we do our best to stop most of them"
		If you can cope with 90% …… then doing better than most people.
No solution test	9	"learning from a first attack can prevent a greater impact from a subsequent and different vulnerability"
One shot operation	7	"it has not prevented any further breaches because everyone is worried about the latest thing"
		"More technology increases the threat landscape"
Potential Solutions	8, 17, 27	"No good trying to defend against the latest NSA zero-days - patching should have been done before hand"
		"but the same idea in China is forced on people rather than being given as a tool to use."
		"…the Internet as we know it will never be secure so what we need to do is create another Internet from the ground up with built in security"
Unique	3	"No company can defend against a government sponsored state attacker"

Table 68 Participant J Wicked Problem Codeable Events (continued)

Label	Paragraphs	Text
Symptom	8, 9	"Biggest risk is not doing the basics and people still don't understand that"
		"you are likely to be breached so you need to know what the response to the breach will be"
Explanation	3, 9	"The bigger you are the easier it is for outside agents to infiltrate the company"
		"Reactive nature is just a lack of understanding"
		"issues related to the basic architecture of the system"
No right to be wrong	12	"If you think technology can solve the problem then you don't understand technology and you don't understand the problem."
		"If you think one box or software produce from a vendor will fix the underlying issues with a network is wrong – you are probably just installing another vulnerable device."
		"Almost certainly a lack of knowledge. A lot of people are not security minded. Do not understand that they need to know about security."
Social Complexity	1	"All security like this is shared. You cannot have government, business, or individuals solely responsible"

Table 69 Participant L Wicked Problem Codeable Events

Label	Paragraphs	Text
No definitive formulation	3	"Private sector is based more on a risk assessment. State more concerns with intangible items such as political costs of attack on state institution."
Stopping Rule		
No True or False	3	"Balance between public security and cyber security – balance now for public security at cost of Info Sec with state hacking, surveillance capabilities etc."
No solution test	11, 16	"[hacking back] will create more chaos"
		"law enforcement actions that can create insecurity in other areas"
One shot operation	9, 12	"State environment potentially damaging cyber-security – needs elected officials to understand the implications of the intelligence agencies hanging on to zero days"
		"DDOS C2 computers are probably not the perpetrator's computers so hack them and you are really hacking someone else"
Potential		
Solutions		
Unique		
Symptom	16	"Hacking back is a good example. Policy makers don't know what issues it can create – techies looking at it are keen on it but don't know what problems they can cause."
Explanation		
No right to be wrong		
Social Complexity	1	"Definitely collaborative. Inter-sectoral. state, private sector and civil society. Skills shortage driving development of public private partnerships. Threat information sharing, specific schemes to exchange staff between state and private sector. Private public cooperation essential"

Table 70 Participant M Wicked Problem Codeable Events

Label	Paragraphs	Text
No definitive formulation	1, 8	"Difficult to protect from every possible angle"
		"Not always a bad thing to have vulnerabilities that enable the state to be able to keep an eye on what is going on"
Stopping Rule	5, 9	"systems connected everywhere are vulnerable everywhere"
		"Tit for tat hacking could be highly unproductive"
No True or False	6	"Threat of regulation will induce self-regulation in some areas. Need to be careful about stifling innovation. Balancing act and difficult to get right."
No solution test		
One shot operation		
Potential		
Solutions		
Unique	1	"Traditional methods of protection don't apply and something different is needed"
Symptom	5	"People losing passwords, being members of Ashley Madison – catastrophic mistakes and consequences create a chain of events – virtualised data systems that provide access to everything – systems connected everywhere are vulnerable everywhere"
Explanation	3	"…sleeper type threat is almost undetectable until you understand normal behaviour…"
No right to be wrong	3	"Believe mediated data – believe instruments and tools above own senses."
Social Complexity	2	"…a level of social pressure and a normalisation of behaviours and social community"
		"Issue with other countries not conforming"

End of Document