THE CYBER SECURITY DILEMMA AND THE SECURITISATION OF CYBERSPACE

STEVE HERSEE

Submitted to Royal Holloway, University of London for the award of Doctor of Philosophy in Information Security

Supervised by

Professor Pete Adey

Professor Keith Martin

Declaration of Authorship

I Steven Hersee hereby declare that this thesis and the other work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed: _____

Date: _____

ABSTRACT

This thesis analyses the different securitisations of cyberspace by the Digital Rights Community (DRC) and the British state. It considers both the internal and external characteristics of these securitisations, covering the power relations between a variety of securitising actors and their audiences and the use of language and metaphor to construct cyberspace threats. It considers the consequences of these securitisations, paying particular attention to the interplay between threats to national security and threats to digital rights, which are often framed as competitive and mutually exclusive.

After considering the competitive nature of these securitisations, this work frames the conflict as a security dilemma, which has resulted in a spiralling, legal, public relations and technological conflict between the British state and the DRC. This has led to distrust, enmity, an inability to co-operate and a sub-optimal outcome for both national security and digital rights. The characteristics of this Cyber Security Dilemma (CSD) are analysed to help understand why it has arisen, why it has become so intense and why it is proving difficult to mitigate or transcend. Fear, uncertainty and a failure to appreciate the concerns of the other side are established as the most significant causes of the conflict.

This thesis draws on historical examples, theoretical material and examples from the television show Hunted, where the researcher was both performer and ethnographer. Techniques to help resolve the CSD are discussed, with attention paid to the need for trust building, interpersonal bonding and security dilemma sensibility. Current and historical attempts to resolve the issue are analysed for their effectiveness and a range of principles are proposed to help guide future approaches to the issue. These include the need to establish trust, work in collaboration with others, reject extreme rhetoric and raise the quality of the debate.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

1: INTRODUCTION, LITERATURE REVIEW AND METHODOLOGY

The 2013 Snowden disclosures exposed and reinvigorated a conflict between governments and the Digital Rights Community (DRC) which originated in the 1960s. The conflict reflects differing views on how digital rights and national security should co-exist in cyberspace and is fuelled by the potential for cyberspace to facilitate both crime and state surveillance, on a massive scale. Whilst the Foundation for Information Policy Research (FIPR) declared the conflict over in 2005, the Snowden disclosures demonstrated that it has never ended; 'the fight simply entered the next round, with stakes raised and gloves off' (Moore & Rid, 2016, p. 8; Foundation for Information Policy Research, 2005). The conflict has eroded trust between the British state and the DRC, which has led to widespread opposition to state surveillance and disputes between the government and technology companies over how they co-operate on criminal and terrorist investigations.

Using the Copenhagen School's Securitisation Theory, this thesis explores the origins of the conflict, the relationships between the key actors and the impact of language on its intensity and durability. It frames the conflict as a security dilemma and considers how suspicion and mistrust have created a spiralling conflict that reduces security for both sides. The thesis concludes with an assessment of past attempts to ease the conflict and suggests strategies that could be employed to help resolve it.

1.1 CONTEXT

The term cyberspace was introduced by William Gibson, within his 1982 story, 'Burning Chrome' but was popularised in his 1984 novel, 'Neuromancer'. Gibson describes cyberspace as 'a consensual hallucination experienced daily by billions of legitimate operators … Unthinkable complexity' (Gibson, 1984, p. 67). Since then cyberspace has assumed a variety of meanings. The term is often used as a metaphor for space and is used to describe a virtual space which can be inhabited, owned and operated in. The US Air Force claims to fly and fight in cyberspace and digital rights activists, such as John Perry Barlow, claim that they 'come from cyberspace' (Barlow, 1996; United States Air Force, 2006). Cyberspace is also used as a synonym for the Internet, although it is generally considered to encompass a broader swathe of technology, including the Internet and any other information

systems that affect our lives (HM Government, 2011, p. 11). For this work, the term cyberspace is used to describe the environment that emerges from the connection of computing devices, including the geographical, political, legal and social characteristics of this space.

Cyberspace is now accessed by over three billion people worldwide and has become a critical element of infrastructure within the United Kingdom (UK) (Internet Live Stats, 2015). It brings seemingly endless opportunities for states, industry and society, including enhanced communication, economic opportunities, networking tools and more open government. It also has more controversial applications for the security and military sectors and provides safe environments for individuals to oppose the state and circumvent the law. Cyberspace is constructed as a space that threatens both individual rights and national security and this has led to an ongoing debate over how it should be governed.

1.1.1 The Crypto Wars

The Crypto Wars emerged in the 1960s and 1970s after cryptography became more accessible to the public and it became increasingly evident that the public's desire for secure communication was at odds with the government's approach to national security. In 1976, Whitfield Diffie and Martin Hellman published proposals which allowed two parties, with no prior knowledge of each other, to jointly establish a shared secret key over an insecure network, thus allowing them to communicate in secret (Diffie & Hellman, 1976). For digital rights campaigners, this technique had potential to protect them from government intrusion, but for the British and American governments, it could further deny law enforcement the data they needed to prevent and investigate crime.

In the US, one of the National Security Agency's (NSA) first major actions on public encryption related to the Data Encryption Standard (DES), which was published in 1977. The algorithm was developed by IBM and was submitted to the National Bureau of Standards in response to an invitation to companies to propose a secure encryption standard. After initial submission, the NSA worked with IBM to reduce the key size from 64 to 56 bits, which strengthened the algorithm against attacks such as differential cryptanalysis but weakened it against brute force attacks. This made DES stronger against most attackers but weaker against those with massive computing power, such as the NSA itself. The algorithm was approved and put into widespread use around the world but many were suspicious of the NSA's

involvement, considering it to be 'born in sin' (Stowsky, 2003, p. 18). The NSA's plan to control encryption standards was a partial success since DES was widely adopted, but it also damaged trust in the NSA as an honest defender of cybersecurity.

In 1991, Phil Zimmermann developed Pretty Good Privacy (PGP), which was designed to be used to sign, encrypt and decrypt texts, emails and files. Zimmermann, a long-time anti-nuclear activist, released the source code free-of-charge to Peacenet, which supported grassroots political organisations, a Usenet newsgroup, and several internet bulletin boards. In 1993 Zimmerman was investigated by the US government for exporting the software without a license, as cryptosystems with keys larger than 40 bits were treated as munitions. Zimmerman then attempted to avoid regulations by publishing the entire source code in a book, which are protected under the US first amendment (Zimmerman, 1995).

The next major salvo in the Crypto Wars came in 1993 with the introduction of the Clipper Chip, which was an advanced microchip that could provide strong cryptographic protection for communications. A copy of each chip's decryption key would be stored in escrow by the US government so that they could decrypt messages if required. The Clipper Chip faced immediate opposition from technical experts who said it was insecure, and human rights advocates who said it was a huge breach of civil liberties. It was discredited in 1994 after Matt Blaze from AT&T published a paper on significant vulnerabilities in the hardware (Electronic Privacy Information Centre, 1994; Diffie, 1993; Blaze, 1994). Following the failure of the Clipper Chip, the US government continued its attempts to force companies to store encryption keys in escrow. In new proposals a government-certified third-party would keep a key to every device used for communications so that the government could access it if required. The proposals were fiercely opposed by the same technologists and civil liberties advocates who had opposed the Clipper Chip. Many technology companies also objected due to the expense of implementing such a system and the US government eventually dropped the plans (Abelson, et al., 1997). In the following years, state intelligence agencies attempted to circumvent this problem of encryption by weakening encryption protocols, seeking to enforce hardware and software key escrow, infiltrating cryptographic services, co-opting encryption providers and banning the export of encryption (Bowcott, 2015; *The Guardian*, 2013). On the other side, the DRC tried to improve cryptography and encourage its increased implementation amongst service providers and the public (Electronic Frontier Foundation, n.d.).

In the UK, the Crypto Wars followed a similar path to the US, although the British government restricted the sale of encryption services for longer. On 25th May 2005, following the expiry of a sunset clause in the Electronic Communications Act which would have allowed the UK government to regulate companies selling encryption services, the Foundation for Information Policy Research (FIPR) declared that the 'the "Crypto Wars" are finally over - and we've won!' (Foundation for Information Policy Research, 2005). In 2010, as cyber attacks became more prominent and the threat of cyber warfare was brought to the fore, the UK government began to focus attention on the cyber threat. The 2010 National Security Strategy (NSS) labelled cyber attack as a tier one national security threat, alongside terrorism and an international military crisis (HM Government, 2010). The subsequent 2011 UK Cyber Security Strategy further highlighted the scale of the threat and committed the government to spending £650 million[1] to combat it.

Whilst many believed that the DRC had successfully won the Crypto Wars, the British and American governments continued their attempts to gain access to encrypted communications through alternative means. The 2013 Snowden disclosures revealed that the Government Communications Headquarters (GCHQ) and the NSA had, for years, been undermining encryption standards, stealing encryption keys and coercing companies into installing backdoors into their software (*The Guardian*, 2013). Snowden's intelligence disclosures placed state surveillance under the spotlight, turned the issue into mainstream news and intensified the conflict. The DRC argued that state surveillance intruded on everyone's rights and compromised everyone's security, whilst the British state suggested that encryption was making cyberspace anarchic and inaccessible to law enforcement (Open Rights Group, 2015). Following the murder of Lee Rigby, the intelligence and Security Committee (ISC) concluded that encryption was becoming increasingly problematic and the Director of GCHQ, Robert Hannigan accused social networks of acting as the 'command and control centres of terrorism' (Hannigan, 2014). Following a terrorist attack on Westminster Bridge in London, the government called for social media companies to do more to ensure that their technology was not used to facilitate terrorism (Intelligence and Security Committee of Parliament, 2014; Rudd, 2017).

[1] This later rose to £850 million

Whilst often fought behind the scenes, the dispute has occasionally erupted into open conflict. Following a terror attack in San Bernardino in the US, Apple and the FBI engaged in a very public conflict over access to data on the perpetrator's encrypted iPhone. During the conflict Apple CEO, Tim Cook, accused the FBI of trying to create the software 'equivalent of cancer' and the FBI's supporters accused Apple of supporting terrorism (Cotton, 2016; ABC News, 2016). The FBI wanted access to the iPhone belonging to the perpetrator of the attack, Syed Farook, because they believed that it could provide evidence of his motivations and potential intelligence on a wider terror network, but Apple refused as they believed that providing the FBI with access would grant them the ability to unlock any iPhone 5c, not just Farook's (Apple Inc, 2016). The FBI sought a court order forcing Apple to issue an update to the phone, which would then allow a brute force attack. But after Apple opposed the court order the FBI reportedly purchased knowledge of a vulnerability in the iPhone from an unnamed black-market vendor (Aspen Institute, 2016).

The dispute between the DRC and the British state reflects a wider conflict between individual rights and national security. Philosophers such as Thomas Hobbes and John Locke have long debated the degree to which individuals must surrender their freedoms in exchange for protection by a sovereign, but in cyberspace this is particularly challenging as the issue is constructed by each side as indivisible, intractable and binary (Locke, 2009; Hobbes, 2016). Encryption is constructed as the guarantor of digital rights but also as on or off, secure or not, broken or unbroken; 'Either we build encryption systems to keep everyone secure, or we build them to leave everybody vulnerable' (Schneier, 2016). Likewise, the state's ability to enforce the rule of law is constructed as dependent on its ability to access *all* encrypted communications. Without this, cyberspace will become 'anarchic' (Hogan-Howe, 2014). The conflict both inhibits co-operation, which could help improve both digital rights and national security, and justifies actions by both sides which might not ordinarily be deemed necessary or reasonable.

1.2 Research Design

This thesis is a study of the conflict between the British state and the DRC, covering the seven-year period following the release of the NSS. The aim of the research is to critically assess this conflict, help to identify strategies to help resolve it and address current gaps in our academic knowledge.

Despite much academic writing on surveillance, digital rights, the Crypto Wars and the securitisation of cyberspace, there is little research that addresses both the actions of the government and the DRC. There is a lack of research on how the DRC constructs cyberspace threats and the role they play in the conflict. This research aims to address this by providing a comprehensive assessment of threat constructions by both the DRC and the British state, highlighting similarities and differences.

There are many proposed solutions to this conflict, but these primarily focus on how one side (usually the state) should change its policies to mitigate the concerns of the other (Cavelty, 2014). More research is required into how the interplay between the two sides serves to generate and exacerbate the conflict itself, which is the gap the research in this thesis aims to fill. Having established the nature and intensity of the conflict, this research also aims to help inform policymakers by identifying and analysing strategies that can benefit both digital rights and national security.

1.2.1 Research Questions

To achieve this, the following research questions and objectives are considered.

Q1: How do the British state and the DRC construct cyberspace threats?

An understanding of the following aspects will help to address this question;

- The key actors and audiences involved in the construction of cyberspace threats;
- The power relations between the key actors and how these influence the acceptance and institutionalisation of these threats;
- How the linguistic and grammatical characteristics of these threat constructions influence the acceptance and institutionalisation of these threats.

Q2: How have competing threat constructions led to conflict between the DRC and the British state?

An understanding of the following aspects will help to address this question;

- The degree to which the conflict between the DRC and the British state conforms to norms of conflict within international relations;
- The factors that intensify or alleviate the conflict.

Q3: What strategies can be applied to help resolve this conflict?

An understanding of the following aspects will help to address this question;

- Whether challenging the threat constructions underpinning the conflict between the DRC and the British state can help to alleviate the conflict;
- Existing attempts to resolve the conflict and their success or failure;
- The most successful efforts and potential future strategies.

1.2.2 Scope

Due to the interconnected nature of cyberspace, it is difficult to establish precise geographic and political boundaries for this thesis. The following represents the general focus of this thesis, although additional material from outside these bounds is occasionally used, where necessary.

1.2.2.1 Political Area of Interest

Conflicts between digital rights campaigners and nation states exist in different forms throughout the world, but the dispute is particularly interesting in the UK. Due to its sophisticated surveillance capabilities and the exposure of these capabilities by Edward Snowden, its modern and comprehensive surveillance legislation and the high profile of its national security threat, the UK is a fascinating environment to study this dispute.

- Alongside the US, the UK was one of two countries to have a significant proportion of its surveillance capabilities exposed to the world by Edward Snowden. Whilst the documents were taken from the NSA, they also included huge volumes of material about GCHQ and brought significant attention to the UK's surveillance operations.

- The UK has some of the most well-known intelligence agencies in the world, including the signals intelligence agency GCHQ. This agency has seen its funding increased, despite other government cuts, and is thought to 'punch above its weight' due to its close relationship with the NSA and other intelligence agencies (The Telegraph, 2015). GCHQ has risen to public prominence due to its increasing role in national security protection, as well as the Snowden disclosures.

- The Investigatory Powers Act (IPA) was enacted in November 2016 and whilst its justification and implications are disputed, it is unarguably one of the most modern and comprehensive pieces of surveillance legislation in the world. It provides both extraordinary powers and unprecedented oversight of the intelligence agencies.

- Terrorism and national security have been major influences on public discourse since the 2001 attacks in New York. Periodic terrorist attacks in the UK have kept the terrorist threat in the news and public consciousness. The link between terrorism and cyberspace ensures that cybersecurity is an important facet of national security, giving it enhanced status and attention.

Whilst the primary focus of this research is the UK, the interconnectedness of cyberspace, combined with the international nature of rights organisations and technology companies, means it is necessary to also consider external events. Events in the US are particularly relevant due to close political and security co-operation and the fact that major technology companies, such as Apple and Google, are headquartered there.

1.2.2.2 Timeframe

This work focuses primarily on events that occurred in the seven-year period following the publication of the UK NSS, which include the Snowden disclosures, the passage of the IPA, the wide-scale rollout of end-to-end encryption and continued terrorist attacks. This work will also draw on historical events which have had an enduring impact on the conflict.

1.2.2.3 Key Actors

A variety of actors contribute to the conflict between national security and digital rights but, for this work, the securitising actors have been split into two broad groups, the Digital Rights Community (DRC) and the British state. The DRC is deliberately broad and encompasses all those who support digital rights and consider state surveillance to be a threat to those rights. Actors within the DRC include technology companies, whistle-blowers, academia, Members of Parliament (MPs), celebrities, human rights organisations, security experts and members of the public. To limit the scope of this project, the role of the media will not be directly addressed, although other research suggests it plays a significant role in securitisation and conflict (Hass, 2010). The opposing grouping could be labelled

the National Security Community, but can be more narrowly defined as the British state, which consists of those organisations responsible for defending national security. Whilst it is acknowledged that these groups are not homogeneous and individuals within them carry a wide spectrum of opinions, the terms DRC and British state are used to help identify the predominant attitudes and opinions within them.

1.2.3 Analytical Frameworks

To address the research questions, two separate and complementary analytical frameworks are used. The Copenhagen School's Securitisation Theory is used to help understand how cyberspace threats are constructed, why these constructions are accepted or rejected by different audiences and how this empowers the state and the DRC. This constructivist framework is used because it facilitates the study of the relationship between the securitising actors and their audiences, rather than focussing on the nature of cyberspace threats themselves, which is the subject of other work (Deibert, 2012; Deibert & Crete-Nishihata, 2012; Stohl, 2006). By focussing on how threats are constructed, this research can avoid becoming entangled in the conflict itself and instead focus on the purpose and consequences of these threat constructions. As Dunn Cavelty argues, 'the elusive and unsubstantiated nature of cyber threats means that approaches rooted in the constructivist mindset with a subjective ontology are particularly suitable for its analysis' (Cavelty, 2007, p. 21).

Herz and Butterfield's concept of the security dilemma is also used to help understand how the actions of the state and the DRC create a spiralling conflict of insecurity. Whilst the security dilemma is not a constructivist approach, it does complement the use of Securitisation Theory. The security dilemma framework helps to expose how each side fuels the conflict by eliciting fear in the other. By focussing on this element this research can engage with the core question of how the conflict between the DRC and the British state has arisen.

Figure 1.1 demonstrates how Securitisation Theory and the security dilemma are combined to help analyse the conflict.

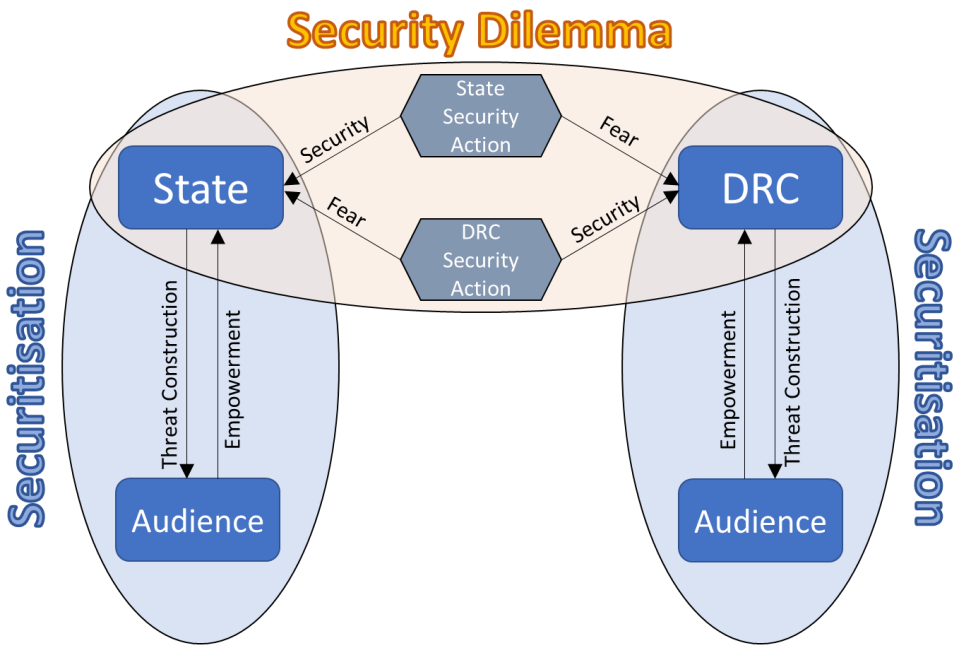

Figure 1.1: The relationship between Securitisation Theory and the security dilemma

1.3 Literature Review

This literature review provides an overview of current research into the conflict between the British state and the DRC and highlights a variety of research gaps, including a lack of focus on the UK, a failure to adequately consider how non-state actors securitise cyberspace, and a lack of research into the potential applications of the security dilemma to the conflict. The review considers how existing research already addresses some elements of the research questions and enables data collection to be targeted towards these gaps in current knowledge. This review considers research from a wide range of disciplines, including Information Security, International Relations, Security Studies, War Studies and Geopolitics. The first half starts by considering the broad issues of cyberspace governance and then focusses on the conflict between digital rights and national security and the framing of surveillance as a form of control, through the concept of Panopticism. The second half considers how cyberspace threats are framed and discusses the theoretical frameworks of securitisation and the security dilemma.

1.3.1 Cyberspace Governance

The issue of cyberspace governance is critical to this work, since it is through control of cyberspace that the state can promote and deliver national security and the DRC can promote and deliver digital rights. There is a substantial body of work relating

to cyberspace governance, although this largely focusses on efforts by states to censor, control and filter cyberspace. The terms 'internet governance' and 'cyberspace governance' are highly contested but, as Milton Mueller suggests, discussion of the issue is often framed around cyber-libertarian and cyber-conservative rhetoric (Mueller, 2010). Either the state can extend its normal governance structures to the Internet or technological determinism means that central control is not achievable and power is in the hands of civil society. But the state and civil society are not the only actors involved in the governance of cyberspace. The World Summit on the Information Society defines the key actors in cyberspace governance as states, the private sector, civil society, and intergovernmental and international organisations (World Summit on the Information Society, 2003). These groupings define the key stakeholders in internet governance and have been adopted widely, including by Jovan Kurbalija in his Guide to Internet Governance (Kurbalija, 2016, p. 225). Whilst much of the literature on internet governance is grouped around the state and civil society, the emergence of large and influential technology companies has led to additional scrutiny of the increasingly important role they play.

1.3.1.1 The State

In the 1980s and 1990s, many writers associated cyberspace with the general notion of the decline of the state. Michael D Birnhack, for example, discusses perceptions of cyberspace in the 1990s, which describe the Internet as a 'post-national situation' ruled by a mixture of industry and anarchy (Birnhack & Elkin-Koren, 2003, p. 2). The state had supposedly abandoned its role in governing cyberspace and left the domain to the 'invisible hand' of market powers. But Birnhack argues that the turn of the millennium marked the 'comeback of the state' which was reflected in attempts to recentralise and take control of existing private nodes of power. 'These nodes of power and control are now being recruited, or co-opted, to serve the State and in fact, many powerful private entities are volunteering to join the State's efforts' (Birnhack & Elkin-Koren, 2003, p. 2). Birnhack's warning that 'this convergence might lead to an unholy alliance with potentially troublesome results', is echoed by other writers and institutions such as the Citizen Lab in Canada, which conducts research into increasing state authority in cyberspace (Birnhack & Elkin-Koren, 2003, p. 2; Senft, et al., 2014; Senft, et al., 2014; Dalek, et al., 2013). Ronald Deibert counters early ideas that cyberspace could not be regulated and argues that states are now 'moving to assert their

interests more forcefully in cyberspace' by imposing increasing constraints on how their citizens interact with it (Ronald Deibert, 2012, p. 1). He highlights the tensions between the old norms and rules, which governed cyberspace and the state-based forms of control that are gradually replacing them. Milton Mueller follows similar thinking, arguing that previous questions of 'can the net be governed?' are now redundant and have been replaced by questions of whether it should be governed differently to everything else (Mueller, 2010, p. 1). He argues that there is a 'battle for the soul of the internet' and that 'the problem of governing the Internet has proven to be a disruptive force in international relations' (Mueller, 2010, p. 1). He dismisses both cyber-libertarian claims of ungovernability and state claims that cyberspace should be regulated like physical space, arguing that the Internet's disruption of communications technology precludes a return to business as usual.

1.3.1.2 Civil Society

Other authors consider how cyberspace can be governed by alternative means than the state. Michael Mehta uses Foucault's concept of governmentality or 'the art of governance', which includes not just state politics but also techniques to shape and control a population and an individual's ability to control itself (Foucault, 2002). He applies the concept to cyberspace and argues that governments have shifted from a reliance on violence to discipline their populations, to mechanisms of state normalisation, self-control and self-regulation, aided by increased state surveillance (Mehta & Darier, 1998; Lemke, 2001). Mehta also addresses self-governance, describing how unacceptable behaviour in internet chat rooms is punished by censorship. Kitchen, Dodge and Bartlett all consider how the absence of state authority can result in new forms of discipline arising. Rob Kitchen and Martin Dodge argue that customary laws play a significant role in cyberspace governance by facilitating the punishment of those who transgress the communal rules (Dodge & Kitchen, 2001).

> If participants of Multi-User Domains or newsgroups transgress the bounds of customary laws then they must accept community administered punishment (Dodge & Kitchen, 2001, p. 58).

Jamie Bartlett follows a similar train of thought, arguing that in 'dark web' markets, the lack of government enforcement results in greater scrutiny of the trustworthiness of sellers (Bartlett, 2015).

> There are no regulators to turn to if the seller or the site administrators decide to take your money. It's all illegal, at constant risk of take-downs or infiltration by law enforcement agencies. And yet dark net markets are thriving (Bartlett, 2015, p. 141).

Lawrence Lessig takes a different approach, considering the role that computer code plays in governing cyberspace. He argues that whilst laws, norms, market forces and architecture are the four major regulators of cyberspace, 'code regulates all aspects of our lives, more pervasively over time than any other regulator in our life' (Lessig, 1999, p. 233).

1.3.1.3 Technology Companies

Others consider the role of technology companies in cyberspace governance. Laura DeNardis considers the 'privatisation of Internet Governance' and the increasing role of internet content providers (DeNardis, 2010, p. 11). She highlights Facebook's role in internet privacy, Yahoo's cooperation with the Chinese government to expose dissidents, Twitter's cooperation with the US government during Iranian protests and Google's filtering of YouTube video (DeNardis, 2010, pp. 11-12). She also raises concerns over 'the use of Internet governance techniques for competitive advantage' (DeNardis, 2010, p. 16). In other work DeNardis and Andrea Hackl consider internet governance by, not of, social media platforms, considering their roles in anonymity, privacy and censorship (DeNardis & Hackl, October 2015). They argue that 'because of their unique role as the intermediaries providing citizens with access to the digital public sphere, social media platforms are central points of control on the Internet' (DeNardis & Hackl, October 2015, p. 1).

As Kurbalija suggests, these different conceptualisations of cyberspace governance often result in disputes (Kurbalija, 2016). Kurbalija argues that telecoms specialists view cyberspace through the prism of infrastructure, computer specialists view it through standards and applications, human rights activists view is from the perspective of freedom of expression and governments view it through the prism of threats and the protection of national interests (Kurbalija, 2016). These different constructions of cyberspace may also have a significant influence on the construction of cyberspace threats.

1.3.2 Digital Rights and National Security

The conflict between the British state and the DRC in cyberspace is situated within a wider conflict between human rights and national security and the literature in this area is grounded in the work of Thomas Hobbes and John Locke. Hobbes describes the 'state of nature' as an environment where every man is equal and must fight for survival, thereby creating a natural state of war (Hobbes, 2016). In Hobbes' conceptualisation, every man has liberty but in the absence of security, life is 'solitary, poor, brutish and short' (Hobbes, 2016, p. 39). Hobbes suggests that to escape the state of nature individuals must lay down some liberty and confer strength in a single sovereign (the Leviathan), which can provide security for all. John Locke also considers the need for a sovereign but argues that absolute or arbitrary powers are a potential threat to liberty so the people should maintain the power to dissolve the sovereign when required (Locke, 1689, p. 133). Locke proposes the 'prerogative', which is the power held by the sovereign to act for the public good but suggests that this must only be exercised in the interests of the people. The problem of 'who shall judge when this power is made right use of' is left open as Locke concedes there that is no answer but to 'appeal to Heaven' (Locke, 1689, p. 168).

The views of Hobbes and Locke are reflected in the 'reason of state' doctrine, which is outlined by Giovanni Botero and describes how state power can be exercised according to whatever is required to maintain itself (Botero, 2017). The doctrine argues that the state may act beyond the law if it does so for the common good, for the good of the people or the preservation of the state. Mark Neocleous demonstrates how 'reason of state' has morphed into 'interest of state', 'security of state' and finally 'national security' (Neocleous, 2006). Charles de Secondat argues that because the state is the creator of individual security and the guarantor of liberty, national security can be used to justify any action that is designed to protect the state, even if this transgresses the law or normal moral bounds (Secondat, 1749).

> If the legislative power believed itself endangered … it could, for a brief and limited time, permit the executive power to arrest suspected citizens who would lose their liberty for a time only so that it would be preserved forever (Secondat, 1749, p. 159).

The argument that liberty must be traded for privacy is contested by Mark Neocleous who claims that 'the supposed search for a balance between security

and liberty is misplaced' (Neocleous, 2007, p. 132). Instead, he suggests that the idea of insecurity should be embraced.

> To keep harping on about insecurity and to keep demanding more security (while meekly hoping that this increased security doesn't damage out liberty) is to blind ourselves to the possibility of building real alternatives to the authoritarian tendencies in contemporary politics … simply accepting insecurity as part of the human condition would, for a start, help in resisting everything being described as a security issue' (Neocleous, 2007, p. 147).

The conflict between national security and human rights in cyberspace is particularly intense because it is framed as absolute and extreme. Either the state is abusing individual liberties through mass surveillance or we risk anarchy due to the state's lack of ability to access areas of cyberspace. Most literature focusses on these extremes, although some commentaries argue that a balance between the two should be struck (Amnesty International, 2013; Clegg, 2014; Huppert, 2013).

1.3.2.1 Digital Rights

Since the 2013 Snowdon disclosures, the volume of research into the impact of cyberspace on digital rights has increased and a range of writers conclude that surveillance is disproportionate and damaging to digital rights. David Lyon argues that surveillance is a prominent means of power for governments but is 'out of control' and carries 'major risks for ordinary citizens' (Lyon, 2015, p. preface VII). It has, he argues, 'ballooned in recent decades' and become 'increasingly unaccountable and less and less visible to ordinary people' (Lyon, 2015, p. 12). The UN's special rapporteur for human rights, Frank L Rue argues that states are increasingly acting to 'restrict, control, manipulate and censor content disseminated via the Internet without any legal basis' (Rue, 2011, p. 8). He suggests that these actions are being taken in a manner incompatible with human rights and create a 'chilling effect' on the right to freedom of opinion and expression (Rue, 2011, p. 8). Deibert covers the same theme and writes extensively on the impact of surveillance and filtering measures on both citizens and cyberspace itself (Deibert & Rohozinski, 2008). Deibert divides cyberspace into three spheres of agency to understand how the state 'targets' cyberspace; civic networks, resistance networks and darknets. He then examines how the state exerts its power over these groups

through increasing use of Internet filtering, censorship and surveillance, at the expense of individual rights (Deibert, 2008).

1.3.2.2 National Security

Whilst there is a significant body of literature which considers how the state impinges on digital rights, there is also a substantial body of work that invokes the Hobbesian 'state of nature' to focus attention on threats to national security. David Tohn, for example, argues that without a cyber sovereign, cyberspace is a wild and ungoverned place.

> 'If Philosopher Thomas Hobbes lived today, he would say man's cyber-life is nasty, brutish, and if you are not careful, short. The world of cyber-crime, cyber-terrorism, and cyber-warfare is truly a wild, unruly, and ungoverned place' (Tohn, 2009).

Tohn argues that today's 'cyber world' is akin to medieval Europe and needs state intervention to tame it. Speaking at the Munich Cyber Security Conference, the President of Estonia, Toomas Hendrik Ilves, also compares cyberspace to a state of nature claiming that 'Our world is Hobbesian' and 'we need our Locke, Jefferson and Voltaire for the digital age' (Ilves, 2014). Although Ryan Kaminski argues that whilst there are no international institutions that remotely resembles a Hobbesian Leviathan, the cyber state of nature can still be escaped as the reality of the situation forces states to commit the 'political muscle' to do so (Kaminski, 2010, p. 91).

Other authors draw attention to specific threats to national security from cyberspace. Dan Verton warns that the next terrorist attack on the United States (US) could come from cyberspace and it could 'wreak havoc' and have a 'debilitating effect on the economy' (Verton, 2003, p. 9). He argues that countries are making it easy for would-be attackers by publishing 'vast amounts of data about our infrastructures', including information about vulnerabilities (Verton, 2003, p. 9). Richard A. Clarke paints a similarly apocalyptic image of cyberspace, arguing that the speed with which cyber weapons can be deployed creates the prospect of a 'highly volatile crisis' between states. This, he argues, cannot be avoided through deterrence, in the same way that nuclear war is (Clarke, 2010, p. 9).

Other authors have written of the threat to national security from the dark web and other spaces online that are inaccessible to the state. Gabriel Weimann highlights several examples where terrorists have communicated and planned

attacks online using encrypted applications such as Telegram (Weimann, 2016). Whilst noting that we should not impair legitimate and lawful freedom of expression, he argues that 'the alarming infiltration of Internet-savvy terrorists to the "virtual caves" of the Dark Web should trigger an international search for a solution' (Weimann, 2016, p. 204). Moore and Rid also identify the dangers of dark webs, by producing analysis demonstrating that 'the most common uses for websites on Tor hidden services are criminal, including drugs, illicit finance and pornography involving violence, children and animals' (Moore & Rid, 2016, p. 21).

1.3.3 Panopticism

A central element of the conflict between the DRC and the British state is the DRC's fear that state surveillance compromises individual rights. Whilst the state considers surveillance to be targeted towards criminals and terrorists the DRC fear that surveillance is not just passive but acts as a form of control, undermining individual choice, privacy and personal freedoms. This idea is often expressed in the literature through the concept of Panopticism, which is based around Jeremy Bentham's 18th century design for an ideal prison. The Panopticon allows a single guard to observe all inmates and is designed to condition good behaviour because the inmates never known when they are being observed.

Foucault develops the concept of Panopticism as a metaphor for modern disciplinary societies and their desire to normalise behaviour (Foucault, 1975). Foucault argues that the Panopticon creates a consciousness of permanent visibility as a form of power, where bars, chains, and heavy locks are no longer necessary for domination and discipline. He contends that Panopticism is not just limited to prisons, but can be applied to many different areas of society, including schools, hospitals and factories. Whilst his work preceded the widespread use of computers, his invocation of the Panopticon as a metaphor for societal control has been applied by other writers, to areas such as biometric passports, identity chips, and the commercial sector (Jensen & Draffan, 2004; Haiven & Stoneman, 2004; Head, 2014). Panopticism was first applied to cyberspace by Shoshana Zuboff, who describes how computer power makes the output of workers more observable, whilst workers cannot tell when they are being observed (Zuboff, 1989).

The literature around Panopticism can be grouped into approaches that consider the state as the operator of the Panopticon and approaches that consider the role of technology companies and the public. Several authors suggest that state

intelligence agencies, including GCHQ and the NSA, are attempting to turn the whole of cyberspace into a global Panopticon. Zachary Bruno argues that the NSA's PRISM program, combined with the increasing popularity of smartphones, has resulted in the Foucauldian Panopticon being everywhere at all times (Bruno, 2014). Whilst most academic writing focusses on the US and the NSA, various media reports in the UK have highlighted the similarities between GCHQ and the Panopticon. John Lanchester, for example, writes in the Guardian that 'we risk becoming a society which is in crucial respects a giant Panopticon, where the people with access to our secrets can see, hear intercept and monitor everything' (Lanchester, 2013).

Other authors, such as Stephanie Fast, address the role of social media companies and their ability to observe and influence user behaviour. Fast compares the social network Facebook with the Foucauldian Panopticon and finds significant parallels in its structure and use of surveillance, examination and normalisation (Fast, 2015). She describes how the structure of Facebook encourages users to share data, which is then widely accessible and used to deliver advertising and normalise user behaviour. Fast also compares the Foucauldian idea of the Panopticon as a laboratory with an experiment by Facebook's Core Data Science Team, which altered users' newsfeeds to see how this changed their mood. (BBC News, 2014).

The voluntary nature of social media panopticons is addressed by Lilian Mitrou et al, who consider how social media draws users into self-participatory Panopticons that enable sensitive information to be reconstructed from seemingly anonymous data (Mitrou, et al., 2014). They demonstrate how YouTube and Twitter can be used to profile users, with only limited computing power and publicly available data. Susan Barnes also considers the participatory nature of Cyber-Panopticons but focusses on the 'privacy paradox', which describes how, despite increased concern over online privacy, individuals still share increasing volumes of personal information on sites such as Facebook and Twitter (Barnes, 2006). Utz and Kramer describe the paradox as an apparent discrepancy between privacy concerns and privacy behaviours and Nissenbaum claims that people appear to want and value privacy, yet simultaneously appear to not want or value it (Nissenbaum, 2009; Utz & Kramer, 2009).

These different perspectives on who controls, utilises and participates in the Cyber Panopticon reflect the wider issues of cyberspace governance and the conflict between national security and digital rights.

1.3.4 The Construction and Framing of Cyberspace Threats

In addition to a host of work identifying cyberspace threats, several writers have also considered how the dispute between national security and digital rights has been framed and constructed by a range of actors.

Author's including Myriam Dunn Cavelty, consider the framing of cyber threats by states. Cavelty highlights the fact that cyber threats have consistently been framed as a grave danger by the US, despite a large attack having never materialised (Cavelty, 2007). She suggests that both 'hypers' and 'de-hypers' agree on this point but differ as to whether a future attack is imminent or not (Cavelty, 2007, p. 20). Cavelty suggests that in the wake of the September 11 terror attacks on the US, cyberspace is linked seamlessly with the concepts of terrorism and technology, thus ensuring that cyber threats are 'inevitably presented as a national security issue' (Cavelty, 2007, p. 29). Hansen and Nissenbaum explore how different forms of discourse are used to securitise cyberspace as a threat to national security by employing different grammars of security (Hansen & Nissenbaum, 2009).

Other authors consider the impact of this discourse on cyberspace threat construction. Yury Kabanov analyses the discourses and policies of the European Union (EU) and Russia to help understand the obstacles to cooperation on cybersecurity issues (Kabanov, 2014). After comparing the different contexts, actors, referent objects, security sectors and grammars of the discourse, Kabanov argues that the different policies of the EU and Russia and the problems of co-operation are the result of major dissimilarities in the understanding of cyberspace threats as well as different grammars of security.

David Gorr and Wolf Schünemann also consider the differences in cybersecurity discourses between different regions, focussing on a comparison between Germany and Russia (Gorr & Schünemann, 2013). Employing the 'Sociology of Knowledge Approach to Discourse' (SKAD), they place discourse into interpretative schemes such as 'Perception of Cyberspace', 'Challenges', 'Framework for Action' and 'Propositions for Action' (Keller, 2006; Foucault, 1971). Using this system, they dissect, categorise and compare German and Russian discourse and find that whilst securitisation is evident in both countries, perceptions of cyberspace and risk differ significantly. German discourse is more heavily focussed on the stability of the economy whilst Russian discourse is more focused towards the stability of the political system.

Whilst these approaches compare different cyberspace constructions across different geographic regions, they do not consider different approaches within the same region but pertaining to different issues. For example, there is no current work that compares the construction of threats to digital rights in the UK with the construction of threats to national security.

1.3.5 Cyber Securitisation

Myriam Dunn Cavelty considers how threat construction impacts on the cybersecurity discourse (Cavelty, 2013). She classifies threats into technological, socio-political and human-machine clusters and considers how these are represented in cybersecurity discourse. Threats in the technological cluster are often represented through biological and military metaphors, such as viruses and weapons; threats within the socio-political cluster are often associated with lawlessness and anonymity, and threats in the human-machine cluster are often associated with vulnerability and unknowability. Cavelty suggests that this use of language has a significant impact on cybersecurity debates. Biological and military terminology speak to deep-seated fears in the human psyche that make national security solutions the logical choice. The spatial metaphor of cyberspace encourages activists to perceive cyberspace as a frontier and place of freedom, whilst also encouraging law enforcement to see it as a lawless space that must be tamed (Barlow, 1996; Hogan-Howe, 2014).

The most common theoretical framework used to consider the construction of threats in cyberspace is Securitisation Theory, which proposes that issues become securitised in response to *speech acts* by *securitising actors*. Securitisation involves a *referent object*, which is perceived to be threatened, a *securitising actor* who carries out securitisation by means of a speech act and an *audience* who are receptive to this securitisation (Waever, 1989). If the securitising actor carries authority and performs the speech act in accordance with particular grammar rules, then the securitising act will be successful. If an issue becomes securitised then it is removed from political debate and 'extraordinary means' can be used to address the threat.

Whilst Securitisation Theory has been widely accepted as a useful mechanism for understanding how discourse influences the construction of security, some have criticised the rigidity of such an approach. Thierry Balzacq, for example, criticises the high degree of formality to the discursive action of security, arguing that this

results in the concept of security as a speech act having a fixed, permanent, unchanging code of practice (Balzacq, 2005). For Balzacq, this reduces securitisation to a conventional procedure, with rigid conditions for success. Instead, Balzacq suggests that securitisation should consider the role that context plays in a securitising act, arguing that how an act resonates with an audience's feelings, beliefs, histories and culture, is critical to its success. Others criticise Securitisation Theory's narrow focus on the speech act itself. Matt McDonald claims that 'the form of act constructing security within the Copenhagen School is defined narrowly, with the focus on the speech of dominant actors' (McDonald, 2008, p. 563). This focus excludes other forms of representation, such as images, and encourages focus only on the discursive interventions of those voices deemed institutionally legitimate to speak on behalf of a particular collective, usually a state.

Securitisation Theory has been applied to a wide range of different issues including the 'war on terror', Islam and migration (Vultee, 2010; Cesari, 2009; Boswell, 2007). Several authors have addressed the securitisation of cyberspace by the state, including Citizen Lab, which produces a variety of work designed to 'monitor, analyse and impact the exercise of political power in cyberspace' (Citizen Lab, n.d.). Ronald Deibert, the Director of Citizen Lab, focusses largely on the increasing spread of cyberspace controls and argues that despite a past widespread belief that 'cyberspace was immune to government regulation', scholarship now shows that 'governments can shape and constrain access to information, freedom of speech and other elements of cyberspace' (Deibert & Crete-Nishihata, 2012, p. 339). Deibert claims that commercial actors also securitise cyberspace and inflate threats to 'serve their more parochial market interests' and that this has an impact on government decision making (Deibert & Crete-Nishihata, 2012, p. 340). Deibert is highly critical of the spread of cyberspace controls, which he says represents a 'norm regression' (Deibert & Crete-Nishihata, 2012, p. 345).

Several authors argue that the state's securitisation of cyberspace is not justified. Clement Guitton argues that putting cyber threats at the national level is not justified and is inconsistent with how cybersecurity budgets are spent (Guitton, 2013). Helen Nissenbaum argues that state claims of national security threats in cyberspace have led to excessive reactions such as reduced restraints of government powers, breaks from normal democratic procedures and steep incremental funding for security agencies. She also warns that this form of

securitisation can 'open the population to the risk [of] suppression' (Nissenbaum, 2005, p. 72).

Other research has focussed specifically on the speech acts of government figures. Ola Hjalmarsson investigates state securitisation of cyberspace in the US, focussing particularly on the speech acts of the Obama Administration. He concludes that by invoking catastrophic disaster scenarios, such as Pearl Harbour and September 11, 'the securitizing actors can relate previous catastrophes to hypothetical disaster scenarios involving cascading effects that present existential threats to a range of referent objects linked to cyberspace' (Hjalmarsson, 2013, p. 20).

Others consider the means through which securitisation is achieved. Kevin Schwarz considers how the state securitisation of cyberspace in the US is achieved through 'technification', the process by which issues are constructed as technical, removed from political debate and left in the hands of experts (Schwarz, 2016). He concludes that 'cyberspace became conceived as a realm that was purely technical' and that this has led to 'technical experts acting as securitizing agents, securitizing cyberspace through technification' (Schwarz, 2016, p. 68). Most research in this area is focussed on the securitisation of cyberspace in the US and there is a lack of research specifically focussing on the UK.

The literature is often highly critical of state surveillance and the securitising acts which serve to legitimise it. Kingsmith, for example, concludes that 'closed censorship of the Internet translates to an Orwellian future, devoid of open-information, agency or digital freedom' (Kingsmith, 2013, p. 11). In doing so, Kingsmith and others are making their own securitising moves by constructing the state's securitisation of cyberspace as an existential threat to liberty, freedom and democracy. Michael Williams terms this concept 'the securitisation of securitisation' and outlines a strategy of utilising fear to 'inhibit processes of securitisation' (Williams, 2011, p. 454). Deibert applies a similar concept to cyberspace arguing that 'the securitization of cyberspace may be inevitable, but what form that security takes is not' (Deibert, 2012, p. 274). Deibert wants to securitise state surveillance because he believes that doing so will inhibit the securitisation of cyberspace as a threat to national security.

Whilst most of the literature focuses on the state as the securitising actor, there are some attempts to consider alternative perspectives. A.T. Kingsmith, for example, criticises both the hyper-libertarian and hyper-fascist conceptualisations

of cyberspace which he says creates a 'false dichotomy which makes simplistic and deterministic suppositions that new technologies perpetuate either freedom or control' (Kingsmith, 2013, p. 5). He argues that technologies are never about freedom or control but depend entirely on the social context in which they are situated.

Jens Kremer considers how cyberspace threats are conceptualised in different ways, which he calls different 'security mind-sets' (Kremer, 2014, p. 220). He considers a 'military security mind-set' that is primarily concerned with national security and a 'liberal security mind-set' which considers human rights and balancing interest. Kremer sees the issue of different security conceptualisations as 'the core of the problem when it comes to security and cyber threats' (Kremer, 2014, p. 221). His paper is illuminating but misses out a particularly significant 'security mind-set'. He suggests that the 'military security mind-set' calls for a massive militarisation of cyberspace, whereas the 'liberal security mind-set' attempts to regulate cyberspace threats through increased policing. Both mind-sets, according to Kremer, call for increased state activity in cyberspace and this neglects the widespread mind-set (highlighted in the literature above) that the state itself poses the greatest threat in cyberspace.

One author who fully considers the notion of securitising threats to digital rights is Mariya Georgieva, who considers the impact of alternative securitising actors, such as Edward Snowden (Georgieva, 2015). Georgieva argues that whilst the state has traditionally held the powers to 'identify threats, exaggerate their significance to its survival and employ far-reaching countermeasures to protect itself', Snowden demonstrated that alternative non-state securitising actors can challenge state securitisations (Georgieva, 2015, p. i). Georgieva argues that Snowden successfully reversed the thinking around cyberspace threats by replacing fear of threats to the state with a fear of the state itself. In doing so Snowden 'successfully shifted the focus of the securitisation of cyberspace from values such as the survival of the state and effective national security to the survival of privacy and personal choice' (Georgieva, 2015, p. 44).

Securitisation Theory was formulated to address how states construct threats and legitimise their security responses, so it is understandable that the literature focusses on the securitisation of cyberspace by the state. However, in the dispute between the DRC and the British state, the DRC also plays a significant role in constructing cyberspace threats by warning that surveillance threatens to destroy

both democracy and human rights (Berners-Lee, 2012; Muižnieks, 2013). This aspect has not been adequately addressed. Addressing securitisations by both the state and the DRC will not only provide a more complete picture of the conflict but will also help to inform how these competing securitisations interact with one another.

Further consideration of the security dilemma literature is made throughout Chapters 2, 3 and 5.

1.3.6 The Cyber Security Dilemma

Whilst Securitisation Theory addresses the concept of competing securitisations, it does not consider how these competing securitisations interact with each other. To address this issue, it is necessary to consider the literature on security competition.

Former White House security adviser Richard A. Clarke addresses the issue of cyber conflict between states. He argues that not only is state-based cyber conflict a serious threat, but is also increases the likelihood of traditional war (Clarke, 2010). James Farwell and Rafal Rohozinski analyse the Stuxnet cyber attack and warn of the danger posed by a confluence between cybercrime and state action (Farwell & Rohozinski, 2011). They argue that the existence of the broader 'Olympic Games' programme, which incorporated Stuxnet, undermines the argument that fears of escalation would make state-based cyber conflict implausible (Farwell & Rohozinski, 2012). Thomas Rid also engages with the concept of cyber conflict, but takes an alternative perspective, arguing that war is inherently violent and 'cyber attacks help to diminish rather than accentuate political violence' (Rid, 2013, p. xiv).

Helen Nissenbaum divides cybersecurity into two distinct conceptions; technical security and cybersecurity (Nissenbaum, 2005). Technical security is concerned with protecting computer systems and their users from attack through the three components of confidentiality, integrity and availability. Cybersecurity links computer security with notions of national security. Nissenbaum suggests that the inherent differences between the two means that they are placed in opposition and 'vie for public and expert support' (Nissenbaum, 2005, p. 73).

A substantial theoretical framework through which to study competing cyberspace securitisation is the security dilemma which addresses two interrelated issues; how to interpret the security actions of another and how to respond to these actions. The concept was proposed by John Herz and Herbert Butterfield and suggests that fear of the other can lead to spiralling arms races, insecurity and potentially war

between states, despite the benign intentions of each side (Butterfield, 1951; Herz, 1950). The security dilemma is applied to cyberspace by several writers including Ben Buchanan, who applies it to cyber espionage, Nicholas Rueter who applies it to cyber warfare and Myriam Dunn Cavelty who applied it to the conflict between national security and digital rights (Buchanan, 2016; Rueter, 2011; Cavelty, 2014).

Ben Buchanan uses the security dilemma to consider the offensive/defensive information problem with regards to state hacking in cyberspace (Buchanan, 2016). He argues that whilst state hacking may appear to be an offensive pursuit, such activity is often driven by defensive requirements. 'Two nations, neither of which seeks to harm the other, but neither of which trusts the other, will often find it prudent to penetrate each other's systems' (Buchanan, 2016, p. cover). One nation's attempt to secure itself through hacking and information gathering results in escalating tensions, increased hacking and less security for all. Buchanan suggests that there is no single solution to the problem, which must be addressed through multipronged efforts that establish stability, start to build trust and then begin to minimise the risks of misinterpretation.

Nicholas Rueter considers a similar dilemma between states but focusses on the prospect of cyber warfare (Rueter, 2011). He argues that cyberspace is particularly prone to the security dilemma because it is easier to attack than defend in cyberspace and it is difficult to determine whether a state's investment in cyber capabilities is designed for offensive or defensive purposes. Whilst describing the situation as grim, Rueter suggests it can be improved by the establishment of international institutions and norms to facilitate co-operation, technological developments to increase the cost of attack and better signalling of state intentions through cyber doctrine and increased transparency.

Myriam Dunn Cavelty argues that there is a security dilemma between the state and the public, which despite huge efforts and vast spending on cybersecurity, has resulted in cyberspace becoming more insecure (Cavelty, 2014). Dunn Cavelty argues that national security and a form of security that is relevant to the people 'should not and must not be at loggerheads with each other' and in cybersecurity, in particular, the two can meet (Cavelty, 2014, p. 703). However, unlike traditional conceptualisations of the security dilemma, which blame the emergence of security problems on the inability of two parties to understand the defensive nature of each other's security moves, Dunn Cavelty blames the state for the emergence of the Cyber Security Dilemma (CSD). She cites the militarisation of cyberspace, the

weakening of security through state-based malware, state attempts to de-anonymise cyberspace and the extension of the notion of national security to cyberspace as evidence of the state's role in reducing both individual and national security. In addressing the dilemma between national security and individual freedoms, Dunn Cavelty's work is the most applicable to this thesis, however she only addresses the CSD from the perspective of individual security and human rights. More research is required into the national security perspective and their fears that totally secure communications impede the ability of law enforcement to prevent and investigate criminal and terrorist activity.

Further consideration of the security dilemma literature is made throughout Chapters 4, 6 and 7.

1.3.7 Research Gaps

Existing research covers a wide range of themes related to this thesis. Research into cyberspace governance provides a good appreciation of the different types of governance that may be favoured by the DRC and the British state. Jovan Kurbalija's suggestion that different perspectives on the nature of cyberspace might cause disputes over cyberspace governance is useful to help unravel the different perspectives of the British state and the DRC. Research into national security and surveillance provides historical and real-world context to the dispute over national security and human rights and adds depth to the current understanding of the conflict between the British state and the DRC. Applications of Hobbes and Locke to cyberspace by Tohm, Hendrick and Kaminski provide insight into why the British state and the DRC consider cyberspace to be threatening and why this has resulted in conflict. But there are still gaps in the research, which are summarised below.

1.) There is a substantial body of work on the securitisation of cyberspace, which focusses primarily on the state as the securitising actor. This work is largely focussed on the US government as the key securitising actor and there are no comprehensive assessments of how the British state constructs cyberspace threats. Likewise, research into cyberspace discourse largely focusses on the US, Russia and the EU rather than the British state. Further work in this area will help build an appreciation of how the British state convinces the public of cyberspace threats and how this impacts on the conflict with the DRC.

2.) Whilst Mariya Georgieva studies Edward Snowden as an alternative securitising actor, there is a significant absence of work on the securitisation of cyberspace by the DRC. The conflict between the state and the DRC can only be understood if the actions and motivations of both sides are addressed, but current research is heavily focussed on the state. This is a significant shortcoming of the literature and needs to be addressed within this thesis. Such work can lead to a greater understanding of the conflict between the state and the DRC as it will provide a parallel understanding of how each side has constructed cyberspace threats and how these constructions interact to fuel the conflict. Likewise, existing research into cyberspace discourse is also focussed on states but needs to include DRC discourse as well.

3.) The security dilemma has been applied to cyberspace to help understand competition relating to cyber warfare and cyber espionage but only Myriam Dunn Cavelty applies it to the conflict between the state and the DRC. This work relates directly to the subject of this thesis, although its applicability is limited by its short length and failure to consider how the interaction between the two sides exacerbates the conflict. This thesis will thoroughly apply the security dilemma to the dispute between digital rights and national security, to consider how this conflict has arisen and why it has resulted in spiralling insecurity.

4.) Whilst current literature covers the consequences of state actions in cyberspace, such as the creation of cyber Panopticons, there is very little that covers the issues from the state's perspective. To understand the conflict between the state and the DRC it will be necessary to develop a greater understanding of the British state's fears and why they act as they do.

To address these research gaps a range of research techniques and data collection methods are considered.

1.4 APPROACH

The following three research questions will be addressed within this thesis;

1. How do the British state and the DRC construct cyberspace threats?
2. How have competing threat constructions led to conflict between the DRC and the British state?
3. What strategies can be applied to help resolve this conflict?

To consider how to answer these questions it is first useful to consider some existing approaches and their limitations.

1.4.1 Existing Approaches

A range of techniques have been used within the literature to address similar questions. When considering the securitisation of cyberspace most authors use primarily open source documentation. For example, in her analysis of US cyber threat discourse, Myriam Dunn Cavelty draws upon a range of sources, including formal US government policy documents, senate testimony, speeches, lectures and official statements (Cavelty, 2007). Research into the securitisation of cyberspace by the DRC is limited to Mariya Georgieva's study of Edward Snowden as an alternative securitising actor (Georgieva, 2015). Georgieva uses open sources throughout her research including newspaper reporting, comments by his supporters and a variety of interviews he gave to the media.

Some authors have used comparative discourse analysis techniques to consider different acts of securitisation. These have also collected data from primarily open sources. In their comparative analysis of the different securitisations of cyberspace from the German and Russian governments, Gorr and Schünemann use data from open sources, including a relatively small sample of Russian (15) and German (17) government documents and existing interviews (Gorr & Schünemann, 2013). Kabanov takes a similar approach when considering the different securitisations of cyberspace by Russia and the EU (Kabanov, 2014). He uses specific government documents to demonstrate the evolving Russian and EU discourse on cyber threats and combines these with analysis of government policy and the creation of new institutions.

These works make significant contributions to the literature, but their reliance on government documents and published interviews limit their ability to reflect the motivations and intentions of the key influencing actors, which could be better understood through interviews or ethnographic work. However, the intelligence community is notoriously difficult to access for academic researchers, due to trust issues, secrecy and national security.

Academic work, utilising interviews and ethnography from the intelligence community is limited and is normally produced by those with some form of insider status. However, there are still some examples such as Rob Johnston, of the Centre for the Study of Intelligence (CSI), who studied the analytic culture in the US

Intelligence Community (Johnston, 2005). Johnston conducted ethnographic work and interviews with hundreds of analysts across the US intelligence community, including those within military intelligence, the CIA, FBI, NGIA and NSA. The CSI is embedded within the CIA and was established to introspect on the agencies' intelligence functions, so Johnston was well positioned to conduct the study. Bridget Nolan conducted an ethnographic study of the National Counter Terrorism Centre (NCTC) in the US, which involved interviews with and observation of intelligence analysts (Nolan, 2013). Nolan conducted the study whilst working as an intelligence analyst, as part of a graduate fellowship program at the CIA, and acknowledges that this placed her in a unique position to conduct research into the intelligence community.

> External reviews have been non-existent partly because the IC (Intelligence Community) tends to eschew evaluation by outsiders, so any sociological exploration of information sharing and collaboration at NCTC would require a sociologist who was already an insider to the IC (Nolan, 2013, p. 6).

Nicolas Hare and Paul Collinson also focus on the culture of intelligence agencies within their analysis of organisational culture and intelligence analysis within the Defence Intelligence Assessments Staff (DIAS) (Hare & Collinson, 2012). They conducted several interviews with senior managers and considered how factors such as the personality of the analyst affected their work. Hare and Collinson are both Ministry of Defence (MoD) employees, demonstrating the benefits that insider status provides when seeking access to the UK intelligence community. In one example of a non-insider using interviews with the intelligence community, Mandeep Dhami interviewed 22 staff within GCHQ's Joint Threat Research Intelligence Group (JTRIG) and seven other staff from GCHQ who support JTRIG operations (Dhami, 2011). The interviews were conducted in pairs or individually and lasted about an hour. Her report is classified, designed to support GHCQ's work and not meant for public consumption, but was disclosed to the public by Edward Snowden in 2013.

Existing approaches demonstrate that much can be achieved through the collection and analysis of information available within the public domain. However, to address the research gaps and research questions a more comprehensive approach is required.

1.4.2 Methodology

The thesis attempts to address a multifaceted conflict between a range of different actors. The conflict exists on several levels, including the public statements that serve as acts of securitisation, the referent objects each individual actor values, and the actors' own individual interpretations of the threats to these referent objects. Therefore, it is necessary to analyse a range of data from both sides of the conflict, covering public statements, private opinions and individual reactions to perceived threats.

The conflict is fought largely within the public arena, through statements, legal arguments, policies, debates, campaigns and legislation so it can be studied by analysing the large body of publicly available data on surveillance and digital rights discourse. This provides a good understanding of the conflict's origins, causes, and grammars and is in line with existing research into the securitisation of cyberspace. But, whilst this information is extensive it is less effective in helping to explain why the state and DRC securitise cyberspace and how these competing threat constructions lead to conflict. To understand the motivations of the DRC and the state, as well as their fears and personal understanding of the threat, it is necessary to acquire more nuanced information. This can be achieved by conducting interviews with key actors from within the state and the DRC, who can explain what they fear, why they fear it and how they are affected by the actions of the other side.

This thesis frames the dispute between the state and the DRC as a security dilemma, which, at its heart, is an inability of each side to understand the actions and intentions of the other. Whilst this can be mitigated by information sharing, security dilemma theory indicates that it can only be overcome when each side has directly experienced the fears and anxieties of the other. To understand the strategies that can be applied to help overcome this conflict it is therefore helpful to observe and learn from scenarios where actors from each side are exposed to some of the experiences of the other. To acquire this insight, an ethnographic study of surveillance actors is also required.

The following section considers each of the three methods used throughout this thesis:

- open source data collection and analysis;
- interviews;

- an ethnographic study.

1.4.3 Open Source Data Collection

This thesis uses information from a wide range of sources but focusses on several key actors, events and other data, which have been selected for their relevance and prominence in the conflict.

1.4.3.1 Actors

Whilst a variety of actors from across the state and DRC are considered throughout this work, the following represent the key actors.

- GCHQ is the UK's signals intelligence agency and is associated with both digital surveillance and cybersecurity. Alongside the NSA it was the focus of the Snowden leaks and has been prominent in articulating the dangers of encryption. It is also the focus of anger and distrust from the DRC[2].
- Whilst there are several rights organisations within the UK which cover surveillance, the Open Rights Group is the only one which focusses solely on digital rights and freedoms. It contributed significantly to the IPA and positions itself in strong opposition to GCHQ.
- By disclosing thousands of documents from GCHQ and the NSA, Edward Snowden not only kickstarted a new public debate around digital rights and surveillance powers, but he also made himself the central focus of much of that debate. He has been highly critical of GCHQ and remains an inspiration for the DRC.
- The big technology companies, such as Google, Facebook and Apple, play a critical role in the dispute between digital rights and national security. They control technology that can significantly assist or thwart digital rights and

[2] It is important to note that whilst GCHQ's public voice is carefully managed, and it is often viewed as a single entity (see Chapter 7), it is staffed by individuals with a wide range of different views. Likewise, the DRC are comprised of a diverse range of individuals and whilst it is fair to say that the majority of this community mistrust GCHQ, this cannot be said definitively of all. Whilst actors such as the state, GCHQ and the DRC are often treated as singular throughout this work, attempts have also been made to reflect these individual perspectives.

surveillance. Prominent individuals, such as Tim Cook, are often vocal in their opposition to state surveillance.

The following lists the key information sources available to support this thesis.

GCHQ

GCHQ is responsible for both cybersecurity, through the National Cyber Security Centre (NCSC) and intelligence collection. The GCHQ website now provides a large amount of information on policy and how the organisation works. It also provides transcripts of public speeches and a list of press releases. The following are some of the key information sources from GCHQ.

- **Press and Media pages.** Press releases, news articles and events. Transcripts of public speeches made by GCHQ staff.
- **How We Work page:** Background on GCHQ policy, partnerships and oversight.
- **Who we are page:** Information on the staff who work at GCHQ.
- **What we do page:** Information on threats and how GCHQ combats them.
- **Twitter Account:** Commentary on news events.

Open Rights Group

The output from several digital rights organisations is used within this thesis but data collection is focussed primarily on the Open Rights Group. It's web site, Facebook and Twitter accounts provide information on its activities, opinions and perspective. The following are some of the key information sources from the ORG, although, in addition to these sources, ORG representatives also provide quotes to the media and express their opinions through their own social media accounts.

- **Blog**: Blogs by ORG staff, published every few days and including public comments.
- **Press Releases**: Press releases published in response to major news. These are often quoted within news reports.
- **Campaigns Web Page**: Details and updates on major ORG campaigns.
- **Correspondence Page**: A reproduction of all correspondence between ORG and official bodies.
- **Reports and Publications Page**: All reports produced by ORG.
- **Policy Updates Page:** A weekly update with information on all ORG activities.

- **Facebook and Twitter Accounts:** Commentary on news events and user comments.
- **Twitter Account:** Commentary on news events.

Edward Snowden

In addition to the influence of the material he disclosed, Edward Snowden is now an influential actor himself, despite his current exile in Russia. Information on his opinions is available from a range of sources, including the following;

- **Interviews:** Several interviews have been conducted with Snowden since his exile. These include a two-hour question-and-answer session with Guardian readers and reporters and an extensive interview with NBC News.
- **Twitter:** Frequent Twitter statements published by Snowden.
- **Appearances:** Recordings and reports of Snowden's 'appearances' at various events around the world.
- **Other Media:** Several books on Edward Snowden, including Luke Harding's 'The Snowden Files' and 'Glenn Greenwald's 'No Place to Hide'. These provide an insider's view into Snowden and his time in Hong Kong.

Technology Companies

The large technology companies, including Apple, Google and Facebook, are influential within surveillance and digital rights discourse. Through the websites and public statements listed below, they provide a range of information on their policies and opinions.

- **Policy Pages:** Policy information provided by Apple, Google and Facebook through their policy and 'Community Standards' pages.
- **Press Releases:** Press releases related to surveillance and digital rights available through Apple Newsroom, Facebook Newsroom and Google 'Press Corner'.
- **Reform Government Surveillance:** A joint campaign between technology companies, which provides their perspective on surveillance, through a website, twitter account and Facebook page.

1.4.3.2 Events

Several key events have shaped the conflict between digital rights and national security. The government labelled cyber attack as a tier one threat to national security for the first time within the SDSR, NSS and UKCSS and articulated its view

of the cyber threat and the necessary countermeasures against it. The Snowden disclosures focussed international attention on the capabilities and accountability of intelligence agencies and the dispute between Apple and the FBI, in 2016, highlighting the increasingly important role of technology companies in the conflict. The Investigatory Powers Act of 2017 provided the first post-Snowden legislation on surveillance powers and provided a significant focus for both the DRC and the state.

SDSR, NSS and UK CSS

The Strategic Defence and Security Review (SDSR), National Security Strategy (NSS) and UK Cyber Security Strategy established cybersecurity as a key government priority and they provide insight into the government's thought processes around cybersecurity. They provide good examples of the government's securitisation of cyberspace and, as key policy documents, they also set the tone and style of other securitising acts from other government.

- **Published reports of the SDSR, NSS and UK CSS**

Snowden Disclosures

When Snowden took around 50,000 files from the NSA and fled to Hong Kong, he gave access to this data to a select group of journalists and associates. A small percentage of this was released into the public domain and is accessed through the following sources.

- **Snowden Surveillance Archive:** Searchable archive of all documents disclosed by Edward Snowden, which have appeared in the media. Produced by the University of Toronto.
- **Newspapers:** Newspapers with direct access to the Snowden disclosures, including the Guardian, the New York Times, the Washington Post, Der Spiegel, Le Monde, El Mundo and The Intercept.
- **No Place to Hide:** Book by Glenn Greenwald detailing the Snowden disclosures.
- **Snowden Twitter Account:** Commentary by Edward Snowden on surveillance issues and his disclosures.

Apple versus FBI

Information on the dispute between Apple and the FBI over access to the San Bernardino iPhone is widely available in the media. The Electronic Privacy

Information Centre (EPIC) also provides a comprehensive resource, including all court documents from the case. The following are the main sources of legal documents related to the case:

- **Amicus Briefs:** Expert witness statements presented to the court in support of Apple or the FBI.
- **Official Legal Documents:** Initial application by the FBI, Apple's defence and subsequent rebuttals.

Investigatory Powers Act

The IPA was a major focus for the state and DRC during the period of this work. The official IPA website contains versions of the draft and final bill alongside thousands of pages of evidence provided by the DRC and the British state. The following are some of the key information sources on the IPA:

- **Written and Oral Evidence:** 830 pages of transcribed oral evidence and 1532 pages of written evidence, submitted by state institutions, individuals and the DRC.
- **Other Information:** Copies of the draft and final Bills, amendment reports, press notices and briefing papers.

1.4.3.3 Other Data Sources

A wide range of additional data sources are used throughout this thesis including Twitter comments, newspaper reporting, television reports, polling data and a range of websites and blogs. Online search engines are particularly useful for finding the most influential discourse as they provide results weighted towards more popular web pages, which helps to identify the most influential discourse. However, as outlined by Anderson and Kanuka, they are also influenced by the user's location, the websites they have visited and their previous search history (Anderson & Kanuka, 2003). Within this thesis, data from a range of search engines that do not personalise data is combined with data from search engines with personalised search disabled, to try to limit this potential source of bias.

Advanced search features are also used to discover specific information. For example, specific date and regional settings are used to discover popular discourse related to particular events, within particular countries. In addition, the snowball technique is used to discover discourse related to particular issues by chaining information from news reports, social media and public statements. For example,

a submission to the IPB may include a reference to a news report, which is then accessed directly. This report may provide a partial quote from a digital rights activist, which is also accessed directly and may, itself, provide additional material for research.

Other prominent sources of information include the Intelligence and Security Committee, as it provides a repository for information relating to surveillance legislation and activities, the WikiLeaks website, which provides an insight into secret communications between the state and technology companies, and a range of official government sources, which provide the official position of the state.

Intelligence and Security Committee

The Intelligence and Security Committee (ISC) oversees the intelligence and security agencies. It produces reports following major events such as the murder of Lee Rigby, the proposed Investigatory Powers Bill and the Edward Snowden disclosures and makes recommendations to the government. The following are some of the key information sources on the ISC:

- **ISC Reports:** Reports produced by the committee, including several on surveillance powers;
- **Transcripts and Public Evidence**: Oral and written evidence provided to the ISC.

Official Government Sources

The government website and social media pages provide official information including statements and speech transcripts by the Prime Minister and other officials, press releases and policy information. Key elements related to surveillance and digital rights include:

- **Prime Minister's Office:** Speeches and statements by the Prime Minister;
- **Home Office:** Speeches and statements by the Home Secretary;
- **Foreign & Commonwealth Office:** Speeches and statements by the Foreign Secretary.

Wikileaks

Wikileaks provides a leaked archive of emails involving Hillary Clinton's campaign chairman, John Podesta. They expose Clinton's relationship with technology companies and their private views on surveillance and digital rights.

1.4.4 Interviews

Analysis of the discourse helps to provide an understanding of the major storylines within the conflict between the state and the DRC and indicates how these lead to the securitisation of cyberspace and the emergence of the CSD. But this discourse does not provide a comprehensive understanding of the different perspectives of the British state and the DRC and fails to address issues such as how analysts at GCHQ feel about allegations that are made against them. Aside from leaks and reports from private events, cyberspace discourse from the state is heavily controlled and sanitised and tends to conform to pre-determined political positions. Whilst the DRC is generally more willing to share their personal views, they still focus on slogans and pre-determined storylines, which fit their model of communications campaigning. In addition, it is rare for a member of the DRC to be provoked or challenged, which might provide an insight into their feelings, motivations and desires and this leaves a potential gap in understanding.

To address this issue, interviews are conducted with members of the British State and the DRC to provide insight into their feelings, motivations and desires. A semi-structured approach is used to enable the author to pursue interesting lines of enquiry and encourage interviewees to introduce new ideas and topics. ORG staff are used to represent the DRC as it is the only organisations within the UK specifically focussed on digital rights and GCHQ staff are used to represent the British state as they are the UK's predominant state intelligence actors.

1.4.4.1 GCHQ

Due to the sensitivity of GCHQ's work, their public statements are carefully controlled and only media trained senior leadership tend to appear in public. The GCHQ website contains interviews with other GCHQ staff, but these provide only a superficial insight into their individual perspectives (GCHQ, 2016). To understand how and why the state securitises cyberspace and why there is a conflict with the DRC, it is necessary to understand the views, emotions and thought processes of state intelligence actors and a good way to achieve this is to speak to them directly.

GCHQ provided permission for interviews to be conducted with their staff. This may have been assisted by my perceived insider status[3] and the organisation's support for the Royal Holloway Centre for Doctoral Training in Cyber Security (CDT). This

[3] I previously worked with GCHQ as a liaison officer to an MOD agency. See 1.5.3 Ethics for further details.

research is used throughout this thesis and provides additional material that is not accessible within the public discourse. Whilst the Open Rights Group is relatively easy to observe through open events and published recording of its events, GCHQ is much more difficult. Ethnographic work at GCHQ would provide additional information on the practices and experiences of state intelligence actors, but this was not possible to arrange.

To satisfy GCHQ's security requirements, several criteria were established before interviews were conducted. Permission was required from GCHQ before each interview. Interview questions were made available to GCHQ before the interviews and were adapted slightly at their request, although during the interviews, spontaneous follow-up questions were permitted. Interview transcripts were provided to GCHQ following the interviews to ensure that they accurately reflected what was said, although no alterations or omissions were made.

Interviews lasted between one and two hours and were held within GCHQ's headquarters in Cheltenham. The following GCHQ employees were selected, after negotiation with GCHQ over their availability and suitability and were chosen to cover viewpoints relating to policy, communications and analysis. At the request of GCHQ, only their first names are provided below.

- Cyber Policy Advisor (David)
- Head of Cyber Crime (Adrian)
- Head of Communications and Campaign Planning (Matt)
- Head of News (Emily)
- Public Communications and Campaign Planning (Fiona)

The interviews are semi-structured and focus on the topics listed in Table 1.1.

Introduction:	To establish their backgrounds, general views and motivations for working at GCHQ
Cyber Worldview:	To establish their opinions on surveillance and digital rights, including what powers the intelligence community should hold and what restrictions should be placed on them.
Cyberspace Threats:	To establish their opinions on cyberspace threats; where they come from and what they threaten.

GCHQ:	To establish their opinions on GHCQ's purpose, how it seeks to achieve this and what limitations there are on its work
GCHQ's Message:	To establish their opinions on how GCHQ communicates with the public and what challenges it faces in doing so.
Alternative Views:	To establish their opinions on the DRC including why they are thought to oppose GCHQ, how widespread their views are and how this affects GCHQ and its staff.
Use of Language	To establish their opinions on phrases used by the DRC to denigrate GCHQ such as 'Snoopers' Charter' and 'Mass Surveillance'. To establish their opinions on the public use of language by GCHQ staff, such as the former director's claim that social networks were the 'command and control centres of choice' for terrorists.

Table 1.1: GCHQ interview topics

1.4.4.2 Open Rights Group (ORG)

The opinions of the DRC are more easily accessible than those of the British state because there are no security restrictions on their pronouncements and their focus is on communications campaigning and getting their message heard. ORG make extensive use of their website and blog to spread their message and their staff are freely available to talk to at events and meetings. Staff also frequently express their views on social media and news websites and occasionally take part in television interviews. However, whilst ORG frequently comments on the actions and policies of the state, they are rarely questioned on their own policies and motivations. To understand what motivated their policies, how they approach state surveillance and why they use particular language to promote their cause, interviews were conducted with two senior ORG policymakers. ORG director, Jim Killock and Policy Director, Javier Ruiz were selected for interview to cover the viewpoints of those involved in policy making and communication.

Interview questions were made available to ORG before the interviews, although during the interviews spontaneous follow-up questions were permitted. Interview transcripts were provided to ORG following the interviews to ensure that they accurately reflected what was said although no alterations or omissions were

made. Interviews lasted between one and two hours and were held at a public location near to the ORG headquarters.

The interviews are semi-structured and focus on the topics listed in Table 1.2.

Introduction:	To establish their backgrounds, general views and motivations for those involved with ORG
Cyber Worldview:	To establish their opinions on surveillance and digital rights, including what powers the intelligence community should hold and what restrictions should be placed on them
Cyberspace Threats:	To establish their opinions on cyberspace threats; where they come from and what they threaten
ORG:	To establish their opinions on ORG's role, how it seeks to achieve this and what difficulties it experiences
ORG's Message:	To establish their opinions on who ORG targets and how it gets its message across
Alternative Views:	To establish their opinions on the intelligence services, including why they act in the way they do and what might motivate them
Use of Language	To establish their opinions on phrases such as 'Snoopers' Charter' and 'Mass Surveillance', which they often use. To establish their opinions on the public use of language by GCHQ staff, such as the former director's claim that social networks were the 'command and control centres of choice' for terrorists

Table 1.2: Open Rights Group interview topics

1.4.5 Hunted Ethnographic Case Study

The culture of state intelligence actors, the pressures and ethical dilemmas they face and how their attitudes and opinions are affected by exposure to surveillance practices, are all factors that are difficult to study but play a significant role in the conflict. Whilst discourse analysis and interviews provide a good appreciation of the policies, perspectives and approaches of the state and the DRC, they cannot address how actors on both sides would react to exposure to the lives of the other, including their perspectives, their fears and their anxieties.

Participant observation is an extremely useful tool for the study of securitisation as it provides 'an account of the world from the standpoint of "insiders"' (Balzacq, 2011, pp. 44-45). As Balzacq explains, 'participant observation has been especially important to researchers who investigate the "backstage" of securitizaion, that is processes of securitisation that are obscured from the view of outsiders' (Balzacq, 2011, p. 45). This makes participant observation particularly useful to the study of surveillance and state intelligence actors who are, by their nature, obscured from the view of outsiders. As Scott Watson highlights, ethnographic research has been poorly utilised by securitisation scholars and 'there is a need to move away from the sole reliance on content and discourse analysis, towards other approaches, such as ethnographic research that explore how audiences interpret and negotiate securitised representations' (Watson, 2012, p. 299).

Whilst GCHQ provided staff for interview they declined to permit an ethnographic study due to security concerns. However, an alternative opportunity existed in the form of the reality crime show, Hunted. Within the show, several members of the public take on the role of state fugitives and attempt to stay on the run for 28 days. Meanwhile, a collection of current and former police, military and intelligence actors attempt to track them down using the powers of the state. Due to my experience, working for the police and the Royal Air Force, I was able to take part in the show as the lead analyst within the hunter's headquarters, Hunted HQ. Taking part in the show, observing the participants and conducting interviews provides a valuable opportunity to gain insight into the world of state intelligence actors. It also provides a unique opportunity to observe their reaction when they themselves are subject to surveillance, through the mechanics of the show. The insights gained supplement the information gathered through discourse analysis and interviews. More information on the nature of the show is provided in Chapter 7.

Whilst there are some who would argue that reality television shows are an ethnography in themselves, ethnographic studies of reality television shows are rare (Clement, n.d.). Some, for example Deligiaouri and Popovic, study reality television shows by conducting interviews with participants, while others, such as Annette Hill, focus on audience reactions (Deligiaouri & Popovic, 2010; Hill, 2005). This thesis's use of interviews and its observation of Hunted participants is unique as it considers Hunted not as a television show but as an environment where

participants simultaneously perform the role of state intelligence actors, whilst also being monitored and observed by the public.

Whilst Hunted can provide an appreciation of the behaviour and motivations of state intelligence actors, it also provides an opportunity to study how these actors are perceived by the public. There has been some previous research into the influence of entertainment media on the perceptions of the security services, although this has mainly focussed on the police, rather than state intelligence agencies. A poll carried out by Fitzgerald et al revealed that 29% of Londoners derived their knowledge of the police from 'media fiction', with only 20% deriving their knowledge from direct experience (Fitzgerald, et al., 2002, p. 78). It is likely that the percentage who derive their knowledge of the intelligence services from media fiction is even higher given the lack of direct contact most people have with state intelligence actors. Donovan and Klahm reveal that most of the literature on television crime drama focuses on the processes, the nature of the crimes, the ethnicity of the suspects and the nature of the criminal justice system, whilst having 'relatively little to say about the portrayal of police on TV' (Donovan & IV, 2015, p. 1263). Their own study reveals that viewers of crime dramas are more likely to have a positive image of the police and 'are more likely to believe the police are successful at lowering crime' (Donovan & IV, 2015, p. 1261). Whilst low error and misconduct rates in crime dramas might contribute to this positive impression, Donovan et al also highlight the humanisation of police officers including their portrayal as 'passionate and well-intentioned … good guys' (Donovan & IV, 2015, p. 1275).

1.4.5.1 Hunted Ethnography Design

To observe the thoughts and motivations of the state intelligence actors participating in Hunted, I acted as a participant/observer by taking part in the show as lead intelligence analyst within Hunted HQ. This role provided a unique opportunity to conduct an ethnographic study of the show's participants and to experience the practices, emotions and personal experiences of state intelligence actors. Within this role I observed the other participants and the culture of the unit and experienced the pressures, emotions and challenges involved. The study was conducted over 28 days during Series 2 of the show, which was filmed in London. Notes were kept throughout filming and interesting issues were investigated through formal interviews and conversations with the participants. The ethnographic study engaged with the following issues;

- How state intelligence actors conceptualise issues of surveillance and digital rights, whilst conducting work that intrudes on individual privacy.
- How state intelligence actors respond to operating in an environment with far greater transparency than they are accustomed to.
- How exposure to state intelligence actors affects different audiences.
- How state intelligence actors react to becoming surveilled themselves and how this affects their thoughts, feelings and actions.

Listed below are key additional sources of information on the show, which are widely available online, including the episodes, audience reaction and media reporting.

- **Episodes**: Recordings and transcripts[4] of each episode capture the thoughts and actions of the show's participants.
- **Audience Reaction**: Twitter and Facebook postings available through the Twitter account @Hunted_HQ and the hashtag #hunted.
- **Media Reporting:** Articles published in a variety of newspapers and magazines, which include interviews with participants.

1.4.5.2 Hunted Interviews

Whilst episodes of the show and media reporting provide useful information, they do not afford a comprehensive understanding of the views, thoughts and emotions of the participants, particularly with regards to how the show changed or embedded their views. To address this, semi-structured interviews are conducted with the following Hunters and TV producers;

- Peter Bleksley (Chief)
- Ben Owen (Deputy Chief)
- Aisha Ishaq (Intelligence Officer)
- Paul Vlissidis (Head of Cyber)
- Aaron Eccles (Production)

Interviews with the Hunters focus on their experiences and motivations during the show, the impact of being filmed and whether their views changed during the experience. The interview with Aaron Eccles focusses on his expectations for the show and the public's response to it.

[4] https://www.springfieldspringfield.co.uk/episode_scripts.php?tv-show=hunted-uk-2015

The interviews are semi-structured and focus on the topics listed in Tables 1.3 and 1.4.

Hunters

Introduction:	To establish their backgrounds, general views and motivations for taking part in the show
Cyber Worldview:	To establish their opinions on surveillance and digital rights, including what powers the intelligence community should hold and what restrictions should be placed on them
Cyberspace Threats:	To establish their opinions on cyberspace threats; where they come from and what they threaten
Motivation	To establish their motivations whilst taking part in the show
The Other	To capture how they felt about the 'other side' during the show. How the hunters felt about the fugitives.
Post Filming	To establish whether filming the show affected their views on surveillance and digital rights
Post Screening	To establish whether these views changed once the show was broadcast and the participants were able to observe the actions and emotions of the 'other side'.

Table 1.3: Hunter interview topics

Production Staff

Introduction:	To establish their role within the show
Approach:	To establish how they approached issues of surveillance and digital rights within the show.
Engagement	To establish how the producers engaged the audience using the @Hunted_HQ Twitter account.
Reaction	To establish how the audience reacted to the show and the show's use of Twitter to interact with them. To assess how the audience's reaction shifted during the show.
Personal Experience	To establish their personal experience whilst producing the show and if it changed their attitudes towards surveillance and digital rights.

Table 1.4: Production interview topics

Further information on Hunted is provided in Chapter 7.

Data Analysis

To utilise this data, a range of qualitative analytical techniques are considered, including content and discourse analysis.

1.4.5.3 Content Analysis

Content analysis is a research method, which involves the systematic analysis of a range of texts or other communication artefacts to determine their properties. Texts are codified and ordered and then systematically analysed to identify correlations and generate statistics such as word frequencies and associations. Content analysis is increasingly used to measure the success of public relations and the impact of political scandals but is rarely applied to securitisation (Balzacq, 2011, p. 52). Whilst it is a powerful statistical technique, it can only be used to address the language used within a text and does not consider the wider context of that text. As a result, it is not used in this work.

1.4.5.4 Critical Discourse Analysis

Instead of focussing exclusively on the language of a text, discourse analysis also considers its context and other social aspects. Critical Discourse Analysis (CDA) treats discourse as a social practice, considering power relations, ideology and politics, through a critical lens. It is, therefore, a useful tool to help understand why actors have securitised cyberspace, why these acts have been successful and how they are viewed by others. CDA provides a tool to critically analyse the discourse from securitising actors to help understand why they use particular language in certain contexts and why that language leads to successful securitisation or not. CDA is used within this thesis to analyse the most prominent discourse around surveillance and digital rights, from both the British state and the DRC.

1.4.5.5 Intertextual Analysis

There are two methods by which CDA can be applied to the surveillance and digital rights discourse; intratextual analysis and intertextual analysis (Balzacq, 2011, p. 43). Intratextual analysis considers a specific element of discourse and assesses its meaning, intent and performative power. Different texts are then compared based on these characteristics. Intertextual analysis considers the storylines that emerge through the interplay of bodies of texts. Through the repetition of themes, storylines are generated that give overall coherence to a range of discourses. The notion that backdoors are inherently dangerous is an example of a storyline that

has emerged from the body of surveillance and encryption discourse, rather than from one particular text. The securitisation of cyberspace and the conflict between the state and the DRC is reflected in a wide range of securitising acts, conducted by a wide range of securitising actors, which makes it particularly suitable for intertextual analysis. This technique is used throughout the thesis, to determine how different acts and discourses combine to influence the dispute between the British state and the DRC.

The first stage of this intertextual approach is to identify the common storylines that emerge from the digital rights and surveillance discourse. This is achieved through a review of storylines identified by other authors and an analysis of the most common themes within the discourse. After these storylines are established, the discourse is analysed within the context of these storylines. Within Chapter 2, for example, the storylines of hypersecuritisation, technification and everyday security practices, which are identified by Hansen and Nissenbaum, are combined with storylines of darkness, shadows and silence, which were evident within the discourse (Hansen & Nissenbaum, 2009). The discourse is then analysed in relation to these storylines to establish the role they play in the dispute between the British state and the DRC.

1.5 Chapter Structure

This thesis is organised into three parts. Part 1 considers the securitisation of cyberspace. Part 2 considers how this has led to conflict. Part 3 considers existing efforts to resolve this conflict and presents some general principles that could help address the conflict in the future.

Part 1:

This part addresses how cyberspace has been constructed as a threatening space by the DRC and the British state. It utilises the CS's approach to securitisation, whilst also drawing upon other useful adaptions of the theory including Hansen and Nissenbaum's application of Securitisation Theory to cyberspace (Hansen & Nissenbaum, 2009). It considers the two categories of facilitating conditions as laid out by the Copenhagen School; the external, contextual and social conditions, which include the context and power relations between the audiences and the securitising actors and the internal, linguistic-grammatical rules, which include the format and structure of the speech act itself (Barry Buzan, 1998).

Chapter 2 identifies the key securitising actors from within the state and DRC as well as the key audiences that are influenced by securitising acts. It addresses the authority, reach and trustworthiness of each securitising actor, their relationships with the audiences and the degree to which they can convince these audience of their securitising claims.

Chapter 3 identifies the securitising claims made by the DRC and the British state and provides examples of securitising acts that have constructed cyberspace as threatening to digital rights and national security. It considers how the acts' structure, grammars and heuristic artefacts, combine to increase the likelihood that they will be accepted by their audiences.

Part 2:

This part addresses the role of the security dilemma in exacerbating the conflict between the DRC and the British state. It utilises the original conceptions of the security dilemma introduced by Herbert Butterfield and Robert Jervis, as well as drawing on more contemporary interpretations and recent applications of the security dilemma to cyberspace (Butterfield, 1951; Herz, 1950; Jervis, 1978).

Chapter 4 demonstrates how the security dilemma applies to the conflict and how the competing securitisations identified in Part 1 have resulted in a spiralling arms race and a breakdown in trust between the British state and the DRC. It considers how the unique characteristics of cyberspace make it susceptible to the security dilemma and addresses the impact this has had on the conflict.

Part 3:

This part considers strategies for resolving the dispute between the DRC and the British state. It considers how issues can become desecuritised and returned to normal politics and how security dilemmas can be overcome. It also presents a case study from the television show Hunted, which is used to make several observations that could help to solve the conflict.

Chapter 5 considers the negative impacts of the securitisation of cyberspace and the normative dilemma of how to approach the issue. It also considers different approaches to desecuritisation and why these have proven to be so difficult to apply to cyberspace.

Chapter 6 considers some of the factors that exacerbate or mitigate the conflict between the state and the DRC, which has resulted in the CSD. It considers the factors that enable security dilemmas to be overcome and considers how various actors have attempted to overcome the conflict between the British state and the DRC. It considers unilateral attempts to win the conflict and more collaborative approaches. It also considers why these approaches have so far failed

Chapter 7 is a case study using the television show Hunted. It explores some of the findings of the previous chapters through the environment of Hunted, including how exposure to the other and their experiences impacts on sensibility and trust.

The thesis concludes with a summary of how cyberspace has been securitised and how the logics of the security dilemma have created a spiralling conflict between the state and the DRC. It then describes several principles that could be applied to overcome these issues.

1.6 ETHICS

Funding for this thesis was provided by the Engineering and Physical Sciences Research Council (EPSRC). Research was conducted within the EPSRC Centre for Doctoral Training (CDT) in Cyber Security at Royal Holloway, which is supported by the UK government as part of the 2011 Cyber Security Strategy. The author has previously worked within the intelligence community, including a placement at GCHQ, although he was not employed directly by GCHQ itself. GCHQ interviewees were aware of the author's background and whilst this may have encouraged interviewees to provide more open and honest answers, it may also have caused them to make assumptions about the interviewer's opinions and omit information that was assumed to be already known. To mitigate these issues, the interviewees were encouraged to consider the author as an academic rather than a past colleague and the author conducted the interviews to reflect this.

As part of the ethnographic study into the television show, Hunted, the author worked in Hunted HQ as the lead intelligence analyst. The experience could potentially lead to bias towards state intelligence actors and bias against digital rights campaigners. To mitigate this, the author acknowledged this potential source of bias and made sure to maintain neutrality throughout the research.

The author's role could also have impacted on interviews with other participants in the show. He worked closely with the other Hunters who were later interviewed and this relationship helped to establish trust before the interviews. He also worked in opposition to the Fugitives, although never came in direct contact with them during the show. Some of these were later interviewed and these interviews may have been influenced by consideration of the author as part of the rival unit who had been opposed to them. Interviewees may also have been influenced to hide critical opinions of the surveillance efforts used within Hunted so as not to offend the author. To mitigate these issues, interviewees were encouraged to consider the author as an academic and not as a fellow participant on the show. Interviews were conducted away from the TV studios; sufficient time was allowed between the show's filming and the interviews and the author presented questions as an outsider with no insider knowledge of the show.

2 THE SECURITISATION OF CYBERSPACE: POWER RELATIONS

2.1 INTRODUCTION

According to the Copenhagen School, the success or failure of an act of securitisation relies upon the internal characteristics of the act, including the language and its meaning and the external characterises of the act, which are the power relations between the security speaker and the audience. 'To study securitisation' according to the Copenhagen School, 'is to study the power politics of a concept' (Barry Buzan, 1998, p. 32). The power relationship between the security speaker and the audience relies on how audiences judge the authority and trustworthiness of the security speaker.

In cyberspace, there are a range of securitising actors who have differing relationships with different audiences and differing abilities to convince each audience that a referent object is under threat. Digital rights organisations might be trusted by the public but have limited reach, whereas whistle-blowers such as Edward Snowden might have the ability to reach millions but are mistrusted by many. This complex web of relationships helps to determine which acts of cyberspace securitisation are accepted, by whom and why.

This chapter considers the actors involved in the securitisation of cyberspace and their relationship with a variety of audiences. It considers how these power relationships impact on the acceptance or not of securitising acts and demonstrates which actors are most influential with which audiences and why. In doing so, this chapter contributes to a greater understanding of how cyberspace has become securitised.

2.2 AUDIENCES

According to the Copenhagen School, there are four key elements of Securitisation Theory; the referent object, the securitising actor, the threat and the audience. However, as Ole Waever acknowledged in 2014, the role of the audience had not been well explored (Waever, 2014).

> A key concept in securitisation which has received too little attention in the early versions of the theory, but I would today say is the most important, is the audience. Because it's not just a

> matter of threat speak; anyone can stand up and say this or that is a threat. Something happens at the moment when an audience accepts that because of this alleged threat they are willing to accept that we to go to war, keep secrets, shut down this debate, make whatever extraordinary measures we otherwise wouldn't do. So the crucial decision is, in some sense taken by the relevant audience (Waever, 2014).

Thierry Balzacq pays particular attention to the audience, describing it as one of the three faces of securitisation alongside political agency and context. He describes the centrality of the audience as one of the three core assumptions of securitisation theory.

> The success of securitisation is highly contingent upon the securitising actor's ability to identify the audience's feelings, needs and interests. To persuade the audience (e.g. the public), that is, to achieve a perlocutionary effect, the speaker has to tune his/her language to the audience's experience (Balzacq, 2011, p. 9)

The 'empowering audience' is one which has a direct causal link with the issue and which can enable the securitising actor to adopt measures to tackle the threat. A securitising move is successful when the empowering audience accepts the threat and empowers the securitising actor to combat it. The audience can support the securitising actor by both formal and moral means. Formal support is tangible, such as the provision of legal authority via a vote, or the granting of authority through an election, whereas moral support is more abstract, taking the form of general support and solidarity for a cause.

According to Balzacq, to persuade an audience the speaker must resonate with their language.

> An effective persuasion requires that a speaker's argument employ terms that resonate with the hearer's language by speech, gesture, tonality, order, image, attitude, idea, identifying [her/his] ways with [her/his] (Balzacq, 2005, p. 184).

But often, an actor must persuade multiple audiences, each of which is subject to different logics of persuasion. Securitisation can be achieved through a single speech act or it may be necessary to target different acts towards different

audiences. It is therefore necessary to consider the nature of each audience and ask why they might be susceptible to particular logics of persuasion. Opinion within each audience may also differ so it is also necessary to consider the *degree* to which an issue has been securitised by an audience and the *degree* to which this has empowered the securitising actor.

This chapter considers the legislature, who can grant the security and intelligence agencies power and restrict their activities, the public, who can provide informal support or opposition to government policies, and technology companies who provide the government with intelligence data and produce the software and hardware used by most of the public.

2.2.1 The Public

Whilst individual citizens have little influence over the state, collectively they are the largest audience and can influence who forms the government and what their policies are. The public can provide formal support to the government by voting them in or out of office and they can also resist the state by opposing surveillance and utilising technologies that impede the state's ability to conduct it.

The public can support the DRC by engaging with digital rights campaigns, contributing funding and utilising and promoting security technologies such as encryption and Tor, which becomes more secure the more users it has. The public also has significant influence over the other two audiences, the legislature and technology companies. When voting on surveillance legislation, Members of Parliament (MPs) are likely to take into consideration the views of their constituents as well as the public at large. Technology companies also rely on the public to purchase their products and use their services, so a privacy and surveillance policy that is in tune with public demands is desirable.

2.2.2 The Legislature

The legislature establishes the law that governs intelligence and security agencies, technology companies and the public. Whilst the sitting government can propose legislation, majority votes in the House of Commons and House of Lords are required for bills to pass into law. As support or opposition to surveillance legislation often crosses party lines, individual MPs have significant power to determine the scope and scale of surveillance activities in the UK. The legislature also has the power to hold technology companies to account by legislating to govern their activities.

2.2.3 Technology Companies

Whilst technology companies can be considered either securitising actors or threat actors, they can also be viewed as an audience. The technology industry has the power to hinder state surveillance by resisting requests to access customer data, producing transparency reports, designing products to be more resilient to state surveillance, acting as an expert witness against surveillance legislation and providing finance and moral support to the DRC. Conversely, the technology industry can assist the state by complying with state data requests in a timely manner, facilitating state access to customer data, blocking terrorist accounts, removing terrorist material, reporting suspicious activity on their platforms and remaining opaque about how they co-operate with state surveillance activities.

2.3 Securitising Actors and Power Relations

According to the Copenhagen School, the securitising actor is the initiator of the securitising act and utilises particular language to convince the audience of the existence of an existential threat. To achieve this, they must be trusted, be able to reach the audience and have the authority to speak security.

2.3.1 The State

The British government and the security and intelligence agencies are the two main securitising actors within the state and each has different reach, trustworthiness and authority. As the following section demonstrates the government can reach a huge audience but lacks trust and finds it difficult to speak with authority on technical issues. Whereas the intelligence and security agencies carry more authority but have a more limited reach. The role of each as a securitising actor and the power relations between them and the audiences are discussed in the following section.

2.3.1.1 The Government

The British government's ability to communicate on matters of surveillance and privacy is unrivalled amongst the other securitising actors. Statements by the Prime Minister and Home Secretary will invariably make the national news and the Prime Minister's official Twitter account has over five million followers. The government can also spread its message through engagement with the media and technology industry and the production and publication of government policy reports such as the UK Cyber Security Strategy (UK CSS). It has the authority to demand meetings

with large technology companies, such as Facebook and Google, and can also summon senior officials to Parliament (Independent, 2017).

But, despite this platform, the government's ability to speak with authority on issues of surveillance and digital rights is limited by the widespread belief that politicians do not understand modern technology (see Section 3.2.3). Official reports such as the UK CSS carry the gravitas of government, but pronouncements by politicians are less authoritative and often re-enforce views about government ignorance of technology. At a side event, hosted by the Spectator, during the 2017 Conservative Party Conference, Home Secretary Amber Rudd claimed that she didn't need to understand end-to-end encryption to understand that it was helping criminals.

> We will do our best to understand it … I don't need to understand how encryption works to understand how it's helping - end-to-end encryption - the criminals (Rudd, 2017).

Whilst her comments were reportedly met with huge applause from the audience, for many they were evidence that the government simply does not understand how the Internet works (Spectator Events, 2017; The Register, 2017; Open Rights Group, 2017).

The government is unrivalled in its ability to reach a wide audience and it can use the gravitas of public office and the authority of state institutions to support its claims, but its ability to securitise is weakened by doubts over its credibility, especially with regards to highly technical issues such as encryption.

Relationship with the public

Whether government claims on surveillance and terrorism are accepted by the public depends on the degree to which they are trusted. As Jamie Bartlett suggests, 'the online surveillance debate is about whether you trust the government or not – not privacy v security' (Bartlett, 2015; Bartlett, 2015). Trust in the British government has been declining in the last few years. A 2016 Ipsos MORI survey revealed that politicians are the least trusted profession with only 15% of the public claiming to trust them to generally tell the truth; a reduction of 6% since 2015 (IPSOS Mori, 2016). This compares poorly with the most trusted professions such as nurses (93%), doctors (91%) and teachers (88%).

Several factors have contributed to falling levels of trust in the British state, including the conflicts in Iraq and Afghanistan, the expenses scandal and the 2007 financial crash. The war in Afghanistan was supposed to be swift but in 2009, eight years after its start, 106 British personnel were killed and Lieutenant General David Richards admitted that Afghanistan was 'more intense and prolonged than any other conflict in the last 50 years' (BBC News, 2006). Before the invasion of Iraq in 2003, the British government had promised a swift conflict, but on the 23 June 2003 six British soldiers were killed by an angry mob in Basrah and this marked the start of an insurgency in the province which led to the death of 179 UK servicemen (The Telegraph, 2009). Tony Blair and George Bush were widely believed to have lied about their reasons for invading Iraq after the Iraq Survey Group report rejected most of their original claims (Iraq Survey Group, 2004). The Report of the Iraq Inquiry (aka Chilcott Report) also condemned some of Tony Blair's behaviour and indicated that he had committed to the war before the issue had been debated in Parliament (Chilcott, 2016). The heavy casualties, allegations that British troops took part in torture and the lack of significant evidence of WMDs in Iraq vindicated those who had opposed the wars and caused significant damage to the reputation of the British government (The Baha Mousa Public Inquiry, 2011). As a result, opinion on national security and counter-terrorism measures begin to shift with many believing the terms were used to justify authoritarian state powers.

Another event that contributed to falling trust in the British state was the MPs expenses scandal, which revealed that many had abused the system on a massive scale. Eight MP's faced criminal charges and four were jailed. One case which attracted public interest was Sir Peter Viggers' claim for £1600 for a duck house on the pond on his second home. The case came to symbolize the dishonesty, detachment and self-centred nature of MPs and led to a significant drop in trust in the government. The global financial crash of 2007-08 also diminished faith in the government after they failed to predict the crash and then failed to meet their own targets to bring subsequent austerity programmes to an end. Whilst the government can easily reach the public their ability to securitise is constrained by a lack of trust in them.

Relationship with technology companies

The government is keen to attract technology companies to the UK and in 2010 David Cameron vowed to establish the east end of London as a 'world leading technology city to rival the US's Silicon Valley'. This effort has been supported by

subsequent governments making the UK the most desirable location for foreign technology workers in Europe (Cameron, 2010; City AM, 2016; City AM, 2017; YouGov, 2016).

Whilst technology companies generally accept the government's claim that cyberspace can be threatening to national security, they do not accept that this justifies co-operating unquestioningly with the security and intelligence services. As a result, the government has resorted to alternative means to achieve this co-operation, including regulation, the threat of financial penalties, public shaming and diplomatic pressure through the US. Before the general election in 2017, Theresa May threatened to fine social media companies if they did not take down extremist material quickly enough, mirroring a policy that had already been instigated in Germany (Politico, 2017). In January 2015, Prime Minister David Cameron asked the US President, Barrack Obama, to 'step up pressure' on technology companies to ensure they do more to co-operate with intelligence agencies and, on multiple occasions, the government attempted to publicly shame technology companies by accusing them of not doing enough to prevent attacks (Hannigan, 2014; May, 2017; Cameron, 2015).

But a deteriorating relationship has left the government frustrated and the Home Secretary, Amber Rudd, accused the technology industry of 'patronising' and 'sneering' at politicians who try to regulate them (Rudd, 2017). The technology industry has responded to criticism by claiming that the British government 'paints an inaccurate picture' of how much work they do to combat terrorism, but politicians, such as Keith Vaz, have said that with their wealth and power they should be doing more (Vaz, 2016).

Relationship with the legislature

To pass legislation relating to cyberspace and national security the government needs to achieve majority votes in both Houses of Parliament and so must convince the legislature that cyberspace threats are significant enough to justify new legislation. The ability to achieve this relies on several factors, including the size of the government's majority, the existence of a coalition, the authority of the Prime Minister and the amount of goodwill held by the ruling party.

One method that the government can use to influence MPs is to appeal to their fear of being responsible for a terrorist attack. ORG director Jim Killock suggests that the government gains support for surveillance policies by suggesting to MPs

that in the aftermath of an attack they should not want 'to be the minister that didn't provide us with the powers that therefore led us to not knowing [about the threat]' (Killock, 2016)? This is, perhaps, a powerful persuasion technique.

Politics itself plays a significant role in the ability of the government to pass surveillance legislation, as demonstrated by the rhetoric of the Conservative and Labour parties, which switched when there was a change in government. Whilst in opposition, the Conservative Party led by David Cameron fiercely opposed new surveillance powers, accusing the Labour government of 'ignoring warnings' of a 'surveillance society', which had been issued by Information Commissioner Richard Thomas (Grieve & Laing, 2009, p. 3). In a report published on the Conservative website titled 'Reversing the rise of the surveillance state', the Conservatives accused Labour of expanding surveillance powers and overseeing 'a seismic shift in the relationship between the citizen and the state, at the expense of the former' (Grieve & Laing, 2009, p. 4). The report quotes a range of evidence from the DRC including Privacy International, Professor Ross Anderson and Liberty, and promises that a Conservative government will examine 'the current level of protection of the individual against the surveillance state, with a view to strengthening personal privacy in a Bill of Rights' (Grieve & Laing, 2009, p. 11).

In 2010 the Conservatives were elected into Government in coalition with the Liberal Democrats and shortly afterwards proposed the Communications Data Bill, which was designed to increase the power of intelligence agencies. It was defeated when Nick Clegg, withdrew his party's support, claiming it required a 'fundamental rethink' (Clegg, 2012). But in May 2015, after early results indicated that the Conservative Party would be elected into government with an absolute majority, the Home Secretary Theresa May announced that new surveillance legislation would again be a priority.

> We believe that it is necessary to maintain the capabilities for our law enforcement agencies so that they can continue to do the excellent job, day in and day out, of keeping us safe and secure (May, 2015).

Despite receiving an overall majority in the 2015 general election, the government still had to gain the support of Parliament due to opposition to the bill from within their own party. The proposed legislation was initially rejected by MPs after it was heavily criticised by the Intelligence and Security Committee (ISC), but after months

of debate in Parliament and a series of amendments, MPs voted in favour of the bill by a majority of 266 and the Investigatory Powers Bill was enacted on 29 November 2016 (Intelligence and Security Committee of Parliament, 2016).

The legislature is entirely responsible for the passing of new legislation and must, therefore, be convinced by the government that new powers are justified. As a result, they often act as a moderator on surveillance legislation, initially rebuffing government attempts to pass new laws and then finally voting for them once greater safeguards are introduced.

2.3.1.2 The Security and Intelligence Agencies

The security and intelligence agencies are restricted in their ability to communicate their message due to issues of secrecy and national security, but whilst they cannot discuss capabilities or specific investigations, they can talk in general terms about threats to national security and how surveillance powers are used.

GCHQ was originally established during the First World War as the Government Code and Cypher School (GC&CS) and is famous for its role in breaking the German Enigma codes during World War Two. The agency reports to the Foreign Secretary and according to the Intelligence Services Act (1994), which placed the organisation on a legal footing for the first time, GCHQ's focus is on supporting 'the defence and foreign policies or Her Majesty's Government' as well as the 'prevention and detection of serious crime (HM Government, 1994). GCHQ's Twitter feed has around 57,000 followers and public statements by senior figures within the security and intelligence agencies are usually broadcast and published by the media. Whilst MPs are frequently accused of not understanding modern technology, the same cannot be said of GCHQ because the case against modern surveillance partially relies on the argument that GCHQ and NSA's surveillance capabilities are so sophisticated that they pose a substantial threat to individual privacy. Intelligence officials such as GCHQ director Jeremy Fleming are much more able than the government to speak with authority on issues of encryption and surveillance, even if they might not be trusted to use surveillance powers for the public good.

Relationship with the public

Whilst polling suggests that only 15% of the public trust politicians to generally tell the truth, 71% still trust the police, more than the clergy (69%), news readers (67%) and the ordinary man/woman in the street (65%) (IPSOS Mori, 2016). But the public appears to be more suspicious of the intelligence agencies. When asked whether

the public trusted GCHQ not to abuse their capability to intercept the internet-based communication of every British citizen if they had the resources and capability to do so, 42% said Yes compared to 52% who said no (YouGov, 2015).

Whilst the British Intelligence Agencies have historically been trusted by the British public, several recent events may have diminished that trust. Having operated largely behind the scenes for decades, the public's perception of the intelligence agencies has changed since the 2011 attacks in New York due to their increased prominence in the 'War on Terror'. The securitization of terrorism following 9/11 resulted in huge increases to the budgets and remits of intelligence agencies, but they have also been accused of failing to prevent attacks, being complicit in torture, providing misleading intelligence on WMD in Iraq and committing unnecessary intrusions into individual privacy.

In September 2002, the government published a dossier titled 'Iraq's Weapons of Mass Destruction: The Assessment of the British Government'. The report claimed that Iraq was developing chemical and biological weapons and attempting to reconstitute its nuclear program. The report, which was billed by many as the 'dodgy dossier', was much maligned at the time and was later proven to be largely incorrect. Large parts of the dossier were also confirmed to have been plagiarised from a student's thesis. The Chilcot report said that the intelligence community had worked from the start on the misguided assumption that Saddam had WMDs and did not consider the possibility that he had destroyed them (Chilcott, 2016). It also reported that the 'overstated firmness of the evidence' for WMD had produced a 'damaging legacy, including undermining trust and confidence in Government statements, particularly those which rely on intelligence which cannot be independently verified' (Chilcott, 2016, p. Executive Summary p131).

The 2005 London bombings and their aftermath also damaged faith in the intelligence agencies. An ISC report into the attacks revealed that two of the perpetrators had previously been under surveillance by MI5 and this led to questions about MI5's competence (Intelligence and Security Committee, 2009). Two weeks after the London bombings, an additional attempt was made to attack the London transport system, which led to the mistaken police shooting of Jean Charles de Menezes. An inquest into the incident returned an open verdict, but protests were staged against the Metropolitan Police and many saw the incident as an example of an overzealous counter-terrorism strategy and poor police surveillance and intelligence gathering procedures (Vaughan-Williams, 2007).

The reputation of the intelligence agencies was also damaged by allegations of their involvement in torture during the 'war on terror'. At Guantanamo Bay, UK Intelligence officials were accused of complicity in torture and turning a blind eye by leaving a room when torture was about to take place (Blakeley & Raphael, 2016). Polling by YouGov revealed that 64% of the public believed that the British intelligence agencies had been involved in torture, although 34% said that there were circumstances where torture was necessary and 47% said that there were circumstances where using information obtained through torture was justified (YouGov, 2014).

Trust in GCHQ, was also damaged by the Snowden disclosures and subsequent legal judgements against them. In December 2014, the Investigatory Powers Tribunal ruled that the PRISM and Upstream intelligence sharing agreements between the UK and US did not comply with human rights laws because rules and safeguards designed to protect privacy had been kept secret (The Investigatory Powers Tribunal, 2014). The ruling did not claim that the programmes themselves were illegal. Once the rules governing the programmes were published they became compliant with human rights law but the case was damaging to GCHQ's reputation. A more serious breach was revealed in 2016 when the Investigatory Powers Tribunal ruled that GCHQ had unlawfully collected data for 17 years. The tribunal revealed that GCHQ's bulk data collection 'failed to comply with article 8' of the European convention on human rights (Investigatory Powers Tribunal, 2016).

Whilst the Security and Intelligence agencies can speak with authority on issues of terrorism and are far better placed than the government to speak on technical issues such as surveillance, the Snowden disclosures and subsequent legal rulings against GCHQ have damaged public trust. The securitising claim that GCHQ's ability to monitor crime and terrorism online is diminished due to encryption and other security measures is particularly difficult to uphold, given the widespread public belief that GCHQ already has overwhelming powers (YouGov, 2013).

The government, police and intelligence agencies have an unparalleled ability to speak to the British public. Whilst the government often lack the authority to speak on technical issues, this is mitigated by the expertise of GCHQ. However, several incidents including the 'dodgy dossier', the expenses scandal and the Snowden disclosures have had a significant impact on trust in the state and its institutions, which has lessened the impact of the state's securitising claims on cyberspace.

Relationship with technology companies

The intelligence agencies and technology companies such as Google and Facebook have many similarities and are in competition for the same valuable resource of information. Facebook and Google collect and exploit information on their users for profit, whilst GCHQ use the information they gather to protect national security. Like the security and intelligence agencies, technology companies are also accused of threatening digital rights by creating panoptic platforms that allow them to observe the public without their knowledge (Fast, 2015; Mitrou, et al., 2014; Bruno, 2014).

This common desire to master information is demonstrated by similar investments that are made by the intelligence agencies and the technology industry. For example, the US intelligence's agencies investment arm 'In-Q-Tel' and Google both invested heavily in the intelligence start-up 'Recorded Future', the intelligence analysis platform Palantir was founded by Facebook Board member and initial funder Peter Thiel, and Keyhole, the precursor to Google Earth, was also funded by 'In-Q-Tel' (Fast Company, 2013; Wired, 2010). There has also been a great deal of cooperation between the intelligence agencies and technology companies. In the UK, telecoms companies including BT and Vodaphone allowed GCHQ to tap their fibre optic cables, whilst in the US, Microsoft has partnered with the New York Police Department to create a real-time monitoring system that combines intelligence on criminals and terrorists with CCTV and automatic number plate recognition (Fast Company, 2012; *The Guardian*, 2013). Privacy Advocate Mark Weinstein claims that it is this competition that leads technology companies to oppose state surveillance rather than any actual concerns for digital rights (Weinstein, 2014).

> These companies are not railing against the government for data mining. It's their go-to moneymaker. What they're fighting against is someone else doing it using their sites. They want to be Top Dog, left alone to secretly conduct business as usual without regulations or intervention. Handing over their treasure trove of information to the government makes them pawns. Holding onto that information for themselves makes them capitalist kings (Weinstein, 2014).

The relationship between the security and intelligence agencies and technology companies was damaged by the Snowden disclosures, which revealed the extent to

which they had been subverted and infiltrated by GCHQ and the NSA (*The Guardian*, 2013). Despite previous allegations of collusion between technology firms and the intelligence agencies, the Snowden disclosures showed that GCHQ and the NSA were intercepting data from companies without their knowledge through programs such as 'Muscular', which gave GCHQ and the NSA ability to intercept unencrypted data when in transit between Google data centres (*Washington Post*, 2013; Cryptome, 2000). The technology companies reacted angrily to these revelations, which is demonstrated by a Google Engineer's blog post, which he wrote in response to NSA slides that explained how they compromised Google's system.

> A giant Fuck You to the people who made these slides. I am not American, I am a Brit, but it's no different - GCHQ turns out to be even worse than the NSA. We designed this system to keep criminals out. There's no ambiguity here … In the absence of working law enforcement, we therefore do what internet engineers have always done - build more secure software. The traffic shown in the slides below is now all encrypted and the work the NSA/GCHQ staff did on understanding it, ruined (Hearn, 2013).

In response, Google, Microsoft and Yahoo all announced that they would now encrypt traffic between their data centres and in a blog post Microsoft claimed 'that snooping potentially now constitutes an "advanced persistent threat'',' effectively comparing NSA and GCHQ surveillance with sophisticated state-sponsored cyber attacks from China and Russia (Microsoft, 2013; Tech Crunch, 2013).

In some cases, technology companies went beyond boosting their security and took measures to deny the government, even whilst providing the same data to commercial organisations. In 2017, Twitter blocked any companies who supported law enforcement from accessing their data feeds, explaining that they did not want Twitter to be involved in surveillance (The Telegraph, 2017).

> We prohibit developers using the Public APIs and Gnip data products from allowing law enforcement — or any other entity — to use Twitter data for surveillance purposes. Period (Twitter, 2016).

The intelligence agencies and technology companies are in competition for access to the same data, but prior to the Snowden disclosures, the relationship survived through mutual interest and secrecy. However, the power of technology companies

has grown, and following the Snowden disclosures, they have demonstrated their unwillingness to submit to the demands of the intelligence community.

Relationship with the legislature

The intelligence agencies do have significant influence over MPs, reporting directly to the Home and Foreign Secretaries and sitting on the Cabinet Office Briefing Room (COBR) when necessary. When a new Prime Minister is appointed, one of their first briefings is on security and defence. Opposition leaders and shadow cabinet ministers also get briefed by intelligence and security chiefs on issues relating to national security threats (Huffington Post, 2015).

Intelligence agency bosses also make public appeals to MPs for new powers to combat threats to national security. Between the first and second readings of the Investigatory Powers Act, Robert Hannigan, the Director of GCHQ made a speech that raised the severity of threats to national security and claimed that MP's had a responsibility to provide GCHQ with the powers to deal with these threats.

> It is not for me, as an intelligence official and civil servant, or for a law enforcement officer, to make these broad judgements, whether about the use of data in general or encryption in particular; nor is it for tech company colleagues nor even for independent academics … it must surely be for elected representatives to decide the parameters of what is acceptable (Hannigan, 2016).

Parliament does have the ability to scrutinise the activities of the intelligence agencies through either the Home Affairs Select Committee or the Intelligence and Security Committee (ISC), which publicly questioned the heads of the three major intelligence agencies for the first time in November 2013 (The Guardian, 2013). But there are also allegations that the intelligence agencies have abused their relationship with MPs. An investigation by Computer Weekly alleged that GCHQ was routinely accessing the content of MP's private emails and former Cabinet Minister Chris Huhme who had sat on the National Security Council (NSC) claimed that GCHQ had misled ministers by failing to inform them about programmes such as Tempora and Prism, before they were revealed by Edward Snowden (Huhne, 2013; Campbell & Goodwin, 2016).

2.3.2 Digital Rights Community

The DRC is comprised of a wide range of actors, but the main influencers can be broken down into four key categories: rights organisations, technical experts, whistle-blowers and the technology industry. Rights organisations such as Open Rights Group (ORG) are the most consistent opponents of state surveillance, although they have difficulty reaching and convincing a large audience. Technology experts and academia add authority to the cause but also have limited reach. Whistle-blowers, such as Edward Snowden, have been able to raise digital rights issues to a wide audience and technology companies such as Apple are also becoming particularly vocal on the issue.

Without the gravitas of the state to provide them with reach and authority, the DRC relies significantly on individuals to make their case. Security experts such as Whitfield Diffie and Martin Hellman, whistle-blowers such as Edward Snowden and William Binney and technology executives such as Tim Cook are lauded by the DRC as heroes (Sell, 2016; Chakrabarti, 2015). An 'Access Now' awards ceremony honours the year's digital rights heroes, as well as castigating the alleged villains (Access Now, 2016).

2.3.2.1 Technical Experts and Academia

The DRC's case is strengthened by the support of a wide range of technical experts from academia and the technology industry, who bring credibility to the argument for digital rights. The security and privacy literature is dominated by criticisms of state surveillance, which can be broadly divided into social scientists and international relations scholars who criticise the ethics and negative outcomes of state surveillance and information security specialists who criticise efforts by the state to weaken encryption and hoard zero-day vulnerabilities (Cavelty, 2014; Taylor, 2002; Lyon, 2014; Bigo, et al., 2014; Paterson, et al., 2015). Some scholars, such as Raphael Bossong, argue that 'academics should challenge the prevalent securitising discourses and ideas' of surveillance and academic institutions, such as Citizen Lab, have been established specifically to advocate for digital rights and to investigate digital espionage against civil society (Citizen Lab, 2018; Bossong, 2008, p. 24).

Security experts are considered technical experts who can comment impartially on issues of surveillance and digital rights and their research is often used by digital rights organisations such as Electronic Frontier Foundation (EFF) to add weight to

their arguments (Electronic Frontier Foundation, n.d.). Academic experts are also called upon to provide expert commentary on cybersecurity news stories and they have also been active in making the case for digital rights by contributing submissions to consultations on legislation (Parliament.uk, 2016). When several academics wrote open letters to the US government criticising state surveillance, the EFF boasted that 'academics have joined the fight against mass surveillance' (Electronic Frontier Foundation, 2014).

> The fight to bring the surveillance programs of governments around the world within the bounds of human rights law is an international effort, and we are heartened to see that academics have embraced this global strategy (Electronic Frontier Foundation, 2014).

Whilst academics and other technical experts carry authority and are widely considered trustworthy, their reach is more limited than other securitising actors and they often play a more supporting role within the DRC. To address this, academics often group together to write letters and express their collective opinions, which allows them to have a greater impact on the news agenda (US Researchers, 2014; US Researchers in Cryptography and Information Security, 2014; Pateron, et al., 2013; InfoSecurity Group, 2014; The Guardian, 2015; Bernal, 2014; Wray, 2015).

The role of experts as securitising actors is critical as they carry authority and provide trustworthiness for the DRC's cause and, as Hansen and Nissenbaum explain, cybersecurity experts have achieved a greater ability to speak to the public than in other fields.

> In the case of cybersecurity, experts have been capable of defying Huysmans (2006:9) description of the invisible role of most security experts as they have transcended their specific scientific locations to speak to the broader public in a move that is both facilitated by and works to support cyber securitizations claimed by politicians and the media *(Huysmans, 2006, p. 9; Hansen & Nissenbaum, 2009, p. 1167)*.

Relationship with the public

According to the 2017 Edelman Trust Barometer, academic experts are the most trusted category of 'spokesperson', with 60% of the public believing them to be

extremely credible or very credible, followed by technical experts at 59% (Edelman, 2017). Whilst trust was less than in 2016 (66% each), it is still twice the number who trust government officials (30%) and demonstrates the importance of technical and academic expertise to the securitisation of cyberspace. Whilst experts hold a wide range of different positions, for the DRC they can provide the science and expertise to back-up the securitising claims of whistle-blowers such as Edward Snowden and NGOs such as ORG.

Relationship with technology companies

Technology experts, academia and technology companies often conduct research in similar areas and have a close and symbiotic relationship. Experts need data from technology companies to help their research and implement their security findings, and technology companies need research to improve their security offerings and stay ahead of the competition. During Apple's conflict with the FBI, there were 18 amicus (expert witness) submissions in support of Apple. These included a submission by 32 law professors, a submission by the EFF and 46 'technologists, researchers and cryptographers', and a submission from security experts including Bruce Schneier (Electronic Privacy Information Centre, 2016; Zovi, et al., 2016). This contrasts with just four amicus submissions in support of the FBI, with a submission from the families of victims of the San Bernardino shootings representing the only non-official source.

Expert support for Apple also seems to have influenced the ideology of its CEO, Tim Cook. In an interview with Time Magazine, Cook appeared to echo the words of the Berkman Centre, who had recently published a report into the 'Going Dark' problem, suggesting that the amount of information available to law enforcement was greater than ever (The Berkman Centre, 2016)

> We shouldn't all be fixated just on what's not available. We should take a step back and look at the total that's available, because there's a mountain of information about us (Cook, 2016).

The relationship between technical experts and the technology industry allows experts to influence the views and direction of the industry, usually in a direction away from surveillance and towards greater digital rights.

Relationship with the legislature

Technical experts and academia are an essential element of the legal process and their input can influence legislation or even stop it from passing. An open letter by

academic experts helped to support the case against DRIPA and a wide range of technical experts also provided evidence to the IPB consultation, including Professor Ross Anderson of the University of Cambridge, Mark Ryan, professor of computer science at the University of Birmingham and Paul Bernal, lecturer in information technology, intellectual property and media law at the University of East Anglia School of Law (Parliament.uk, 2016; Bernal, 2014).

Prior to the IPA, Nick Clegg commissioned the Royal United Services Institute to establish a Surveillance Review Panel to consider surveillance practices and David Cameron commissioned *The Independent* reviewer of terror to investigate surveillance legislation (Anderson, 2015; Royal United Services Institute, 2015; Intelligence and Security Committee of Parliament, 2015). Each report was researched and written by independent academics and technical experts and was highly influential in the formulation of the IPA, demonstrating the influence of technical and academic expertise.

2.3.2.2 Whistle-blowers

Whistle-blowers have had a significant influence on the securitisation of cyberspace because they generate extensive news headlines, carry authority due to their insider view of the organisations they are exposing, and are often granted mythic status amongst the DRC because of their personal sacrifice. Several whistle-blowers have exposed classified information about GCHQ and the NSA, including Katherine Gunn (GCHQ) and William Binney (NSA), but by far the most influential is Edward Snowden. Labelling Snowden a whistle-blower is contentious as many believe that he acted illegally by exposing classified intelligence, disproportionately because he leaked thousands of documents, and unethically because he assisted the enemies of the UK and US and damaged the national security of both (Kaplan, 2017).

What is certain is that Snowden's opinions on surveillance and privacy have reached a huge audience around the world. When his disclosures were first published by the Guardian Newspaper and New York Post, they made headlines around the world for weeks and were often front-page news in British newspapers. The magnitude of the disclosures, the revelation of their content and the intrigue of his escape to Hong Kong and exile in Russia kept the story alive, and Snowden became a household name.

Despite his exile in Russia, Snowden established a Twitter account with over three million followers, which he uses to criticise UK and US surveillance policies. He also

regularly attends talks and conferences around the world using a BeamPro 'telepresence robot' that acts as a video conferencing device and can be driven around a stage remotely. His first use of the system was to deliver a talk to the TED conference in 2014 titled 'Here's how we take back the Internet', which has over four million views on the TED website (TED, 2014).

Snowden is also able to speak directly to key security advocates, technology experts and academics. In what was reported as a 'call to arms' to tech companies, Snowden appeared by video conference at SXSW 2015 to a private audience of technology and policy experts, including Twitter's senior product counsel and Evernote's CEO (Verge, 2015). Snowden urged them to foil government surveillance by implementing better security technologies such as end-to-end encryption (The Verge, 2015). Snowden has also featured in several books including Glen Greenwald's 'No Place to Hide', 'The Snowden Files' and 'Snowden' by Kieran Fitzgerald. In 2016 Oliver Stone directed the film, 'Snowden' which focussed on his whistleblowing. Snowden is backed by several organisations such as the Courage Foundation and has received celebrity endorsement from individuals such as Russell Brand and Vivienne Westwood, who along with other celebrities signed a joint statement vowing to 'stand in support of those fearless whistle-blowers and publishers who risk their lives and careers to stand up for truth and justice' (The Guardian, 2014).

Whilst Snowden is physically exiled in Russia, one main advantage he has over GCHQ and the NSA is his ability to speak openly about intelligence matters, whereas GCHQ and the NSA are restricted in their ability to discuss surveillance capabilities due to the need to keep state secrets. Asked about how they get their message across to the public, the Head of Communications and Planning at GCHQ showed his frustration that GCHQ is unable to tell their side of the story.

> This is relatively new for us so because it's new there are different opinions about the extent to which we should be open. We have one arm tied behind our back because we can't talk about specific cases (Matt, 2016).

Alongside his ability to reach a huge audience, Edward Snowden also carries substantial authority given his previous role within the NSA and his position as an insider to state surveillance, which gave him access to state secrets. Compared to digital rights organisations who criticise state surveillance from the outside,

Snowden was on the inside of the world's most powerful signals intelligence agency and can claim to understand the threat they pose to digital rights. He frequently uses this experience when making his case against the NSA.

> You could watch entire villages and see what everyone was doing. I watched NSA tracking people's Internet activities as they typed. I became aware of just how invasive U.S. surveillance capabilities had become. I realized the true breadth of this system. And almost nobody knew it was happening (Greenwald, 2014, p. 43).

But there is some disagreement about exactly what responsibilities Snowden held at the NSA and how senior he was. His supporters claim he was a talented and high-level analyst with direct access to an understanding of advanced surveillance capabilities, but his detractors claim he was a systems administrator. An internal NSA memo claimed that he gained access to some documents by tricking his colleagues into sharing their passwords (Reuters, 2014). Oliver Stone's movie, Snowden, reflected the view of many Snowden supporters that he was an exceptionally gifted systems administrator who was handpicked by the deputy director of the NSA to be a high-level analyst and chosen to work on a special project, but when author and journalist Fred Kaplin contacted Chris Inglis, the Deputy Director at the time, he vehemently denied this claim.

> The claim is simply and utterly preposterous—both the claim that a Deputy Director would assign such a task to a low-level contractor (that just does not happen for many many reasons) and the idea that Snowden was working on some special project, separate and apart from his contracted duties to perform system administration and SharePoint server updates (Kaplan, 2017).

Whilst the NSA repeatedly refers to Snowden as a systems administrator, Snowden himself denies the claim, insisting that he was a spy because he had previously worked undercover.

> I was trained as a spy in sort of the traditional sense of the word -- in that I lived and worked undercover, overseas, pretending to work in a job that I'm not -- and even being assigned a name that was not mine … when they say I'm a low-level systems administrator, that I don't know what I'm talking about, I'd say it's somewhat misleading (Snowden, 2014).

Much of this disagreement may lie in the semantics of what it is to be a spy but reflects the differing degrees to which Snowden is trusted by different audiences.

Relationship with the public

To some, Edward Snowden is considered a hero, who made great personal sacrifices to expose wrongdoing, but to others he is a traitor, who betrayed his country and exposed its most important secrets to everyone, including its greatest enemies. Academic literature demonstrates the polarisation of views and several studies have considered the framing of Snowden as a hero or a traitor in the media and the wider world (Caster, 2016; Salvo, 2016; Qin, 2015; Branum & Charteris-Black, 2015; McLoud, 2015; Moretti, 2015). Whilst each considers how Snowden's reputation differs across countries, media type and ideological bias, each agrees that Snowden is portrayed and viewed as either inherently good or inherently bad; a hero or a traitor.

Snowden himself has repeatedly rejected the notion that he sees himself as a hero or a traitor, but instead claims to be an ordinary American citizen.

> I don't see myself as a hero because what I'm doing is self-interested (Snowden, 2013)
>
> If I had to describe myself, I wouldn't use words like 'hero.' I wouldn't use 'patriot,' and I wouldn't use 'traitor.' I'd say I'm an American and I'm a citizen, just like everyone else (Snowden, 2014).

However, many of Snowden's pronouncement use the language of martyrdom, focussing on the justness of his cause, the pre-eminence of his cause, his self-sacrifice and his persecution. These are visualised in table 2.1.

Claim	Quote
Justness of the cause	My sole motive is to inform the public as to that which is done in their name and that which is done against them (Snowden, 2013).
	The reality is, the situation determined that this needed to be told to the public. The Constitution of the United States had been violated on a massive scale (Snowden, 2014).

	I didn't want to change society. I wanted to give society a chance to determine if it should change itself (Snowden, 2013).
Pre-eminence of the cause	What happens to me is not as important; I simply serve as the mechanism of disclosure (Snowden, 2016).
	I care more about the country than what happens to me (Snowden, 2014).
	I may have lost my ability to travel, but I've gained the ability to go to sleep at night and to put my head on the pillow and feel comfortable that I've done the right thing even when it was the hard thing (Snowden, 2014).
Personal Sacrifice	I could not do this without accepting the risk of prison. You can't come up against the world's most powerful intelligence agencies and not accept the risk (Snowden, 2013) .
	I do not expect to see home again, though that is what I want (Snowden, 2013).
	I think it's important to remember that people don't set their lives on fire. They don't walk away from their extraordinarily, extraordinarily comfortable lives ... for no reason (Snowden, 2014).
Persecution	I have been made stateless and hounded for my act of political expression (Snowden, 2013).
	I understand that I will be made to suffer for my actions (Snowden, 2013).

Table 2.1: Snowden's language of martyrdom

To defend himself against charges of criminality and accusations of treachery to the US, Snowden has also argued that his actions were conducted in the best interests of the country, the government and the NSA, even if they didn't know it.

> Sometimes to do the right thing, you have to break a law (Snowden, 2014).

> I am not trying to bring down the NSA, I am working to improve the NSA. I am still working for the NSA right now. They are the only ones who don't realize it (Snowden, 2013).
>
> I don't want to harm my government. I want to help my government (Snowden, 2014).

Snowden's self-portrayal as a martyr is a view shared by many in the UK and throughout the world, and opinion polls show that his actions were supported by around 40-55% of the UK population, whilst only 25%-35% opposed them (Cable, 2015). For some, Snowden has become a cult figure and is viewed in the same light as revolutionary leaders such as Che Guevara. Foreignpolicy.com report how the production of t-shirts, coffee mugs and posters portraying his image demonstrate

Figure 2.1: The Guardian - 'A fitting poster hero for our times'

Figure 2.2: 'Prison Ship Martyrs' war memorial

that Snowden has 'officially joined the pantheon of leftist icons-turned unwitting money makers' and *The Guardian* described him as 'a fitting poster hero for our times' (Foreign Policy, 2013; Jones, 2013) (see Figure 2.1).

In America, Snowden supporters installed a Snowden bust (see Figure 2.2) at the 'Prison Ship Martyrs' War memorial[5], Snowden fan-pages have been established[6] and marches and campaigns have been organised in his name.[7] In the last months of the Obama administration, Snowden made the case for a presidential pardon, arguing that his actions had left America better off, but despite support from Amnesty International and the American Civil Liberties Association, President Obama refused to commute his sentence as he had done for fellow leaker Chelsea Manning (The Guardian, 2016).

Not only does Snowden appear to have made huge personal sacrifices to expose wrongdoing, but his claims against the government were made at a time when trust in the establishment was falling. However, there is also a large amount of suspicion about his motives and whether he did the right thing. This is reflected in the finding of the official US House of Representatives report on the disclosures, which concluded the following (US House of Representatives, 2016, p. i);

1.) Most disclosures did not relate to privacy issues.
2.) Snowden had lied when he said he had checked all documents to ensure they did not harm national security, something which he later admitted.
3.) Snowden had previously been disciplined for his behaviour at work.
4.) Snowden had contact with the Russian Intelligence Services.
5.) Snowden is a 'serial exaggerator and fabricator'.

Snowden was also heavily criticised in a book by Edward Lucas who claims to have dismantled Snowden's claim to want to expose wrongdoing and argues that he deliberately set out to damage the NSA (Lucas, 2014). Lucas also claims that the damage done to western security, diplomacy and western interests far outweighs any benefits from the disclosures.

But whilst many view Snowden's actions as illegal and disproportionate, he has had a major impact on the debate over state surveillance. Due to a loss of trust in the establishment, whistle-blowers are now considered a more trustworthy source of

[5] http://animalnewyork.com/2015/theres-a-massive-illicit-bust-of-edward-snowden-stuck-to-a-war-monument-in-brooklyn/

[6] E.g. https://edwardsnowden.com/, https://cms.fightforthefuture.org/snowden/

[7] https://www.theguardian.com/world/2013/oct/26/nsa-rally-stop-watching-washington-snowden, https://pardonsnowden.org/

information. Worldwide, almost twice as many people believe leaked information to be more trustworthy than official press statements (Edelman, 2017). In a 2015 survey, 30% of respondents said that following the Snowden disclosures they had taken at least one step to shield their information from the government, 15% use social media less often and 13% avoid certain terms in online communications (Pew Research Centre, 2015). Despite his exile in Russia, Snowden is still able to reach significant numbers of people and to many, his views and warnings are credible and authoritative.

Relationship with technology companies

Snowden has stated that he intends to focus his efforts on technical rather than political reform of state surveillance because he sees this as a more universal and long-lasting solution to the problem (Snowden, 2014). To achieve this, he needs technology companies to implement strong security measures, resist government attempts to access user data and expose government data requests.

In the aftermath of the Snowden disclosures, the technology companies were fighting to save their reputations after allegations that they had colluded with the NSA over PRISM and other surveillance programs. Initial disclosures indicated that the NSA could collect data 'directly from the servers of … Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple' and this data was also shared with GCHQ (*Washington Post*, 2013). According to Viktor Mayer-Schonberger, professor of internet governance and regulation at the Oxford Internet Institute, this claim caused a substantial backlash against technology companies, who rely on public trust.

> These companies depend on their users being sufficiently trusting to give them personal data. Many of us are perfectly fine for these companies to use this information for their own commercial benefit, to place more relevant adverts on the right-hand side, but we do not want it passed on to the government or to tax authorities for instance (Mayer-Schonberger, 2013).

In response to Snowden's disclosures, civil rights organisations such as the Centre for Democracy and Technology suggested that technology companies would have to pressurise the state if they wanted to re-establish trust.

> An important step would be for these companies to exert even more pressure; pressure on the intelligence authorities to disclose

> more information about intelligence related surveillance that they are compelled to conduct (Nojeim, 2013).

Due to his status as an exile, the large technology companies have not made substantial comments on Snowden's actions, although Apple's Tim Cook has noted that Snowden got technology companies to talk more about the issue of privacy and surveillance (Cook, 2015). However, since the disclosures, they have been extremely vocal in their criticism of state surveillance and have radically changed how they implement security and interact with the government and intelligence agencies. Google said that they were 'outraged' by the revelations and Apple's Tim Cook said that he 'abhorred' people's information being 'trafficked around' (Cook, 2015; Google, 2013).

Technology companies also made substantial efforts to improve the security of their networks and demonstrate that they are not subservient to NSA and law enforcement. By December 2013, Google, Microsoft and Yahoo had implemented encryption between their data centres to thwart NSA access, by March 2014 Apple, Facebook and others were notifying users of secret data requests against them, and over the next few years several companies implemented end-to-end encryption on their messaging platforms, ensuring that access would be made difficult or even possible for the government (Tech Crunch, 2013; *Washington Post*, 2014; WhatsApp, 2016). The DRC have hailed the change in the stance of technology companies and Snowden supporters such as Glen Greenwald claim that they are now 'petrified' to be seen as NSA collaborators (Greenwald, 2016).

> These companies are now engaged in a genuine commitment to demonstrate that they're willing to protect privacy even against the U.S. government. That has really altered the relationship between the U.S. government and these tech companies, and made it much, much harder to spy (Greenwald, 2016).

Tim Cook, in particular, has been highly critical of state surveillance and won praise from Edward Snowden for his stance against the FBI (Snowden, 2015). After the Syed Farook case, Harmit Kambo of Privacy International claimed that 'Tim Cook has shown himself to be an important privacy advocate, just as Edward Snowden has', and Alex Webb and Selina Wang of Bloomberg claimed that Cook was 'picking up where Snowden left off' (Webb & Wang, 2016). Commenting on Cook's stance, Snowden highlighted the fact that Apple's business model is more conducive to

privacy than rivals such as Google and Facebook and suggested that this was good for the public.

> He's obviously got a commercial incentive to differentiate himself from competitors like Google. But if he does that, if he directs Apple's business model to be different, to say "we're not in the business of collecting and selling information. We're in the business of creating and selling devices that are superior", then that's a good thing for privacy. That's a good thing for customers (Snowden, 2015).

Whilst a cynic could argue that Apple's stance in support of privacy is motivated by a desire to seek commercial advantage, there is no doubt that in Tim Cook Snowden has a critical ally who has the power to make a significant difference to digital rights. Snowden's disclosures not only changed the attitudes of technology companies towards state surveillance and digital rights, but also caused them to implement significant technical changes that made state surveillance much more difficult. In doing so, Snowden has begun to achieve his aim of a 'technical solution' to the problem of state surveillance (Snowden, 2014).

Relationship with the legislature

Snowden's disclosures were condemned by both coalition parties in government. David Cameron said they 'damaged national security' and Nick Clegg, a prominent campaigner for digital rights, called them 'damaging' and of immense interest to those who would do us harm' (Clegg, 2013; Cameron, 2013). Former Defence Secretary Liam Fox called Snowden 'criminally irresponsible' and suggested the disclosures were 'extraordinarily damaging', whilst MP Julian Smith suggested that the Guardian Newspaper, who had published the disclosures, had broken the law and should be prosecuted (The Guardian, 2013; Fox, 2014). During a Home Affairs Select Committee hearing on the disclosures, MP Michael Ellis also accused the Guardian's editor of committing a crime by publishing the disclosures, and chairman Keith Vaz accused them of lacking patriotism (The Independent, 2013). But some MPs, such as David Davis, spoke out in favour of Snowden's actions. Responding to suggestions from a German MP that Snowden should be granted asylum in Germany, Davis agreed and argued that whistle-blowers were essential to keep the intelligence agencies in line.

> The only protection for us all in this sort of area is actually whistle-blowers. It's the only thing that makes these sorts of organisations behave properly. If whistle-blowers can look forward to a life in Germany rather than a life in Moscow, I think that would improve things for everybody (Davis, 2013).

In 2015, Davis joined forces with Labour MP Tom Watson to take the government to the High Court, in order to overturn powers created by the Data Retention and Investigatory Powers Act (DRIPA), which they said had been rushed through parliament with little scrutiny (The Guardian, 2015). But despite some support for Snowden's actions, debate in Parliament was initially limited, causing the Guardian's Editor, Alan Rusbridger, to claim that 'if Parliament's not going to have this discussion and if the courts can only do this in private then I think absolutely it falls to the press to stimulate a discussion' (Rusbridger, 2013).

However, following the publication of reports by RUSI and David Anderson QC, which suggested that oversight of the intelligence services had to be improved, Davis suggested that there was growing support in Parliament for such a move.

> There is a new consensus on this emerging among policymakers, the surveillance community, experts and politicians, is that judicial consent for use of these powers would offer a far higher level of oversight, and would be a far stronger protector of people's liberties, than the current system of ministerial authorisation (Davis, 2015).

Davis' view was reflected in reports by the Home Affairs Committee and ISC, both of which criticised the lack of oversight of the intelligence agencies. In 2014, the Home Affairs Committee published a report into counter-terrorism policy, which suggested that parliamentary oversight of the intelligence services was 'not fit for purpose' (Home Affairs Committee, 2014, p. 57). Amongst its recommendations were calls for the Investigatory Powers Tribunal to produce an annual report on its work to build public confidence, an increased role and resources for the Investigatory Powers Commissioner and a review of the Regulation of Investigatory Powers Act (RIPA). In 2015, the ISC also produced a report that called for greater oversight of the intelligence agencies and new surveillance legislation (Intelligence and Security Committee of Parliament, 2015).

Snowden's actions were widely condemned by MPs and there were few who supported him openly. His claims that the powers of the intelligence agencies should be reduced went largely unheeded and many of the activities that he had accused GCHQ of conducting illegally were later incorporated into the IPA, placing them on stronger legal foundations. However, Snowden's call for greater oversight of the intelligence agencies received far greater traction amongst MPs, and as a result, the IPA provides far greater oversight of the actions of the intelligence agencies. These include a new Investigatory Powers Commissioner, tough sanctions against those abusing surveillance powers, and the requirement for warrants for the most intrusive powers to be approved by both the Secretary of State and a senior judge (HM Government, 2017).

2.3.2.3 Rights Organisations

There are a variety of groups in the UK who campaign for digital rights, including ORG, who are specifically focussed on digital rights and Big Brother Watch (BBW), who focus on privacy more generally. These are supported by international groups such as the EFF, Access Now, Amnesty International, Liberty and Privacy International.

ORG is the only group specifically focussed on digital rights in the UK and attracts support from a range of high profile individuals. Its advisory council includes the deputy leader of the Labour party, Tom Watson, the former Liberal Democrat MP and now Facebook Policy Director, Richard Allan, Professor of Information Security and Privacy at the University of Oxford, Ian Brown, Google privacy lawyer, Trevor Callaghan and 'I.T. Crowd' creator, Graham Lineham who has even featured the group's poster in the lead characters' office.

The ORG operates and contributes to several campaigns promoting digital rights and regularly comments on news articles relating to privacy and surveillance. It's comments often feature in newspapers and its executive director, Jim Killock, is occasionally interviewed on news shows (Killock, 2013). ORG also runs privacy workshops and crypto parties[8] and contributed written and oral evidence to the IPB consultation (Parliament.uk, 2016). Despite having prominent supporters, the ORG does not have a particularly wide reach. Its Twitter account has less than 36,000 followers and the group claims to have around 3,000 active supporters.

[8] Grassroots events organised to demonstrate the benefits of practical cryptography.

Organisations such as ORG carry authority but, despite some high-profile backing, they do not attract widespread support.

Relationship with the public

According to the Edelman Trust Barometer, 40% of the public consider NGO's to be extremely credible or very credible, down 7% on the year before and not that far ahead of government representatives on 30% (Edelman, 2017). It's a surprisingly low figure which, combined with the niche appeal of digital rights organisations, makes it extremely difficult for them to influence the public directly. The ORG website, for example, has only received more than one thousand visitors a month on one occasion, following the passage of the Investigatory Powers Act - it usually receives less than 200 visitors per month[9].

Hosting local meetups and supporting crypto parties is an effective method of warning followers of the threat of state surveillance, but these events do not appeal to the wider public. As Policy Director Javier Ruiz explains, this has led to a debate over whether the organisation would be more effective if it targeted policymakers rather than the public.

> …we have many discussions around public campaigns, we've had some disagreements where some people see the need to be more of a broad-based campaign where there are other views that we are more like an expert group and its more effective to talk to one policy maker than a million people on the street (Ruiz, 2016).

Relationship with technology companies

In the UK, there is a close relationship between rights organisations and the technology industry, and each needs the support of the other to further their objectives. Digital rights organisations need technology companies to implement better security and privacy enhancing technologies, but technology companies also benefit from the endorsement of their privacy credentials from rights organisations. In the UK, the close relationship is demonstrated by the presence of representatives from Google, Yahoo and Microsoft on the ORG's advisory panel (Open Rights Group, n.d.).

One way for rights organisations to influence the technology industry is to raise awareness of their digital rights credentials. The EFF publishes an annual report that

[9] Using traffic analytics from semrush.com

rates the digital rights credentials of over 20 major technology companies, based upon whether they tell users about government data requests and how much they stand up for user privacy (Electronic Frontier Foundation, 2017). The report is published on the EFF's website and is designed to encourage technology companies to adapt their digital rights policies.

But rights organisations also support technology companies when they are acting to promote digital rights. In the case of Apple vs FBI, digital rights organisations including Access Now, American Civil Liberties Union, the EFF, the Electronic Privacy Information Centre, Privacy International and Human Rights Watch all submitted 'expert witness' evidence to support Apple (Electronic Privacy Information Centre, 2016). In Europe the ORG provided an amicus brief in support of Microsoft after the US government sought to gain access to email data stored by Microsoft in Ireland (Counsel for Amici Curiae Digital Rights Ireland Limited, Liberty, and the Open Rights Group, 2014).

But there is also concern that the technology industry's association with digital rights is not just hypocritical but is also designed to remove attention from their own abuses. Julian Assange labelled Google a 'surveillance baron' when discussing how they fund digital rights organisations such as the EFF.

> The EFF is a great group, and they've done good things for us, but nonetheless it is significantly funded by Google, or people who work at Google… I don't know about EFF specifically, but it's the nature of organizations. They don't like to bite the hand that feeds them (Assange, 2014).

Facebook and Google have also been accused of using legal judgements against them to secretly fund groups such as the EFF in order to gain influence over them (Fortune, 2012). Having lost a class action lawsuit due to breaches of user privacy, Google was forced to pay damages anonymously to digital rights organisations, although they were able to help select which ones. The Electronic Privacy Information Centre (EPIC), which brought the lawsuit, received nothing, whilst digital rights organisations who had not challenged them received up to one million dollars of funding.

Relationship with the legislature

Digital rights organisations such as Access Now, ORG and Big Brother Watch have campaigned against surveillance legislation for decades and target the legislature

in several different ways. The ORG can exert direct influence through the MPs that sit on their advisory panel and they also submit evidence and briefings to MPs to influence legislation such as the IPB and the Digital Economy Bill (Parliament.uk, 2016; Open Rights Group, 2017). The ORG also encourage their supporters to lobby politicians on their behalf to encourage them to support digital rights. They host training days to show people how to lobby their MP and coordinate the lobbying of MPs to ensure that they are targeted in the most efficient manner (Open Rights Group, 2010; Open Rights Group, 2017). But whilst rights organisations are respected and trusted, their ability to influence substantial numbers of MPs is limited.

2.3.2.4 Technology Industry

The technology industry occupies a pivotal role in the securitisation of cyberspace, acting as a functional actor that facilitates and impedes state surveillance, a securitising actor that warns about state surveillance, and a threat actor that threatens online privacy. In their roles as securitising actors, companies such as Google, Facebook and Apple carry authority as they are considered to understand technology and how to secure it. Actors from the technology industry are also considered to be modern, forward-looking, cool and in tune with the views of the youth, as opposed to politicians who are often perceived as out of touch (Google, 2017; Tech World, 2016).

The technology companies also have extremely good reach. Over one billion people use the Google search engine and two billion use Facebook (Tech Crunch, 2017; Statista, 2013). Company announcements are hotly anticipated and product demonstrations by Apple are watched by millions of people around the world (Scribble, 2013). Steve Jobs was perhaps the most famous technology leader and attracted a cult following before his death, but Mark Zuckerberg, Bill Gates, Tim Cook and Elon Musk are also household names. During the Apple versus FBI conflict, Apple's CEO, Tim Cook, appeared on a variety of media platforms to promote Apple's case and featured on the front page of Time magazine (See Figure 2.3) (ABC News, 2016; Cook, 2016). Other companies, including Microsoft, Twitter, Facebook and Google rallied around Apple and filed court motions to support them (Miller, 2016). The only major actor who appeared to back the FBI was Microsoft co-founder Bill Gates, who argued that the FBI's request was about an individual phone and would not set a precedent or act as a backdoor (Gates, 2016).

The large technology companies have frequently acted together to oppose state surveillance. Companies including AOL, Apple, Facebook, Google, Microsoft, Twitter and Yahoo, joined together to form the 'Reform Government Surveillance' campaign and authored a joint open letter to the US Senate, expressing their support for a new act to defend Internet freedoms (Reform Government Surveillance, 2015). Apple, Facebook, Google, Microsoft, Twitter and Yahoo also submitted evidence to the IPB consultation arguing that complying with the bill's 'technical capability notices' would require the installation of backdoors into their products which would damage security (Apple & Facebook, 2016).

Figure 2.3 Tim Cook in Time magazine

The support of the technology companies is vital to the cause of digital rights and these companies have huge influence amongst politicians and the public. When actors such as Apple's Tim Cook make claims about the threat of state surveillance, these claims receive a wide audience and carry huge authority. According to digital rights advocates such as Oana Ciobotea, Apple is the army that is needed to fight the war on privacy.

> Apple is almost a religion, and not just in America, but all over the world, from Japan to Romania. It has millions of fans who follow it with cult-like dedication. So when Apple is attacked, people listen and are interested in all the technical details of encryption; nobody even thinks to say "I've got nothing to hide."

> Even though we've seen David trump Goliath several times during our history, to win the war on privacy you need an army — Apple proved to have exactly that (Ciobotea, 2016).

Relationship with the public

Despite the reach and authority of technology companies such as Google and Facebook, there is still a degree of suspicion over their privacy credentials (The Guardian, 2012). The business model of many technology companies is based on advertising which requires the collection of as much user data as possible to target adverts more precisely. Google provides free email to customers and, in return, it scans emails and targets adverts based upon profiles constructed from individuals' private data. Facebook's CEO Mark Zuckerberg has been accused of hypocrisy over his support for Apple, his opposition to state surveillance and his other pronouncements on privacy, given accusations surrounding his own platform, Facebook (Derakhshan, 2016; Stewart, 2011; Yoon, 2016).

The public perception of the hypocrisy of technology companies was evident in the response to a message posted to Facebook by their CEO, Mark Zuckerberg, in which he announced that he had called President Obama to express his frustration at the damage the government was doing to digital rights (Zuckerberg, 2014). Despite much support, the top-rated comments largely attacked Facebook for their own privacy intrusions (Zuckerberg, 2014).

> And we are supposed to trust all the corporations that Facebook sells our data to? Why is the government singled out in this abuse of internet privacy?
>
> Then in 2004, the CIA renamed the world's largest data gathering project: THE FACEBOOK
>
> It's cute when Facebook says they are concerned about your privacy
>
> This is ironic, Mark, given that Facebook and its business model of monetising user data (corporate surveillance) is (alongside Google, etc.) what enables dragnet government surveillance at global scale and at relatively minor cost.
>
> Just a touch hypocritical, no?

Facebook has also been accused of manipulating users' emotions by experimenting with individual newsfeeds to see how they affect user sentiment *(The Guardian*, 2014). Following news of the experiment, a small poll in the Guardian indicated that 84% of people had lost trust in the social network, although the scandal did little to damage Facebook's user base, which is still increasing (The Guardian, 2014).

Since the Snowden revelations, technology companies have been much more vocal in their defence of digital rights and have actively warned about the threat of state surveillance. However, whilst they have a large reach and can speak with authority, many consider them to be complicit in state surveillance, and their own digital rights abuses and suspect that they cynically exploit privacy concerns as a marketing tool.

Relationship with the legislature

Due to their importance to the economy and their popularity with the public, the technology industry is in a very good position to exert influence over the legislature and in recent years the influence of companies such as Google has grown significantly. The 'Campaign for Accountability' reveals the extent of Google's attempts to influence the US government by highlighting the number of Google executives that have become Whitehouse officials, the number of meetings between Google and Whitehouse officials, and allegations that Google and the government co-ordinate policy (Campaign for Accountability, 2016). The 'Google Transparency Project' highlights a similar revolving door between Google and European governments, with over 80 people moving jobs between Google and European governments between 2007 and 2017, significantly higher than in other sectors (Google Transparency Project, 2017). In the UK, Google's executive chairman, Eric Schmidt, worked for six years as David Cameron's business advisor, Tim Chatwni became director of communications at Google after heading communications for David Cameron and Amy Fisher became a special advisor to Home Secretary Amber Rudd having previously worked as a press officer for Google. Similar associations were made with the other political parties. The EU transparency register also demonstrates the extent of Google lobbying and shows that in 2016 it spent over five million euros on lobbying the EU, employed 14 lobbyists and had 157 meetings with the European Commission (EU Transparency Register, 2016).

The importance of the technology sector to the UK economy gives technology companies significant influence over the legislature. After the conservative government promised to reintroduce new surveillance legislation following their election in May 2015, three technology companies threatened to leave the UK. Ind.ie, a self-proclaimed ethical technology company, left the UK and moved to Sweden 'to avoid the possibility of having to add backdoors to our products', Eris Industries (now Monax) said they would leave the UK if the bill was passed as part of a 'mass exodus of tech companies' and Ghost.org announced its move to Holland in opposition to claims that the conservative government was planning to withdraw from the Human Rights Act (Ghost.org, 2015; Monax, 2015; Balkan, 2015). Larger companies also exerted pressure against surveillance legislation. In leaked emails between Hilary Clinton's campaign and Apple, Apple promised to 'amplify encryption messaging' by publicly commenting on the Investigatory Powers Bill (Jackson, 2015). In their written submission, they then claimed that if government proposals were passed, 'the personal data of millions of law-abiding citizens would be less secure' (Apple, 2015). Facebook, Google, Microsoft, Twitter and Yahoo also submitted joint evidence, which took a more conciliatory approach but warned about the dangers of undermining public trust (Facebook, 2015). The concerns of technology companies were restated by the House of Commons Science and Technology Committee report on technology issues associated with the Investigatory Powers Bill, which claimed that the bill risks 'undermining our strongly performing Tech sector' (House of Commons Science and Technology Committee, 2016, p. 3).

But despite significant lobbying, technology companies are still mistrusted by MPs and their positions on digital rights are often considered hypocritical. During the dispute between Apple and the FBI, the US Justice Department attorney alleged that Apple was motivated by a desire to boost its reputation rather than a genuine concern for privacy.

> Apple's current refusal to comply with the Court's Order, despite the technical feasibility of doing so, instead appears to be based on its concern for its business model and public brand marketing strategy (US Justice Department, 2016).

This view was supported by a previous court case relating to a similar issue, during which Apple's lawyer highlighted the economic and reputational harm that might befall them if they complied with the FBI's demands.

> Forcing Apple to extract data in this case, absent clear legal authority to do so, could threaten the trust between Apple and its customers and substantially tarnish the Apple brand. This reputational harm could have a longer term economic impact beyond the mere cost of performing the single extraction at issue (Dreifach, 2015).

Others suggested that Apple's stance was designed to be beneficial to the company as it would help promote the security of its products to the whole of the world.

> The current media coverage represents global, massive free advertising that the iPhone is very secure, with the headline "Not even the FBI can hack an iPhone." Apple will come across as a fighter for consumer privacy and iPhone security, consistent with its brand (Granados, 2016).

In a debate in Parliament on the Snowden disclosures, MP Ben Wallace argued that despite them arguing the opposite, technology companies themselves are a threat to digital rights because they are regulated far less rigorously than the security and intelligence agencies.

> The big capitalist companies in America - the Googles, the Facebooks - harvest our data without your leave, sell it on to intermediaries on and on and on. They make millions, billions of pounds, avoid tax - I haven't yet heard anyone saying how they all keep their servers offshore to avoid tax - and that's the area that needs regulating and protection (Wallace, 2013).

Technology companies have attempted to leverage their importance to the British economy, huge financial powers and lobbying capabilities to exert significant influence over the legislature. They have had some degree of success, in particularly when raising the potential financial costs of surveillance legislation but, despite this, they are not trusted by some legislators who still consider their actions to be self-interested and hypocritical.

2.4 Conclusion

The securitisation of cyberspace has been achieved by a variety of actors who have convinced different audiences that they face an existential threat. Each audience

has been exposed to opposing securitisations from the state and DRC, which are backed up by authoritative security speakers.

Edward Snowden has been able to reach a greater public audience than any other securitising actor from the DRC, convincing many to take greater precautions regarding their own security, purchase products with good security offerings and oppose new legislation on state surveillance. He has also influenced the legislature to moderate surveillance legislation and, perhaps most importantly, he has motivated technology companies to seek to implement 'technical solutions' to surveillance, which deny the government the ability to access user data. Technology companies, such as Apple, have taken up Snowden's mantel, implementing their own anti-surveillance technologies but also lobbying the government not to introduce intrusive surveillance powers. In support, academics and rights organisations have brought rigour and technical expertise to the cause by raising awareness, acting as expert witnesses and submitted evidence to government committees. But the DRC's securitisation of cyberspace is not universally accepted, with many considering Snowden a traitor, technology companies hypocritical and technical experts as irrelevant or not trustworthy.

On the other side, the government can reach the widest audience but they are often considered technologically backward and are not widely trusted by the public. Their relationship with technology companies has deteriorated since the Snowden disclosures and their ability to pass legislation such as the IPB is reliant on significant amendments and the support of other parties. The security and intelligence agencies bring greater credibility, authority and technical expertise to the government's cause but they are limited by their ability to release evidence to support their claims and have been damaged by the intelligence failures prior to the war in Iraq, allegations of abuse and the Snowden disclosures.

There is a battle to persuade each audience to support the cause of either the DRC or the state. Each side attempts to persuade the public, the legislature and technology companies to back their cause and support either national security or digital rights. Chapter 3 demonstrates how this can lead to escalating securitising rhetoric on either side as each attempts to 'out-hype' the other. But, interestingly, there are differences in which audience is considered to be most valuable and susceptible to each cause. There is disagreement within the DRC about the best audience to target to make the most significant impact towards digital rights. The ORG is split between trying to influence the public and the legislature, whereas

Edward Snowden has stated that he sees technology reform as the key to digital rights, rather than legislative reform. For the state, the legislature is the most important actor, as expressed by GCHQ's director Robert Hannigan when he claimed that it was not the role of security agencies or technology companies to make these types of decisions.

This introduces a new element to the conflict where, in addition to arguing over which cause is most worthy, the DRC and the state argue over which audiences can and should be empowered to influence surveillance and digital rights. The state has the greatest influence over the legislature and argues that elected representatives should make the final decisions, whereas the DRC has the most influence over technology experts and technology companies and increasingly argue that they should have the last say (Hannigan, 2016; Snowden, 2014). This has led to a significant conflict between law enforcement and technology companies.

3 THE SECURITISATION OF CYBERSPACE: SPEECH ACTS

Chapter 2 considers the external characteristics of cyberspace securitisation and establishes the key securitising actors and their power relationship with a variety of key audiences. This chapter considers the internal characteristics of cyberspace securitisation; how these securitising actors use particular language to convince the audiences of the existence of an existential threat.

The first part considers how Nissenbaum's three grammars of securitisation, everyday security practices, technification and hyper-securitisation, are used by both the state and the Digital Rights Community (DRC) to construct cyberspace threats as extreme and threatening to everyone. The second part then considers how the use of heuristic artefacts intensifies this threat construction by linking the threat to fears such as darkness, burglary, sickness and war. The final part considers how cyberspace securitisations are made more effective by their connections to other securitised issues such as terrorism and totalitarianism.

3.1 GRAMMARS OF SECURITISATION

The internal category of securitisation captures the characteristics of the speech act itself, including the language and its meaning. To meet the criteria of a securitising move, the speech act must highlight an imminent and existential threat to a referent object and a justification for extraordinary measures to be used to counter it. Buzan and Waever explain that whilst securitisation applies to a variety of different sectors, it is distinct 'sub-forms' or grammars of securitisation that tie referent objects, threats and securitising actors together (Buzan, et al., 1998, p. 27). Hansen and Nissenbaum propose cyberspace as its own sector and define three grammars, which they argue are specific to the cyber sector in their relevance, although they do also resonate with other sectors. The three grammars are hyper-securitisation, everyday security practices and technification (Hansen & Nissenbaum, 2009).

Hansen and Nissenbaum demonstrate the efficacy of these grammars of securitisation by applying them to cyber attacks on Estonia during its conflict with Russia. Several others have used the grammars to help understand certain aspects of the securitisation of cyberspace, including Georgieva, who considers Edward Snowden as an alternative securitising actor, Yury Kabanov, who compares cybersecurity discourses and policies between Russia and the EU, and Tiago Pedro

Vales, who applies the concepts to the politics of Brazilian cyberspace (Kabanov, 2014; Georgieva, 2015; Vales, 2016).

3.1.1 Hyper-securitisation

Hansen and Nissenbaum describe hyper-securitisation as the presentation of 'large-scale, complex, cascading disaster scenarios' and Barry Busan considers hyper-securitisation to be a 'tendency to exaggerate threats and to resort to excessive *countermeasures'* (Busan, 2004, p. 172; Hansen & Nissenbaum, 2009, p. 1157). Whilst Hansen, Nissenbaum and Busan focus specifically on the construction of threats as extreme, it is also useful to consider how a referent object's vulnerability to that threat is also constructed. A good demonstration of this relates to George Bush's construction of global terrorism as a threat to the US.

> On September 11 2001, America felt its vulnerability even to threats that gather on the other side of the Earth. We resolved then, and we are resolved today, to confront every threat from any source that could bring sudden terror and suffering to America (Bush, 2002).

Bush highlights America's vulnerability to threats from around the world and uses this to justify America's foreign actions. The simultaneous construction of extreme threats and extreme vulnerabilities serves to justify extraordinary measures to counter this threat.

3.1.1.1 Extreme Threat

Hypersecuritisation constructs threats as extreme due to their large scale, their cascading nature and their hypothetical and unpredictable outcomes.

Large Scale

Both the British state and the DRC routinely refer to cyberspace threats as large scale. The DRC makes frequent use of hyperbole, portraying the threat of state surveillance as so enormous in scale that it can destroy human rights, democracy and the Internet. Examples include comments by Edward Snowden, security expert Bruce Schneier, EU Commissioner on human rights Nils Muižnieks, and founder of the world-wide-web Tim Berners-Lee.

> I can't in good conscience allow the US government to destroy privacy, internet freedom and basic liberties for people around the

> world with this massive surveillance machine they're secretly building (Snowden, 2013).
>
> It [an encryption ban] wouldn't work, and trying would destroy the internet (Schneier, 2015)
>
> Despite the intentions, secret surveillance to counter terrorism can destroy democracy, rather than defend it (Muižnieks, 2013).
>
> The extension of the state's surveillance powers would be a destruction of human rights (Berners-Lee, 2012).

Whilst these claims open the DRC to accusations of exaggeration, they also construct state surveillance as existentially threatening to democracy, the Internet and human rights; claims which are too dangerous to ignore. The state also constructs the national security threat as massive in scale and often uses figures and statistics to back up this claim:

> Over the last decade the threat to national security and property from cyber attacks has increased exponentially (HM Government, 2010, p. 4).
>
> Cyber-crime has been estimated to cost as much as $1 trillion per year globally (HM Government, 2010, p. 29).
>
> Government, the private sector and citizens are under sustained cyber attack today (HM Government, 2010, p. 29).
>
> Beijing experienced 12 million cyber attacks per day during the 2008 games (HM Government, 2010, p. 29).

However, without context, these claims can be misleading. The spectre of 12 million cyber attacks a day against the Beijing Olympics creates the impression of a massive threat to the London Olympics four years later, but the National Security Strategy (NSS) does not provide any provenance for this information and does not detail the methodology for arriving at this figure. Cyber attacks can be large in scale, destroying thousands of computers and critical infrastructure, or they can be tiny in scale, dealt with easily be security measures such as anti-virus software and firewalls.

But whilst the state constructs the cyberspace threat as large in scale, documents such as the UK Cyber Security Strategy (UK CSS) are also designed to promote

cyberspace as an opportunity for the UK. The UK CSS's vision for the next five years is a positive one and this positivity is evident throughout the strategy.

> Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society (HM Government, 2011, p. 8).

This balance is exemplified within Chapter 4, 'Meeting threats, taking opportunities', which outlines a positive vision of how threats in cyberspace can be mitigated, leading to a more secure and prosperous place for the UK to do business. This sense of balancing threats and opportunities can be found throughout the report.

> The growing role of Cyberspace has also opened up new threats as well as new opportunities (HM Government, 2011, p. 15).

> Our reliance on Cyberspace brings new opportunities but also new threats (HM Government, 2011, p. 7).

In addition, the UK CSS also emphasises the importance of dealing with cyber threats, whilst not breaching individual's rights and freedoms.

> We are determined to tackle the threats, but in a way which balances security with respect for privacy and fundamental rights (HM Government, 2011, p. 5).

> At home we will pursue cybersecurity policies that enhance individual and collective security while preserving UK Citizen's right to privacy and other fundamental values and freedoms (HM Government, 2011, p. 22).

Whilst the state constructs the cyber threat as large in scale, this construction is tempered by a parallel construction of cyberspace as a space of opportunity and government attempts to mitigate the threat as restricted, proportional and sensitive to legal and human rights concerns. The DRC is not so restricted in such a manner and tends to construct state surveillance as existentially threating to human rights and democracy.

Cascading

The concept of cascading security threats is one familiar to the cybersecurity industry due to the nature of cyberspace itself. The concept of the 'network' in general, and the 'Internet' more specifically, is based on the interconnection of computing devices. Whilst the precursor to the Internet, the ARPANET, was originally envisaged by the US Defence Department to ensure the resilience of US defence communications during the Cold War, the dangers of cascading failure have now become prominent within cybersecurity research and discourse. This reflects warnings of cascading infrastructural failure found within other fields such as the resilience discourse (Albert, et al., 2000; Motter & Lai, 2003). The concept of cascading failure is based on the premise that the failure of one node in a network will lead to traffic being redirected to another node, which will then fail and the failure will cascade throughout the system. As Hansen and Nissenbaum explain, cyberspace threats are not just limited to networks but can also cascade out into the real world.

> The power of hyper-securitisation stems not only from a securitisation of the network itself, but from how a damaged network would cause societal, financial, military break-down, hence bringing in all other referent objects and sectors (Hansen & Nissenbaum, 2009, p. 1164).

This concept entered popular discourse around 1999 with the threat of 'Y2K' or the 'Millennium Bug', which highlighted how small computer errors could have significant cascading real-world impacts (BBC News, 2000). Whilst the consequences of the bug were not as big as predicted, there were still several cases of catastrophic real-world impacts, including a case in Sheffield where 154 pregnant women were given incorrect Down's syndrome test results that led to two abortions being carried out (The Guardian, 2001).

The British government argues that cybersecurity threats are not just about computers and networks but can have a significant impact on the real world. Interestingly these cybersecurity threats are claimed to emerge from two opposing sources; too little cybersecurity and too much cybersecurity. Poor security exposes networks to foreign states, terrorists and criminals, whereas too much security allows terrorists to plot and communicate online and criminals to evade detection.

The ‘Going Dark’ problem represents the issue of too much security. Encryption, it is argued, poses a threat to the ability of the state to view private communications, which in turn impacts on their ability to investigate and prevent crime and terrorism.

> The levels of encryption and protection that we are seeing in the devices and methods used to communicate are frustrating the efforts of police and intelligence agencies to keep people safe … The Internet is becoming dark and ungoverned space where images of child abuse are exchanged, murders are planned, and terrorist plots are progressed (Hogan-Howe, 2014).

The construction of cascading security threats is also commonplace within the DRC. In the dispute between Apple and the FBI, Apple claimed that the use of the ‘All Writs Act’ to access Syed Farook’s phone would lead to cascading impacts to health records, financial data and individual privacy.

> The implications of the government’s demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it … could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone’s microphone or camera without your knowledge (Cook, 2016).

It would have been difficult for Apple to have argued that the privacy of Syed Farook was worth protecting from the FBI, but they instead warned of the cascading consequences of granting the FBI access.

A similar construction of cascading threats was made in relation to UK surveillance legislation. Commenting on the passing of the Investigatory Powers Bill, Open Rights Group (ORG) Director Jim Killock argued that surveillance legislation in the UK and US would have a knock-on effect in other countries (Killock, 2016).

> The passing of the IP Bill will have an impact that goes beyond the UK's shores. It is likely that other countries, including authoritarian regimes with poor human rights records, will use this law to justify their own intrusive surveillance powers (Killock, 2016).

This is a common argument within the DRC and makes the case that, even if the UK government could protect its citizen's security by passing laws to allow surveillance, other countries could use this example as an excuse to abuse their own citizen's rights.

Hypothetical and Unpredictable

As Hansen and Nissenbaum explain, the securitisation of cyberspace is often achieved through claims of what could happen if preventative action is not taken (Hansen & Nissenbaum, 2009). As cyberspace is new and rapidly evolving, past precedent is of limited use. The spectre of hypothetical future threats has greater impact and can lead to the securitisation of threats that may never materialise or were never a realistic possibility.

The NSS, SDSR and UK CSS make frequent references to the fast-moving development of cyberspace and the difficulty in understanding new and emerging threats. Both the SDSR and NSS use the term 'Age of Uncertainty' in their titles, which implies an unpredictable landscape of unknown threats. The NSS refers to 'a world of startling change', 'a world that is changing at an astonishing pace' and 'an age of uncertainty' with 'new and unforeseen' and 'evolving threats' (HM Government, 2010, pp. 3-5). The UK CSS also claims that 'predicting and understanding how Cyberspace will be used in future is difficult given the rate of innovation and change. New vulnerabilities and risks will emerge suddenly' (HM Government, 2011, p. 18).

Constructing the cyberspace threat landscape as uncertain aids its securitisation by drawing on fears of the unknown and boosting the case for defensive measures that can deal with any eventuality. The documents also reference hypothetical threats that could develop if we take no action now.

> While terrorists can be expected to continue to favour high profile physical attacks, the threat that they might also use Cyberspace to facilitate or mount attacks against the UK is growing (HM Government, 2011, p. 15).
>
> In times of conflict, vulnerabilities in Cyberspace could be exploited by an enemy to reduce our military's technological advantage, or to reach past it to attack our critical infrastructure at home (HM Government, 2011, p. 15).

> But in future, unless we take action, this threat could become even worse (HM Government, 2010).

The DRC does not tend to highlight the pace of change in cyberspace as a threat and often see it as an opportunity to outmanoeuvre slow political forces or the 'weary giants of flesh and steel' (Barlow, 1996). However, the DRC does heavily rely on the hypothetical. Snowden's disclosures provided information to the public but were primarily focussed on the technical capabilities and technical accesses of NSA and GCHQ, rather than how these capabilities were used. The disclosures, for example, highlighted backdoors that were used to access servers, wires that were tapped and malware that was written, but there was little evidence of how these opportunities were exploited by intelligence analysts at GCHQ and the NSA. Whilst some see GCHQ's ability to access the public's emails as a threat, others only consider it to be a problem if they are doing it on a large scale, without a warrant and against those who are not suspected of committing a serious crime. Knowledge of the capabilities of GCHQ and the NSA, but not their actual activities, facilitates the construction of many hypothetical threats about state surveillance and much of the reporting following the Snowden disclosures focussed on what GCHQ and the NSA *could* be doing, rather than what they *are* doing. The following news headlines are examples of claims of what the NSA and GCHQ can hypothetically achieve.

> Edward Snowden says GCHQ has the power to control your smart phone (BBC News, 2015).

> NSA Cracks Encryption Codes, Can Read Email, Banking, Medical Records (Off The Grid News, 2013).

> Snooping tools GCHQ could use to hack your phone's microphone, camera and keypad (Belfast Telegraph, 2014).

> How the NSA can 'turn on' your phone remotely (Money.com, 2014).

Whilst the state uses the fast-developing nature of cyberspace to construct hypothetical future threats, the DRC uses the secret nature of state surveillance to construct hypothetical current threats. Both constructions help to securitise cyberspace by portraying these hypothetical threats as more dangerous than those that are currently known to exist.

3.1.1.2 Extreme Vulnerability

Whilst the construction of an issue as extremely threatening will contribute to its securitisation, this can be supported by the claim that the referent object in question is particularly vulnerable. This can be achieved by highlighting the limited defences associated with the referent object and the difficulties in defending it. It can also be achieved by constructing vulnerabilities in the referent object as extreme and existentially threatening to its survival.

Limited Defences

The NSS and UK CSS both focus on explaining the extreme vulnerability of UK cyberspace to attack. Whilst specific weaknesses in the nation's defences are mentioned, it is the UK's dependency on cyberspace which is highlighted as the greatest concern.

> Britain today is both more secure and more vulnerable than in most of her long history (HM Government, 2010, p. 3).

> Risks emanating from our growing dependence on it [Cyberspace] are huge (HM Government, 2010, p. 29).

> As our dependency on it [Cyberspace] increases so do the risks and threats we face online (HM Government, 2010, p. 29).

> The scale of our dependence [on Cyberspace] means that our prosperity, our key infrastructure our places of work and our homes can all be affected (HM Government, 2011, p. 15).

Whilst increased dependency on cyberspace is constructed as a threat, cyberspace is also presented as an opportunity, hence reducing our dependency on it is not considered a good way in which to reduce the security threat. Instead, the state argues that the country's increased dependency on cyberspace creates an increasing requirement for more state security spending.

Rather than constructing the public's increased dependency on cyberspace as a threat, the DRC instead sees cyberspace as a tool to liberate activists and oppressed citizens by allowing them to operate in an untraceable manner. Whilst state surveillance is constructed as a threat to this liberation, increased usage of cyberspace itself is not considered a threat.

The securitisation of cyberspace is heavily influenced by the concept that anything but absolute security must be considered as absolute insecurity. The concept of absolute security might work at a technical and mathematical level, but it is more realistic to discuss the degree of security that a piece of software or hardware provides. The Wi-Fi protocol WEP, for example, is considered to be completely insecure because it can be cracked in a matter of seconds but WEP still provides protection against the casual eavesdropper and most people do not have the technical capability or knowledge to defeat it. Likewise, when digital rights campaigners argue that a backdoor is a backdoor for all, they forget that the system was probably not completely secure in the first place and that it likely still remains secure to all but the most sophisticated of hackers.

A similar concept applies to state claims that cyberspace is becoming ungovernable due to encryption. This claim again presents security as binary, and suggests that encrypted communication cannot be accessed by the state. This is misleading, as there are several ways to access the content of an encrypted message other than by breaking its encryption. Intercepting the message before or after it has been encrypted is one such example, and new vulnerabilities are often discovered in encryption algorithms that were once considered secure. Conversely, plaintext messages are not totally insecure if sent without encryption, as the state must still intercept them and know that they are of interest.

The issues of encryption and backdoors are at the heart of the ‘Going Dark’ and ‘Compromised Security’ securitisations. For the British state, the ‘Going Dark’ issue is a major threat to the ability of the intelligence and security services to govern and protect the UK, and several state actors construct the difficulties of the government accessing online data to be a severe threat to national security. The banning of certain uses of encryption, the creating of backdoors and the weakening of encryption algorithms are all claimed to be justified by this existential threat to law and order.

The FBI and its Director, James Comey, claim that the ‘Going Dark’ problem will cause law enforcement to miss out on opportunities to catch criminals and stop terrorist attacks.

> When changes in technology hinder law enforcement’s ability to exercise investigative tools and follow critical leads, we may not be

> able to root out the child predators hiding in the shadows of the Internet, or find and arrest violent criminals who are targeting our neighbourhoods (FBI, 2016).
>
> With Going Dark, those of us in law enforcement and public safety have a major fear of missing out—missing out on predators who exploit the most vulnerable among us...missing out on violent criminals who target our communities...missing out on a terrorist cell using social media to recruit, plan, and execute an attack (James Comey, 2014).

In the UK, the government and security agencies also describe this issue as a threat to national security although the term 'ungovernable' is used more frequently than the term 'Going Dark'.

> We cannot allow parts of the internet - or any communications platform - to become dark and ungoverned space where images of child abuse are exchanged, murders are planned, and terrorist plots are progressed (Hogan-Howe, 2014).
>
> [Do] we want to allow a means of communication between two people which even in extemis with a signed warrant from the home secretary personally that we cannot read? ...My answer to that question is no, we must not. The first duty of any government is to keep our country and our people safe (Cameron, 2015).

The state's desire for visibility of the actions of the populace can be compared to the power of the guard within Jeremy Bentham's Panopticon, who can observe any prisoner at any time without them knowing. Some claim that the state's surveillance machinery as an attempt to create a digital panopticon for the modern day (Bruno, 2014).

The state's claim that all inaccessible areas of cyberspace are threats to national security is mirrored by those who construct any methods to bypass security measures as threats to all aspects of cybersecurity. Those who oppose the potential circumvention of security measures by the state claim that any such efforts by the state will lead to the compromise of everyone's security. During Apple's dispute with the FBI, Apple CEO, Tim Cook, claimed that the FBI's request to create a tool

to access the iPhone of one of the perpetrators would put all its customers at risk of attack.

> The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes (Cook, 2016).

In an interview with the Daily Telegraph, Cook made the claim that any backdoor is a backdoor for everyone. In other words, if the government creates a means of access to some form of hardware or communication then everyone will be able to exploit that access.

> Any backdoor is a backdoor for everyone. Opening a backdoor can have very dire consequences (Cook, 2015).

The ORG make a similar claim in response to reports that the government wanted to be able to force companies to remove encryption from particular online communications if presented with a warrant. Like Cook, the ORG construct the issue as a binary choice between security or insecurity for all.

> Either encryption can only be removed by the intended sender and recipient, or it is broken and unsafe (Killock, 2016).

This view is echoed widely within the technology industry and the DRC, including the Information Technology Industry Council and the technology company Mozilla.

> Weakening encryption or creating backdoors to encrypted devices and data for use by the good guys would actually create vulnerabilities to be exploited by the bad guys (Information Technology Industry Council, 2015).

> There is just no "safe" backdoor. You are either safe or you are not (Dixon-Thayer, 2016).

The claim that any attempt to circumvent security measures would lead to total insecurity has become institutionalised within the cybersecurity community and is often repeated in different forms. The term backdoor has also become

institutionalised to represent any form of government attempts to make data accessible, which is, in turn, recognised as a dangerous threat to security.

The claims that all security vulnerabilities and all difficult to access areas of cyberspace bring about (in different ways) absolute insecurity contribute significantly to the securitisation of cyberspace. Anyone concerned about government attempts to circumvent security is encouraged to accept the securitising claim that all such attempts lead to massive insecurity, whereas those who are concerned with the state's ability to uphold the rule of law are encouraged to believe that all inaccessible spaces in cyberspace are a massive threat to law and order.

3.1.2 Everyday Security Practices

Thierry Balzacq argues that 'the success of securitisation is highly contingent upon the securitising actor's ability to identify with the audience's feelings, needs, and interests' and suggests that 'the speaker has to tune his/her language to the audience's experience' (Balzacq, 2005, p. 184). Hansen and Nissenbaum ague that this is achieved by utilising the second of their grammars of security, everyday security practices, which link the securitised threat directly to the audience. Personalising the threat makes it directly applicable to the audience and their everyday experiences of life. The personalisation of the threat is more likely to elicit a desirable response from the audience because to ignore this threat would be to act against the individual's own best interests. Everyday security practices also draw the audience into the securitisation by securing the individual's partnership and compliance in countering the threat. Company employees of all levels, for example, might play a critical role in defending the company against catastrophic cyber attack by being alert to the threat of phishing emails.

When articulating cyberspace threats, the state makes frequent reference to the direct impact that these threats may have on particular groups, including the country as a whole, industry and individuals. The introduction to the UK CSS outlines the importance of a trusted digital environment for businesses and individuals, and then specifically sets out the measures that will be taken 'if you are in business' or 'if you are an individual' (HM Government, 2011, p. 5).

Whilst national security is often highlighted as the referent object under threat, the documents also frequently highlight how threats can affect every aspect of the everyday lives of citizens. Threatened areas include 'our places of work and our

homes', 'our economic prosperity and our own private lives' and even 'children and the vulnerable' (HM Government, 2011, p. 15). The threat will get worse as 'the scope of potential targets will continue to grow' and incidents will 'affect larger numbers of individuals and organisations' (HM Government, 2011, pp. 15,16).

The UK CSS also includes a whole section, titled 'Affecting individuals and societies', which outlines the numerous ways in which the cyber threat can impact on the everyday lives of citizens. Threats are said to now affect 'society more broadly' and public use of the internet 'makes for a more attractive target for criminals' (HM Government, 2011, p. 17).

The UK CSS discusses a range of threats to national security, but also personalises these threats by discussing how they can impact the daily lives of individuals. In doing so, this aids the securitisation process as threats are presented as threatening to individuals and their everyday lives.

> Attacks in Cyberspace can have a potentially devastating real-world effect. Government, military, industrial and economic targets, including critical services, could feasibly be disrupted by a capable adversary (HM Government, 2010, p. 30).

> Cyberspace is already woven in to the fabric of our society. It is integral to our economy and our security and access to the internet, the largest component of cyberspace, is already viewed by many as the 'fourth utility', a right rather than a privilege (HM Government, 2010, p. 29).

Whilst the state frequently frames cyberspace as threatening to the everyday lives of citizens, it also makes a particular effort to highlight how the state's actions in cyberspace help to protect individuals.

> The levels of encryption and protection that we are seeing in the devices and methods used to communicate are frustrating the efforts of police and intelligence agencies to keep people safe (Hogan-Howe, 2014).

> We need an informed, balanced discussion with communications providers to explore what they can do to help us protect the public from serious crime and terrorism (Hogan-Howe, 2014).

The UK CSS also dedicates a significant amount of text to explaining how businesses and individuals are both capable and responsible for countering the cyber threat. In its roles and responsibilities section, the strategy has separate entries for the state, individuals and business, and outlines the importance of these roles. To underline the importance which the state places on individual and private sector participation in countering cyberspace threats, the role of these groups is given more prominence than that of the government.

> Ordinary people have an important role to play in keeping cyberspace as a safe place to do business and live our lives (HM Government, 2011, p. 22).
>
> The private sector has a crucial role to play in the UK's cyber security (HM Government, 2011, p. 23).

These claims are supported by commitments within the Cyber Security Programme (CSP) to dedicate spending to help individuals and businesses to combat the cyber threat. Examples of these projects include the Cybersecurity Information Sharing Partnership (CISP)[10], which was introduced to allow government and industry to share information on cyber threats, the Get Safe Online campaign[11], which is a private/public partnership, that gives advice on avoiding cyber threats and the Cyber Essentials[12] website, which advises businesses on how to avoid cyber threats.

Whilst the state does make efforts to relate the cyberspace threat to the average citizen, it is also largely focused on the national security threat and the threat to the state itself. The elevation of cyber attack to a tier one threat was first made in the National Security Strategy, whilst £650 million in funding was first announced for cybersecurity in the Strategic Defence and Security Review, and the UK Cyber Security Strategy was tag-lined with the phrase 'Protecting and promoting the UK in a digital world' (HM Government, 2011). Each of these elements highlights the focus on national security and the state and, despite an effort to relate the threat to the individual, the documents are still presented as being primarily focused on national security.

On the other side of the debate, the DRC focus almost entirely on threats to human rights and threats to individual citizens. This is demonstrated by several comments

[10] https://www.ncsc.gov.uk/cisp
[11] https://www.getsafeonline.org/about-us/
[12] https://www.cyberaware.gov.uk/cyberessentials/

made by Edward Snowden, who claims that his sole motivation ‘is to inform the public as to that which is done in their name and that which is done against them’ (Snowden, 2013).

> Even if you're not doing anything wrong, you are being watched and recorded (Snowden, 2013).

> The NSA has built an infrastructure that allows it to intercept almost everything. With this capability, the vast majority of human communications are automatically ingested without targeting. If I wanted to see your emails or your wife's phone, all I have to do is use intercepts. I can get your emails, passwords, phone records, credit cards (Snowden, 2013).

In the case of Apple vs FBI, which was played out in the media and which drew huge interest, Tim Cook presented the FBI’s request to access an iPhone as a threat to individuals and portrayed Apple as a defender of the people.

> The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers. Doing so would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data (Cook, 2016).

Apple also positioned themselves as not just on the side of the public but as part of the public by referring to threats to ‘our’ personal information and to ‘our’ personal safety.

> Compromising the security of our personal information can ultimately put our personal safety at risk. That is why encryption has become so important to all of us (Cook, 2016).

In doing so Apple simultaneously constructed the FBI’s request as a threat to all individuals, positioned Apple on the side of the people and positioned Apple as one of the people. The ORG also focus directly on the threat to individuals, something that is evident in their mission statement.

> Open Rights Group exists to preserve and promote your rights in the digital age. We are funded by over 3,000 people like you. Technological developments have created new threats to our human rights. We raise awareness of these threats and challenge

> them through public campaigns, legal actions, policy interventions and tech projects (Open Rights Group, n.d.).

ORG is also associated with campaigns such as 'Don't Spy on Us' which, by its name, simultaneously portrays the individual as threatened but also establishes ORG themselves as part of this threatened group.

Digital rights organisations also employ everyday security practices by highlighting the ways in which individuals can take responsibility for combatting cyberspace threats. The group is funded by donations from individuals and it encourages supporters to donate to 'help us in this fight' against UK surveillance laws, to volunteer to campaign for the group, to contribute to events, to create literature and to fundraise for the group (Open Rights Group, n.d.). They also encourage supporters to email their MP to lobby for changes in the law and provide instructions on how to contact their MP and what to say (Open Rights Group, n.d.).

Whilst the state does attempt to relate cyberspace threats to individuals, this effort is limited due to a dominant focus on national security and threats to its existence. Claims of threats to national security or to the police's capability to protect the public might be viewed as tangential to the public's concerns rather than directly threatening. As a result, everyday security practices are less relevant to state securitisation of cyberspace than they are to the DRC. At the heart of the DRC's construction of cyberspace threats is the threat to the individual and, as a grassroots movement, the support and involvement of the public is key. Relating cyberspace threats to the public is, perhaps, an easier task for the DRC than it is for the state, due to their closer relationship with the public and greater focus on direct threats to individuals rather than threats to the economy or national security.

3.1.3 Technification

The last of Hansen and Nissenbaum's grammars of cybersecurity is technification, which is the process by which an issue is constructed as complex and technical, requiring expert knowledge to understand and articulate.

> Technifications are, as securitizations, speech acts that ''do something'' rather than merely describe, and they construct an issue as reliant upon technical, expert knowledge, but they also simultaneously presuppose a politically and normatively neutral agenda that technology serves (Hansen & Nissenbaum, 2009, p. 1167).

Due to this requirement for expertise, authority to speak on technical issues is reserved for technical experts who can claim authority to speak security on an issue due to their superior knowledge and understanding of the subject.

Technification can be applied to a range of issues, but Hansen and Nissenbaum highlight three significant aspects of cyberspace that make it a particularly suitable space for technical, expert discourse - a strong emphasis on hypothetical threats, a rapid pace of change in technology and attack methodology, and a daunting knowledge requirement to master the field.

> The strong emphasis on the hypothetical in cyber securitizations create a particular space for technical, expert discourse … the knowledge required to master the field of computer security is daunting and often not available to the broader public, including Security Studies scholars. The breathtaking pace at which new technologies and hence methods of attacks are introduced further adds to the legitimacy granted to experts and the epistemic authority which computer and information scientists hold allow them the privileged role as those who have the authority to speak about the unknown (Hansen & Nissenbaum, 2009, p. 1167).

The hypothetical nature of cyberspace threats, particularly those associated with cascading disaster scenarios such as attacks on critical infrastructure, are particularly prone to technification, as without past precedent and knowledge of technical vulnerabilities, it is difficult for non-experts and the public to assess for themselves the risk of a particular threat scenario materialising. The degree of knowledge required (or at least perceived to be required) to understand inherently technical and fast-moving cyberspace threats adds to the reliance on experts to investigate, assess and articulate these threats.

As well as the ability to understand cyberspace threats, another aspect of cybersecurity which lends itself to mediation by experts is that of privileged access to information on cyberspace threats. In particular, the state has a monopoly on ‘classified intelligence’ relating to cyberspace threats, which gives it authority to speak on these issues. In addition to technifying cyberspace threats by highlighting their complexity, the state can also technify issues by highlighting how they can only be understood properly by those with access to classified intelligence. The

importance of classified intelligence is highlighted by the government's refusal to reveal how almost half of the cybersecurity budget will be spent.

> Around half of the £650 million funding will go towards enhancing the UK's core capability, based mainly at GCHQ at Cheltenham, to detect and counter cyber attacks. The details of this work are necessarily classified (HM Government, 2011, p. 27).

But the state is not the only actor which can claim access to privileged information on cyberspace threats. Threat Intelligence had become a significant product offering for cybersecurity companies, such as 'Digital Shadows', and many cybersecurity companies strongly promote their ability to access information on cyber threats. With regards to the construction of the State Surveillance Threat, access to information also provides authority to speak cybersecurity with individuals, such as Edward Snowden gaining authority from his prior work in the NSA and Julian Assange gaining authority from his access to huge volumes of classified material.

Whilst the technification of an issue can lead to greater authority for an expert to speak security, the process can also lead to a reduction in the ability to scrutinise that expertise. As Schwarz puts it 'the authority of technocrats in this area is rarely questioned because technocrats are treated as extensions of technology' (Schwarz, 2016, p. 2). And as Hansen and Nissenbaum explain;

> [technification] constructs the technical as a domain requiring an expertise that the public (and most politicians) do not have and this, in turn, allows ''experts'' to become securitizing actors while distinguishing themselves from the ''politicking'' of politicians and other ''political'' actors (Hansen & Nissenbaum, 2009, p. 1167).

Despite an outward appearance of apoliticism, Jef Huysmans argues that 'in technocratic or modern societies expert knowledge is inherently political' (Huysmans, 2006, p. 10). But according to Hansen and Nissenbaum, despite the inherently political nature of technical knowledge, the processes of securitisation and technification can allow this political nature to hide.

> Cyber Security discourse's simultaneous securitization and technification work to prevent it from being politicized in that it is precisely through rational, technical discourse that securitization

> may ‘‘hide’’ its own political roots (Hansen & Nissenbaum, 2009, p. 1168).

In doing so, technification can aid in the de-politicisation of issues by ceding the authority to discuss them with experts. This can lead to securitisation, as experts can claim the sole authority to determine what is or is not a security threat. This is not to say that technical expertise is not a useful, or indeed essential, component to cybersecurity debates. However, it does highlight that when issues are construed as technical, they can become depoliticised and securitised.

An additional impact of technification, highlighted by Schwarz, is the danger that ‘framing something in a specific way, like cyberspace as technical, can remove other concerns, such as ethical or political, from the discussion’ (Schwarz, 2016, p. 3). Framing the use of encryption by terrorists as a technical problem can lead to calls for a technical solution, such as weakened encryption, without adequate consideration of the wider political and ethical issues. Likewise, framing the issue of intrusive state surveillance as a technical problem can lead to the design of software which removes the ability of technology firms to comply with legal court orders, again without adequate consideration of the wider political and ethical issues.

The contention that an issue has been technified does not necessarily mean that this process was deliberate or that this technification is necessarily a bad thing. Norman Girvan argues that technification can refer to both the issues (issue technification) and the language that is used to explain these issues to decision makers, stakeholders and the public (discourse technification) (Girvan, 2010). Issue technification is an intrinsic property of a particular subject, so cannot be avoided, but discourse technification is not. As Girvan argues;

> In principle, any technical issue should be susceptible to explanation to the general population in language that it can understand, for without this the democratic process cannot function effectively (Girvan, 2010, p. 109).

Girvan further argues that discourse technification comes about because of a ‘political decision to restrict participation in decision-making’ (Girvan, 2010, p. 109). Girvan sees discourse technification as a deliberate strategy designed to limit those who can be involved in decision making. Whilst there is certainly evidence that technification can be used in this manner, including that which is provided by

Girvan, it cannot be said that this is always the case. Several reasons can explain the presentation of some issues as highly technical, including the inability of the speakers to translate technical issues into everyday language, the overestimation by a technical expert of the public's knowledge of a subject, or an ignorance of the public's desire to want to understand and engage with a particular subject. In some cases, not only is an issue inherently technical, but so too is the language used to discuss it. In these cases, it is a lack of proactive effort to de-technify an issue that restricts the public's interaction with it rather than a deliberate attempt to technify the language.

The issue of the desirability and morality of securitisation will be discussed later in this thesis, but it is worth at this point briefly discussing the desirability of technification. In the introduction to Risk Society, Scott Lash and Brian Wynne discuss the problems associated with technical experts being 'given pole position to define agendas and impose bounding premises a priori on risk discourses' (Lash & Wynne, 1992, p. 4).

> the primary risk, even for the most technically intensive activities (indeed perhaps most especially for them), is that of social dependency upon institutions and actors who may well be- and arguably are increasingly- alien, obscure and inaccessible to most people affected by the risks in question (Lash & Wynne, 1992, p. 4).

Hansen, Nissenbaum, Girvan and Schwarz make a similar case that the risk of technification (as with securitisation as a whole) is that it removes an issue from the public/political domain and places it into the hands of those who are inaccessible and unaccountable to those affected by the issue. The main argument against this is that decision making about very technical issues is best left in the hands of experts but, as Lash and Wynne explain, this raises the issues of trust and credibility. How can we trust that experts are apolitical and acting in our own interests and how do we know that they are not acting ideologically or according to their own agendas? However, when considering how issues in cyberspace become securitised through technification, it is not necessary to understand whether that technification was deliberate or desirable, the important element is that by presenting issues as technical, they are removed from public debate and authority is granted to experts to speak security on these issues. In doing so technification aids securitisation as it makes it harder to challenge the experts who present issues as security threats.

The British state technifies cyberspace threats by simultaneously constructing them as complex, hypothetical, rapidly changing and hidden, whilst portraying itself as the only actor with both the technical expertise and the access to the requisite threat intelligence to manage the defence against these threats. The UK CSS, for example, contains a section titled 'A complex problem', which highlights the difficulties in addressing the problems of cybersecurity (HM Government, 2011, p. 18). This highlights the rapid pace of change in cyberspace, its complexity, the difficulty in predicting threats in this domain and the requirement for classified information in order to understand the threat.

The actual existence of a UK Cyber Security Strategy is a simultaneous form of technification and securitisation because the need for such a strategy alone constructs cyberspace as a complex problem, a security problem and one which the state has the technical authority to address. Table 3.1 provides examples of this technification from within the NSS and UK CSS.

Complex	*The systems that form Cyberspace contain a vast array of components sourced from a global diverse range of suppliers. Multiple sub-contractors produce, test, package and assemble these components (HM Government, 2011, p. 18).*
	The complexity of Cyberspace (HM Government, 2011, p. 18).
Hypothetical	*Predicting and understanding how Cyberspace will be used in future is difficult given the rate of innovation and change (HM Government, 2011, p. 18).*
	New vulnerabilities and risks will emerge suddenly (HM Government, 2011, p. 18).
	We are continually facing new and unforeseen threats to our security (HM Government, 2010, p. 4).
Changing Rapidly	*The growing adoption of the internet and new uses of digitally connected technologies make for a fast moving complex environment (HM Government, 2011, p. 18).*
	The pace of events can make existing defences look slow and inadequate (HM Government, 2011, p. 18).

	In a world that is changing at an astonishing pace (HM Government, 2010, p. 4).
Hidden	*cyber attacks are difficult to detect (HM Government, 2011, p. 22).*
	The covert nature of the threat means that the public and businesses can underestimate the risks (HM Government, 2011, p. 18).
	key data and systems on which we now rely can be compromised or damaged, in ways that are hard to detect or defend against (HM Government, 2011, p. 5).

Table 3.1: Technification examples

Having established cyberspace threats as inherently complex, technical and subject to expert interpretation, the UK CSS positions the UK state, and GCHQ in particular, as the expert agency with the knowledge, technical abilities, expertise and access to intelligence that is required to understand, articulate and defend against these threats. By establishing itself as the expert authority, the state claims the authority to interpret the threat and determine the correct policy response. Table 3.2 provides examples of the state positioning itself as the expert within the UK CSS.

The State as Expert	*GCHQ is home to world-class expertise in cyber security (HM Government, 2011, p. 33).*
	GCHQ's unique expertise (HM Government, 2011, p. 33).
	world-class technical skills of GCHQ (HM Government, 2011, p. 42).
	GCHQ, the Government's signals intelligence agency, has some world-class skills at its disposal (HM Government, 2011, p. 18).
	funding will go towards enhancing the UK's core capability, based mainly at GCHQ at Cheltenham, to detect and counter cyber attacks (HM Government, 2011, p. 27).
	Continue to build up in GCHQ and MOD our sovereign UK capability to detect and defeat high-end threats (HM Government, 2011, p. 9).

	new partnerships between GCHQ and business to capitalise on unique Government expertise (HM Government, 2011, p. 9).
	The intelligence agencies and Ministry of Defence have a strong role in improving our understanding of – and reducing – the vulnerabilities and threats that the UK faces in cyberspace. GCHQ in particular is central to this effort (HM Government, 2011, p. 25).

Table 3.2: The state as expert

As well as establishing cyberspace threats as technical and the state as the actor with the requisite expertise to understand and articulate these threats, the UK CSS also justifies state involvement in countering cyberspace threats by framing them as issues of national importance. The 2010 UK CSS provides a breakdown of a range of different cyber threats and how they impact on a wide range of sectors and groupings, including individuals, businesses and the country. Whilst many of these threats can be considered to just affect businesses or individuals, they are framed as threats to national security. Attacks on individuals are framed as having an impact on 'society' and attacks on businesses are framed as having an impact on the country's economic security.

> Beyond the impact on individuals, the scale of the use of cyberspace means that it can now also affect society more broadly (HM Government, 2011, p. 17).

> the threat to revenues and intellectual property is capable of causing significant economic damage to the UK (HM Government, 2011, p. 28).

> Activity in Cyberspace will continue to evolve as a direct national security and economic threat as it is refined as a means of espionage and crime and continues to grow as a terrorist enabler, as well as a military weapon for use by states and possibly others (HM Government, 2010, p. 29).

National security is the responsibility of the state, so by raising cyberspace threats to the level of national security the state positions itself as the actor responsible for addressing these threats. This mirrors the state's monopoly on violence instantiated through the police and armed forces and its monopoly on the legitimate means of movement, which is established through objects such as the passport (Torpey, 2000).

But, whilst the state positions itself as the expert authority to understand and articulate cyberspace threats, it only presents itself as the legitimate co-ordinator of efforts to counter these threats rather than the sole actor with responsibility for countering them. The UK CSS suggests that a collation of government, industry and the public should have the responsibility for dealing with these threats. The state, due to its technical knowledge, institutions and covert intelligence is framed as the actor most capable of understanding and articulating the threat, but it is co-operation between the state, the public and the private sector which must be mobilised to defeat it.

> Though the scale of the challenge requires strong national leadership, Government cannot act alone. It must recognise the limits of its competence in cyberspace. Much of the infrastructure we need to protect is owned and operated by the private sector. The expertise and innovation required to keep pace with the threat will be business-driven (HM Government, 2011, p. 22).

> We need to build a much closer relationship between government, the private sector and the public when it comes to national security… Business and government will need to work much more closely together to strengthen our defence against cyber attack (HM Government, 2010, p. 5).

A whole section of the UK CSS titled 'Roles and responsibilities' sets out how business, the public and the state are all responsible for meeting the countries cybersecurity challenges.

> Our private sector, key government agencies and academia all have world-leading strengths in Cyberspace. We must bring these together (HM Government, 2011, p. 18).

> Ordinary people have an important role to play in keeping Cyberspace as a safe place to do business and live our lives … Everyone, at home and at work, can help identify threats in Cyberspace and report them (HM Government, 2011, p. 22).

The UK CSS establishes the notion that the state should investigate, analyse and articulate cybersecurity threats and that industry and individuals should follow the government lead in dealing with these threats. This concept is supported by the

establishment within the Cyber Security Programme of the Cyber Security Information Sharing Partnership (CISP). The CISP is designed as a hub which will 'pool government and private threat information and pass that out to nodes in key business sectors, helping them identify what needs to be done' (HM Government, 2011, p. 28). Other initiatives such as 'Cyber Essentials' or the annual conference 'Cyber UK', each of which is run by the government, contributes to the establishment of the state as the prime authority on cybersecurity issues. When other actors fail to recognise the authority of the state in this area, they are sometimes criticised for not being supportive enough. After the death of Lee Rigby, the Intelligence and Security Committee accused technology companies of not doing enough to combat terrorism.

> Their services not only host the material of violent extremism or child exploitation, but are the routes for the facilitation of crime and terrorism. However much they may dislike it, they have become the command-and-control networks of choice for terrorists and criminals (Hannigan, 2014).

The state constructs cyberspace threats as complex, technical and hidden, and in doing so it positions itself as the agent most well suited to addressing this problem. One of the consequences of this is an increased authority for the state as the technical expert with access to classified information to determine and define cyberspace threats. But another consequence of the framing of cyber threats as technical is the promotion of technical solutions to these issues, potentially at the expense of social, cultural or ethical considerations. Javier Ruiz, Policy Director for ORG, explains this issue when discussing the best way to deal with online threats.

> There are real threats around, for example, grooming children on social media and online abuse but is the solution a technological solution or is the solution a social or behavioural solution? For some things you have to look at the solution maybe not being more monitoring and algorithms but teaching people how to behave properly and sensibly so they don't meet someone [in public] who they met on social media, things like that ... GCHQ view the solution as technical because to a hammer every problem looks like a nail (Ruiz, 2016).

The state's construction of cyberspace threats as technical, complex and hidden, and the construction of the state itself as the only institution with the ability and authority to shed light on this dark space, helps to depoliticise and securitise issues by framing the state as the only body with authority to understand them.

The DRC often agree with the state's claim that cyberspace threats are complex and fast moving, and routinely refer to the complexity of human rights in cyberspace (Open Rights Group, n.d.; Ruiz, 2016). But the DRC pays particular attention to the intersection of technology and human rights and positions itself as the authority to define threats in this area. Open Rights Group, for example, describe themselves as existing 'to preserve and promote your rights in the digital age' (Open Rights Group, n.d.) .

> Technological developments have created new threats to our human rights. We raise awareness of these threats and challenge them through public campaigns, legal actions, policy interventions and tech projects (Open Rights Group, n.d.).
>
> The DRC exists because we need people to understand how technology is shaping our rights, for good and for ill, and who it is who is seeking to employ and capture technology for their benefit rather than yours (Killock, 2015).

Whilst the state portrays itself as a defender of human rights, the DRC attempts to position themselves as the more legitimate authority on the issue. The state can represent itself as the natural authority to speak on cyberspace threats by using its position of authority to speak on national security issues, but the DRC attempts to undermine this authority by highlighting the state's lack of understanding of human rights and technology. The ORG, for example are dismissive of state expertise and argue that 'powerful people are frightened, and don't understand the sort of information-age world we want to live in' and politicians 'don't understand new technologies, but comment and pass laws anyway' (Open Rights Group, 2008; Open Rights Group, 2007). As a result, according to DRC campaigners, such as Cory Doctorow, policy making is hindered and 'every tech policy out of Westminster is a silly quick-fix that provides a good headline but makes things worse (Doctorow, 2015).

Whilst the state uses its access to classified information to support its authority to articulate cyberspace threats, the rapid elevation of Edward Snowden's profile following his NSA disclosures gave the DRC the opportunity to claim their own direct access to information on cyberspace threats, particularly those which they claim to arise from state surveillance. Whilst former intelligence officials turned whistle-blowers, such as William Binney, have previously used their status and access to insider information to highlight cyberspace threats, Snowden is in a unique position to do so given the momentous nature of his actions and the worldwide attention that his disclosures have attracted.

In an interview with Glenn Greenwald, Snowden presents his views on the threats posed by state surveillance as emerging directly from his experience at the NSA.

> The stuff I saw really began to disturb me… I watched NSA tracking people's Internet activities as they typed. I became aware of just how invasive U.S. surveillance capabilities had become. I realized the true breadth of this system. And almost nobody knew it was happening (Greenwald, 2014, p. 43).

Both the state and Snowden claim that their access to privileged information allows them to understand cyberspace threats; the state argues that their intelligence must remain classified, whereas Snowden argues that the information he had access to had to be shared with the public. Despite Snowden placing the information he had access to in the public domain and despite some arguing that his 'only apparent qualification is his willingness to steal from his own government', Snowden's actions have provided him with a huge platform on which to promote his views (Pompeo, 2014). At the start of 2017, for example, Snowden had over 2.7 million Twitter followers; over 50 times that of GCHQ and around 10 times that of the NSA. Snowden is viewed by many as an expert on privacy and state surveillance but, as a technical expert, he is also able to portray his expertise as non-political. In an interview with 'The Nation', Snowden described his non-political nature:

> I did what I did because I believe it is the right thing to do, and I will continue to do that. However, when it comes to political engagement, I'm not a politician, I'm an engineer (Snowden, 2014).

Whilst Snowden argues that reform of surveillance laws is required, he also contests that only technical reform can help achieve his objectives because there is not enough public support for political reform.

> From the very beginning, I said there are two tracks of reform: there's the political and the technical. I don't believe the political will be successful. The issue is too abstract for average people, who have too many things going on in their lives. And we do not live in a revolutionary time. People are not prepared to contest power (Snowden, 2014).

ORG Policy Director Javier Ruiz, when discussing differing opinions on campaigning within the group, expressed a similar dilemma between broad-based political campaigning and more technical means towards achieving the group's objectives.

> We have many discussions around public campaigns, we've had some disagreements where some people see the need to be more of a broad-based campaign where there are other views that we are more like an expert group because it can be more effective to talk to one policy maker than a million people on the street (Ruiz, 2016).

Snowden also argues that technical reform will prove more effective, long-lasting and universal than political reform because technical standards can spread throughout the world, regardless of the politics of individual countries.

> The idea for me now … is to focus on technical reform, because I speak the language of technology … What I can do … is to help create the new systems that reflect our values. Of course I want to see political reform in the United States. But we could pass the best surveillance reforms, the best privacy protections in the history of the world, in the United States, and it would have zero impact internationally … But if someone creates a reformed technical system today—technical standards must be identical around the world for them to function together (Snowden, 2014).

'The Nation' questioned whether Snowden's ambition to create a new technical system for the Internet was a political act because it had political ambitions, and Snowden agreed that this was the case.

> In case you haven't noticed, I have a somewhat sneaky way of effecting political change. I don't want to directly confront great powers, which we cannot defeat on their terms (Snowden, 2014).

By constructing state surveillance as a technical threat and by proposing technical solutions, Snowden is attempting to securitise through rational technical discourse. Whilst Nissenbaum and Hansen describe this technifying process as preventing politicisation, in this case Snowden is attempting to bypass politics and use technology to achieve results directly through technological change. To do this he constructs state surveillance as a technical threat with a technical solution.

This construction of surveillance as a technical problem relates directly to the issues of backdoors and encryption, which permeate the debate over state surveillance. There are three major technical claims made by critics of state surveillance, which have been identified from the discourse. These claims present the issues of surveillance and privacy in the light of the technical issues of encryption and backdoors rather than as political issues. The claims are usually made by technical experts and are presented to the audience as technical facts. The first claim is that to perform surveillance the government must either install backdoors, or either weaken or destroy privacy (Backdoor/Weakened Security Claim). The second is that the existence of backdoors or weakened security will lead to catastrophic security and privacy problems, potentially making everyone's communications vulnerable (Catastrophic Vulnerability Claim). The third is that the existence of backdoors or weakened security will lead to unrestricted state intrusion into the lives of citizens (Unrestricted Surveillance Claim). Taken together the three claims form the basis of a rational technocratic argument against state surveillance.

The following three significant articles and statements from DRC members are used to demonstrate these three arguments. The first example is taken from an article written by Jim Killock, which featured in the Independent and was written in response to Robert Hannigan's claim that social networks are the command and control centres of terrorism (Killock, 2014). The article was significant in that it provided a contrary view to Robert Hannigan's statement, which was extremely controversial due to its accusations against social media companies. The second was drawn from an interview that Edward Snowden gave to 'The Nation'. It was one of his most wide ranging and comprehensive interviews and came shortly after his exile in Russia. The third is from an Open Letter to Customers which Tim Cook posted to the Apple website during its famous dispute with the FBI. Snowden described Apple's stance, outlined in the letter, as the 'key' to his desired technical solution to state surveillance (Snowden, 2014; Cook, 2016).

Backdoor/Weakened Security Claim

> They [GCHQ+NSA) will claim that they need to find every criminal and terrorist at the press of a button, and to do this, they must break encryption, and seize all of our data secretly (Killock, 2014).
>
> Building a version of iOS that bypasses security in this way would undeniably create a backdoor… They have asked us to build a backdoor to the iPhone (Cook, 2016).
>
> They were suggesting, "We have to be able to have lawful access to these devices with a warrant", but that is technically not possible on a secure device. The only way that is possible is if you compromise the security of the device by leaving a back door (Snowden, 2014).

Catastrophic Vulnerability Claim

> They can weaken our encryption methods, by adding backdoors, so they can always decrypt things. The problem with that is it means organised crime can find the backdoor, and they can steal our credit card details, passwords, and everything else that we want to keep safe (Killock, 2014).
>
> In today's digital world, the "key" to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge (Cook, 2016).
>
> We've known that these back doors are not secure. I talk to cryptographers, some of the leading technologists in the world, all the time about how we can deal with these issues. It is not possible to create a back door that is only accessible, for example, to the FBI (Snowden, 2014).

Unrestricted State Surveillance Claim

> It [breaking encryption] also gives the intelligence services unrestricted powers to monitor our communications continuously. Perfect surveillance is a kind of omniscience that most people would not trust ordinary mortals with (Killock, 2014).

> The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices (Cook, 2016).

> What happened was that all of a sudden these massive, behemoth companies realized their data centres—sending hundreds of millions of people's communications back and forth every day—were completely unprotected, electronically naked. GCHQ, the British spy agency, was listening in, and the NSA was getting the data and everything like that, because they could dodge the encryption that was typically used (Snowden, 2014).

These three claims, taken together, serve to technify, securitise and de-politicise state surveillance in cyberspace by constructing the problem as a technical issue, solvable through technical means such as stronger and more widely used encryption. This type of technical solution to state surveillance is an extreme outcome because it restricts state surveillance, even when it is legal and politically authorised. It positions the debate over the limits of state surveillance powers within a technical rather than a political framework, thereby securitising the issue through technification.

Whilst, as Hansen and Nissenbaum explain, technification can hide the political roots of securitisation, in the case of businesses it may also be hiding the economic roots. As Snowden explains, big technology companies realised that his revelations of NSA surveillance had 'hurt their business' and 'no one trusts their products anymore' (Snowden, 2014). Companies such as Apple make a virtue from their claim that their products are more secure and better for privacy than their rivals, and actively market the fact that they cannot respond to government search warrants (Apple, n.d.). How well companies protect data from government requests is measured and scored by organisations such as the Electronic Freedom Foundation (EFF), which campaigns for digital rights. Every year they produce a report, titled 'Who Has Your Back', which ranks technology companies over five different categories. Rankings depend on categories such as how well they publicise government data requests, how much they oppose backdoors and their policies on data retention (Electronic Frontier Foundation, 2015). In the most recent report, Apple received five stars and displays these proudly on its website.

> In its latest "Who Has Your Back?" report, once again the EFF awarded Apple 5 out of 5 stars "commend[ing] Apple for its strong stance regarding user rights, transparency, and privacy" (Apple, n.d.).

Apple's reputation for creating secure products and for providing customer privacy is a significant commercial advantage for their business, so it is clearly in their interests to take actions to defend and promote this reputation as and when they can.

Both the state and the DRC construct cyber threats as technical in nature and then present themselves as the experts sufficiently equipped to articulate these threats and act against them. The state uses its responsibility for national security, its access to technical and institutional expertise (particularly at GCHQ) and its access to secret intelligence information to present itself as the expert authority to speak on issues of cybersecurity. The DRC attempts to undermine the state's authority by criticising their expertise and presenting them as out of touch. It also constructs cyberspace as a technical/human rights issue, which only organisations such as ORG and technical individuals with previous access to insider information can understand. This technification aids securitisation by placing the authority to speak on issues of cyberspace threats in the hands of competing experts. This reduces the opportunity for real substantive political debate and reframes the debate into one of which experts we trust and which we distrust.

3.2 Heuristic Artefacts

Thierry Balzacq describes how heuristic artefacts[13] are used by securitising actors 'to create, or effectively resonate with the circumstances that will facilitate the mobilization of the audience' (Balzacq, 2011, p. 36). They help create storylines and frames through which issues are viewed and facilitate the communication of a threat to an audience by tapping into the audience's existing fears, prejudices and emotions. Cyberspace, perhaps due to its technical and abstract nature, is often discussed and understood using heuristic artefacts. The space aspect of cyberspace is itself a metaphor, dependant on whether you consider non-physical spaces to be 'real'. Biological metaphors such as viruses, worms, infections and cyber-hygiene are commonplace, as are military metaphors such as cyber attack, network

[13] For example, analogies, metaphors, metonymies, emotions and stereotypes.

defences, perimeters and vulnerabilities, or home security metaphors such as backdoors.

As Adriane Lapointe explains, metaphors may 'initially provide insight into the challenges we face in cyberspace, but too often end up as empty labels or catchphrases used by different people to mean different things' (Lapointe, 2011, p. 1). Betz and Stevens also acknowledge 'that metaphors and analogies have utility in describing and explaining socio-technical worlds' but also criticise the application of some metaphors, claiming that 'a martial conceptualization of cyberspace is an important determinant of groupthink and reduces scope for collective problem-solving and creativity' (Betz & Stevens, 2013, p. 158). In other words, the use of military metaphors in cyberspace encourages a particular way of thinking and discourages individual and innovative thinking. Artur de Matos Alves also considers the potential negative consequences of the 'battlefield' metaphor to describe cyberspace and concludes that:

> "… by militarizing and securitizing digital networks, they compromise established mechanisms of trust, tightening surveillance and control at the expense of privacy, anonymity, and net neutrality" (Alves, 2015, p. 401).

To help facilitate the audience's acceptance of the threat, the securitising actor can use several heuristic artefacts, which mediate between the alleged threat and the context of that threat to the audience. This may include the deployment of analogies, metaphors, metonymies, emotions or stereotypes which frame the threat in a particular light. Using negative stereotypes to portray the threat actor may resonate with a particular audience; using military or medical analogies may serve to elevate the threat, and exploiting the audience's emotional response to certain issues may also help to aid securitization. Creating new storylines or playing into existing storylines may also help to frame issues as security threats and convince an audience that extraordinary means are required to counter these exceptional threats.

Metaphors and analogies can aid in the securitisation of issues by both escalating the rhetoric (i.e. war) and by resonating with the audience's existing fears, emotions and prejudices, thereby generating a greater acceptance of the threat (Balzacq, 2011, pp. 9-13). Both the state and the DRC use analogies and metaphors to explain cyberspace. This usage can help to understand and explain different

aspects of cyberspace, but it can also escalate issues and link them to threats, fears and human emotions.

3.2.1 Military Metaphors

Military metaphors are embedded in cybersecurity discourse, and cybersecurity practitioners routinely use military language such as network perimeters, cyber attacks and network defences. The British state also makes common use of these metaphors to articulate cyberspace threats. The 2010 SDSR was the first time in which security had been added to what had previously been the Strategic Defence Review. As a result, threats in cyberspace were included in the Strategic Defence and Security Review and the National Security Strategy, which supported it. This conflation of military and security threats helps to establish threats in cyberspace on an equal footing to military threats. This is supported using military language, which is used to describe these threats. Terms such as 'hostile' and 'weapon' help to support this militarisation, as do direct claims of the threat of 'military attack' through cyberspace.

> Hostile attacks upon the UK from other states (HM Government, 2010, p. 47).

> Address deficiencies in the UK's ability to detect and defend itself against cyber attack – whether from terrorists, states, or other hostile actors (HM Government, 2010, p. 47).

> Some states continue to attempt to gain advantage over us through hostile espionage activity or cyber attack (HM Government, 2010, p. 14).

> Government, the private sector and citizens are under sustained cyber attack today from both hostile states and criminals (HM Government, 2010, p. 29).

> Cyberspace … continues to grow as a terrorist enabler as well as a military weapon (HM Government, 2010, p. 29).

> In times of conflict vulnerabilities in cyberspace could be exploited by an enemy to reduce our military's technological advantage (HM Government, 2011, p. 15).

> Some states regard Cyberspace as providing a way to commit hostile acts 'deniably' (HM Government, 2011, p. 17).

This use of military language positions cyber attacks in the same framework as physical war, a concept which the public can more easily relate to. As war is often characterised as a fight for survival, which legitimises all means to achieve this goal, this positions cyber attack as existentially threatening to the country and helps to legitimise extreme measures to help combat these threats. The DRC also use some military language by routinely referring to how human rights are under attack, but they do so in a much more limited manner than the state.

> Instead of acknowledging their mistakes, politicians are now talking about further chilling our free speech and privacy and introducing measures which attack the concept of human rights (Open Rights Group, 2015).

> DRIP was the last straw for most Britons, it is a clear attack on our privacy (Open Rights Group, 2014).

Although the DRC use the word 'attack' to suggest that rights are being limited or reduced, the state uses the word in a much more direct way, which suggests an actual military threat.

3.2.2 Home Security Metaphors

Whilst the state favours military metaphors to describe cyberspace, which resonate with its mandate to protect the nation's security, the DRC primarily focusses on metaphors that relate to an individual's own personal security. The 'backdoor' metaphor appears routinely in securitising claims made by actors such as Edward Snowden and the Open Rights Group, and is used to imply that technical vulnerabilities, particular encryption protocols, certain legal arrangements or even the existence of certain software, would allow the state, foreign states and criminals to access messages or devices in secret, in a similar manner that a thief could access a house through an open back door.

During Apple's conflict with the FBI, Tim Cook used the backdoor metaphor to argue that the creation of software to allow the FBI gain access to the phone of Syed Farook would constitute a backdoor and make it easier for 'cybercriminals and hackers' to gain access to anyone's iPhone. But he also introduced the analogy of a

'master key' to illuminate the argument that the FBI's request would give them unfettered access to all businesses and everyone's homes.

> [The FBI] have asked us to build a backdoor to the iPhone … In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes (Cook, 2016).

On the surface, the metaphor of the backdoor to describe security vulnerabilities, is less concerning than military metaphors, which are inherently threatening. And as Leontine Jenner claims, backdoors in the physical world are often seen in a positive light when considered an alternative, unofficial point of entry, allowing controlled access for goods to be received, waiters to take a smoke break or friends to visit (Jenner, 2018). As Jenner points out, the backdoor 'is meant to be used only by people who are somehow legitimised to do so.' But the backdoor also 'has associations with illicit means, malicious intent and security threats' and when combined with the concept of the master key it can seem particularly threatening (Jenner, 2018). The concepts of backdoors and master keys carry powerful agency through their association with home security and the implication that their existence could make our homes and our most sacred spaces vulnerable. The backdoor metaphor conjures the image of the state entering our houses without us knowing, and the 'master key' analogy enhances this by insinuating that this could be achieved by the state at will. As a result, home security metaphors can act as powerful aspects of securitising acts, by tapping into our innate fears of threats to our homes, our personal possessions and our loved ones.

The issue of backdoors has now become so successfully securitised as a threat to privacy that there is no need to explain the metaphor for many people to understand its meaning. As Buzan et al explain, securitisation can become institutionalised if a given type of threat is persistent or recurrent. 'The need for drama in establishing securitisation falls away, because it is implicitly assumed that when we talk of this issue we are by definition in the area of urgency' (Buzan, et al., 1998, p. 28). This has been achieved with the concept of backdoors as, for some, once an action such as the FBI's attempt to access an iPhone has been framed as 'constructing a backdoor', the action itself becomes securitised and is considered an existential threat. As such, the actual nature of the vulnerability, technical access or legal request is not considered because it is framed as a backdoor, and backdoors have been institutionalised as inherently threatening.

3.2.3 Biological Metaphors

Biological metaphors are common within cybersecurity discourse and as Betz and Stevens argue, one 'might argue that "virus", in particular, has the power to fascinate and instil fear' (Betz & Stevens, 2013, p. 157). Terms such as virus, infection and worm are used to describe malware, and terms such as anti-virus, quarantine and cyber-hygiene are used to describe solutions. Whilst these terms can resonate with human health concerns, they are usually used more to help describe complex concepts than they are to securitise. Of the terms described above, only cyber-hygiene and anti-virus are used within the UK CSS (and each of them once), and they are used to describe best practice security measures rather than to assist in cyber threat construction.

The DRC also tend to use biological metaphors to help describe technical issues rather than to securitise, although as Betz and Stevens point out, whilst 'the use of biological and medical analogies by elites may not be intended necessarily to elicit negative emotions in the public imagination … it would not be unwarranted to suppose they might be deployed for such a purpose' (Betz & Stevens, 2013, p. 157). One such example is provided in the dispute between Apple and the FBI. During the dispute, Tim Cook claimed that helping the FBI to create software to access this data would create a backdoor which would be like creating the 'software equivalent of cancer' (ABC News, 2016). Instead of using the common metaphor of the computer virus, Cook created an analogy to cancer, the most feared disease in both the UK and the US and a common metaphor for corruption and something that is out of place (Aviva, 2016; Harris Interactive, 2011). In comparing the FBI's request to cancer, Cook massively escalated the threat of the FBI's request and created headlines, which framed the dispute in terms of what could be unleashed upon society if the FBI's request was acquiesced to. Whilst other usage of metaphors contributes in aggregate to the ongoing securitisation of cyberspace, by using the metaphor of cancer, Tim Cook securitised the FBI's request in an instant. Outside of the context of the dispute between Apple and the FBI, the cancer metaphor has not been reused. Its potency relates to its shock factor and its extreme escalation of the threat.

3.2.4 Darkness, Shadows and Silence

Whilst military metaphors are used mainly by the state, and home security metaphors are used extensively by the DRC, metaphors of darkness are extensive throughout the cybersecurity discourse. Metaphors relating to darkness and silence

are common within cybersecurity literature and are used frequently in the construction of cyberspace as a threatening place. ‘Dark Net’ is used frequently to refer to the part of the Internet, which is made more secure (and potentially less accessible by the state) through onion routing technology. The ‘Black Phone’ is designed to provide privacy and terrorists are said to be ‘going dark’ by operating securely online.

As demonstrated by Glasgow University’s Mapping Metaphor project, metaphors of darkness are strongly connected with the negative concepts of ‘death’, ‘moral evil’ ‘emotional suffering’ ‘anger’, ‘destruction’ and ‘fear’. But they are also strongly connected to ‘lack of knowledge’, ‘secrecy and concealment’ and ‘disorder’ (Glasgow University, n.d.). Darkness relates to danger and a fear of the unknown.

In the construction of state surveillance as a threat to privacy, metaphors of darkness are used to describe the organisations and people who conduct surveillance, the methods they use and the lack of oversight over these processes. The day after the Guardian announced the Snowden disclosures, Snowden described surveillance operatives and the systems they used as shadowy.

> I grew up with the understanding that the world I lived in was one where people enjoyed a sort of freedom to communicate with each other in privacy, without it being monitored, without it being measured or analyzed or sort of judged by these shadowy figures or systems, any time they mention anything that travels across public lines (Snowden, 2013).

The ORG also apply the metaphor to describe not just those in the security services, but also to anyone in government or private industry who support these activities. The space in which state surveillance takes place is also described in terms of darkness as ‘the realm of the shadowy world of spies’ (Open Rights Group, n.d., p. 15).

> After the invasive and over-reaching Communications Data Bill was shelved in the UK at the start of May, it's already being re-animated by politicians with strong connections to the shadowy world of the security services (Open Rights Group, 2013).

> Whatever the colour of the government, shadowy figures in the upper ranks of the civil service will be pushing for measures like this and ORG will be ready to oppose them (Open Rights Group, 2009).

> DPI is already used by intelligence agencies to reconstruct traffic such as webmail from the data they intercept off high-speed links. Reference 1 describes some of the shadowy firms and deals in this space (Open Rights Group, 2009).

> GCHQ and the NSA subverted the operations of Swiss company Crypto AG, a provider of strong crypto tools that could be bought by third party countries. But those operations remained within the realm of the shadowy world of spies (Open Rights Group, n.d.).

As well as characterising the practitioners, systems and supporters of state surveillance as dark and shadowy, the ORG also use the metaphor of darkness to raise the threat of lack of parliamentary oversight of the intelligence agencies.

> The revelations, made possible by the whistle-blower Edward Snowden, over the past few months have shown without doubt that Parliament has been kept in the dark about the powers and capabilities of GCHQ to conduct mass surveillance (Open Rights Group, 2013).

Academic literature has also perpetuated the use of the darkness metaphor, usually relating it to state surveillance. As Deibert puts it, 'there is a dark side to cyberspace-hidden contests and malicious threats that is growing like a disease from the inside-out' (Deibert, 2012, p. 261). Other authors have also used the metaphor of darkness to describe the practices of state surveillance in cyberspace, including Evgeny Morozov, who argues in his book 'The Net Delusion: The Dark Side of Internet Freedom' that the cyber-utopian belief that the Internet is liberating is wrong and that authoritarian governments are using cyberspace to suppress their populations (Morozov, 2012).

Interestingly, the portrayal of GCHQ and NSA staff as 'shadowy figures' is perhaps aided by the organisations themselves, who are protective of their staff and do not routinely reveal their identities. On the GCHQ website, under the heading of 'Meet our Team', there is an image of four figures representing four different roles in GCHQ (See Figure 3.1). To hide the identity of GCHQ staff members, the figures are

shown as silhouettes. A similar methodology is used in the 'Minority Report' campaign, which is designed to demonstrate the ethnic diversity of GCHQ staff. The

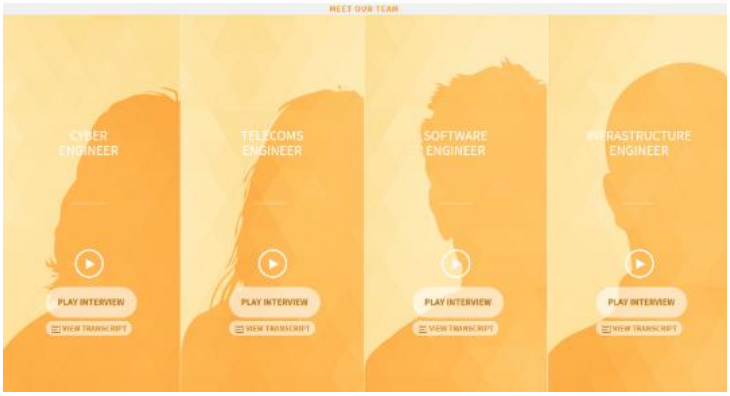

Figure 3.1: Shadowy employees at GCHQ

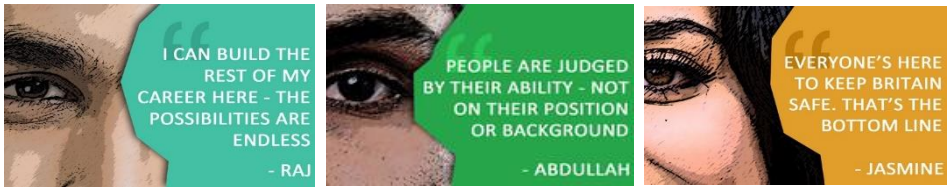

Figure 3.2: Concealed faces within GCHQ's 'Minority Report' campaign.

images used to represent these diverse staff members are cartoonised and partially hidden (See Figure 3.2. Whilst the identity of the individuals is hidden, their sex and ethnic origin are not. Further hints of ethnic origin are also delivered by the labelling of these individuals by their first names, most of which are of non-British origin. Whilst the campaign may be effective in highlighting the ethnic diversity of GCHQ staff, it simultaneously strips the staff of all identity but their ethnic origin and sex, making them appear shadowy and hidden and potentially also suspicious, dangerous and threatening.

Metaphors of darkness are also used to support claims that national security is threatened. They are used to describe areas of cyberspace itself and to support the claim that the state is restricted in its ability to provide law, order and governance in this space. As previously discussed, the FBI routinely use the phrase 'Going Dark' to explain the impact of encryption and other security measures on their ability to investigate and prevent crime. This connects the concept of being left in the dark (i.e. lacking information) with the concept of a dark place (i.e. somewhere dangerous and fearful).

> If the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place (Comey, 2014).

These concepts are also projected by British government and law enforcement figures, although the term 'Going Dark' is replaced by the concept of cyberspace becoming 'dark and ungoverned' (Cameron, 2014; Hogan-Howe, 2014). Director of MI5, Andrew Parker, has also warned of the increased threat of terrorism relating to a reduced ability of the security services to investigate cyberspace activity if 'parts of the radar go dark'. He also warns that 'the dark places from where those who wish us harm can plot and plan are increasing' (Parker, 2015). Darkness in cyberspace, it is argued both facilitates the 'bad guys' whilst restricting the ability of the 'good guys' to investigate.

Into this darkness, the state and surveillance agencies portray themselves as the

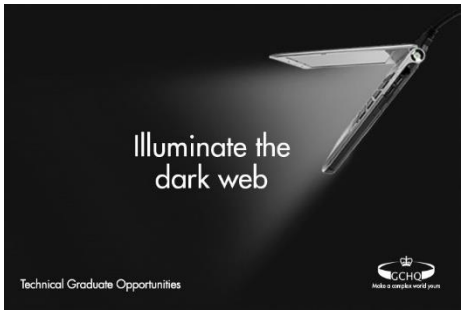

Figure 3.3: GCHQ recruitment advert

Figure 3.4: 'Anonymous' imagery

bringers of light. In an announcement on government efforts to tackle child abuse, David Cameron claimed that the government 'are shining a light on the web's darkest corners' and GCHQ recruitment adverts encourage applicants to join to 'illuminate the dark web' (See Figure 3.3). The use of a raised laptop bringing light to a dark space has hints of the biblical creation story, with God bringing light to a dark world. The message, it would seem, is that cyberspace is dark and scary but with the right tools the state can shine a light and make it safe and secure for everyone.

In parallel with GCHQ's portrayal of themselves as shadowy, some elements of the DRC also represent themselves in this manner. The Anonymous collective, for example, uses a logo of a man in a dark suit with a question mark in place of a head, and use a Guy Fawkes mask from the film 'V for Vendetta' to conceal its supporter's identity (See Figure 3.4). The group styles itself as 'anonymous' and secret and describes itself as 'operating in the shadows' (Anonymous, 2013).

Both sides of the debate use metaphors of darkness to help describe both the threats that are said to exist in cyberspace and the difficulties in combatting these threats. This use of darkness portrays cyberspace as unknown, troubling and dangerous, and this taps into our innate fear of darkness and the unknown. Jim

Killock describes how he thinks that this fear of the unknown might play into GCHQ's own threat modelling:

> If there's something [GCHQ) don't know then there's a threat they don't know about therefore not knowing is a threat in itself (Killock, 2016).

But when talking of his fear of state surveillance in cyberspace, he also indicates that it is not knowing that drives his own fear.

> You can never know what the sinister motivations [of GCHQ] might be because those motivations exist in the heads of people, not necessarily in policy documents (Killock, 2016).

Efforts are made to alleviate fears of the dark and the unknown in cyberspace, such as the Berkman Centre's report into the illegitimacy of the 'Going Dark' metaphor, but it would seem that powerful metaphors of darkness, fear and the unknown are difficult to counter (Berkman Center, 2016). The state's claim to be able to illuminate the darkness of cyberspace may be particularly effective as it plays into an established metaphor in society that evil is represented by darkness and shadow, and must be confronted by goodness, which is represented by light (Benjamins, 2013).

It is interesting that whilst both sides of the debate construct cyberspace threats as dark and threatening, they also portray themselves as dark, secret and hidden. For GHCQ, alongside other intelligence agencies, this is largely a result of practical considerations and the necessity to protect the identity of staff. But there are also some positive representations of security agencies, that use darkness metaphors, such as the portrayal of spies, as secretive, glamorous and intriguing, and it is possible that the security agencies consciously or subconsciously perpetuate these images. For the DRC transparency is usually promoted, but groups like Anonymous use the metaphor of darkness to convey themselves as hidden, omnipresent, uncatchable and therefore powerful.

As we often mistrust that which is hidden, secret and dark, darkness metaphors are used to construct cyberspace as an unknown, dangerous and threatening, place.

3.3 CONNECTED SECURITISATIONS

Whilst issues can be securitised in isolation, this securitisation can be more effective if the issue is linked to wider security concerns. For example, the issue of graffiti in an area may become more threatening if linked to concerns over crime in general, the presence of gangs and ultimately to the possible breakdown of security (Keizer, et al., 2008).

The NSS, SDSR and UK CSS contribute significantly to the securitisation of UK cyberspace by directly linking cybersecurity to several other securitisations and referent objects. The inclusion and prominence of cyberspace in the NSS and SDSR and the publication of a separate UK CSS, help to establish cyberspace as a significant threat to national security. By rating cyber attack as a tier one national security threat, alongside the already securitised concepts of terrorism, environmental catastrophe and war, cyberspace is presented by association as equally threatening. Whilst it was the threat of cyber attack (hostile attacks upon UK cyber space by other states or large-scale cybercrime) that was assessed to be a tier one threat, these documents frequently drop the 'attack' suffix and referred instead to 'cyber' as the concern.

> Our strategy sets clear priorities – counter-terrorism, cyber, international military crises and disasters such as floods (HM Government, 2010, p. 5).

This use of cyber as a prefix, which can be placed before everyday threats (e.g. cyber-terrorism, cyber-espionage, cyber-war, cyber-bullying), helps to construct cyberspace itself as the threat, rather than the forces who wish to exploit it for their own gain. Hence, cyberspace itself becomes a threatening place, inextricably intertwined with terrorism, crime and warfare.

Whilst the NSS, SDSR and CSS link cyberspace to several different threats including crime, abuse, espionage and war, the most prominent connection is with terrorism:

> Terrorists use cyberspace to organise, communicate and influence those vulnerable to radicalisation (HM Government, 2010, p. 30).

> Cyberspace is already used by terrorists to spread propaganda, radicalise potential supporters, raise funds, communicate and plan (HM Government, 2011, p. 15).

The connection between terrorism and cyberspace has been highlighted several times by the US and UK governments following high profile terror attacks. The Intelligence and Security Committee report into Lee Rigby's death highlighted how a social media platform[14] was used to by Michael Adebowale to communicate with an extremist linked to Al Qaeda in the Arabian Peninsula (AQAP) about his plot to kill a British soldier. The implication that Facebook was used to facilitate the attack made front page news.

> Facebook hosted Lee Rigby death chat ahead of soldier's murder (BBC News, 2014).
>
> "Facebook has blood on its hands" for failing to raise alarm, says Lee Rigby's sister (The Independent, 2014).

As previously discussed, GCHQ Director Robert Hannigan reinforced this link by arguing that social networks were the 'command and control network of choice for terrorists' (Hannigan, 2014). During the dispute between Apple and the FBI, US Senator Tom Cotton claimed that 'Apple is becoming the company of choice for terrorists, drug dealers and sexual predators of all sorts' (Cotton, 2016).

The state also connects cyberspace threats with the threat of anarchy and lawlessness. Several government actors have claimed that security measures such as encryption and the difficulty of accessing online data are leading to a breakdown of law and order.

> In a democracy we cannot accept any space - virtual or not - to become anarchic where crime can be committed without fear (Hogan-Howe, 2014).

The construction of a connection between terrorism, anarchy and cyberspace provides a shortcut to securitisation by hijacking the emotions and fears relating to memories of 11 September 2001 in the US and 7 July 2005 in the UK, and applying them to cyberspace. A similar practice is also undertaken by those arguing that the state is a threat to human rights in cyberspace. This most prominent construction has been the association of state surveillance in cyberspace with authoritarianism and totalitarianism. The Pen Surveillance Metaphor Mapping Project studied 133 news articles in the weeks following the Snowden disclosures to investigate the metaphors which were used to help explain concepts of surveillance (PEN America,

[14] This was not officially named although it was widely reported by the press to be Facebook

2014). Whilst metaphors for collecting were most common, metaphors for the literary theme were second, and all three of these themes related to Orwell's 1984 (Orwell, Big Brother and Dystopian). In addition, authoritarian metaphors were also common, including uses of the terms totalitarian, Stasi, Nazi Germany, and police state.

Examples of connections between state surveillance and Nazi Germany include a comparison of Hitler's suspension of mail and telephone privacy with that of the NSA, and a comparison of the NSA's claim to be acting in the interests of its citizens with that of the Stasi (Binney, 2016; Greenslade, 2013). The Russian Foreign Minister also compared the NSA activities with the oppressive regime of Stalin-era Russia (Lavrov, 2013).

By far the most common association was with George Orwell's Dystopian Novel 1984 (See Figures 3.5 and 3.6). In his alternative Christmas message on the UK's Channel 4, Snowden claimed that today's surveillance was worse than Orwell's vision.

> Great Britain's George Orwell warned us of the danger of this kind of Information. The types of collection in the book, microphones and video cameras' TVs that watch us are nothing compared to what we have available today (Snowden, 2013).

This view was echoed widely within the discourse. In 2015, the UN privacy chief also compared NSA and GCHQ surveillance to that in the novel 1984. He claimed that British and US surveillance was 'worse' than in 1984 as you could not escape to the countryside to evade it like the character Winston in the novel. He also directly linked the controlling nature of Orwell's vision with today's surveillance technologies.

Figure 3.5: Example of 1984 references

Figure 3.6: Another Example of 1984 references

> Orwell foresaw a technology that was controlling. In our case we are looking at a technology that is ever-developing, and ever-developing possibly more sinister capabilities (Cannataci, 2015).

Digital rights organisations also frequently link surveillance to totalitarianism. In November 2016 the Open Rights Group held an event titled 'Digital Dystopias: Orwell's 1984 and the Internet Age. It was described as

> a session on surveillance and totalitarianism in literature, and how the nightmarish world of George Orwell's '1984,' as well as the work of other writers, can still be seen as relevant for the digital age (Open Rights Group, 2016).

The digital rights organisation 'Big Brother Watch' constructs the connection between Orwell and state surveillance by using the Orwellian phrase 'Big Brother' within their title. As indicated in Figures 3.5 and 3.6, the phrase '1984 was not supposed to be an instruction manual' has also become popular in anti-surveillance culture.

The construction and exploitation of a link between state surveillance and authoritarianism can also be witnessed in contemporary affairs following the election of Donald Trump (who is widely considered to be an authoritarian) as President of the US. The Executive Editor of the ORG, Jim Killock, connected Trump to GCHQ by warning that he would now have effective control of the organisation.

> Donald Trump has effective control of GCHQ's technology and full access to their data collection. GCHQ and NSA are joined at the hip (Killock, 2016).

The Guardian also made this connection by reporting on fears of Donald Trump 'running' the global surveillance network. They quote former NSA whistle-blower Thomas Drake, who said that surveillance powers were

> ripe for further abuse under an autocratic, power-obsessed president. History is just not kind here. Trump leans quite autocratic. The temptations to use secret NSA surveillance powers, some still not fully revealed, will present themselves to him as sirens (The Guardian, 2016).

The construction of a link between UK/US state surveillance with historical, fictional and future (in the case of Donald Trump) totalitarian regimes aids in the

securitisation of cyberspace surveillance by tapping into existing institutional fears and hatred of these forms of governance.

A clear parallel can be drawn between the way in which those securitising cyberspace use institutionalised threats such as terrorism to bolster their claim, and those who securitise state surveillance use institutionalised threats such as totalitarianism to boost their claims. In both cases, issues are constructed as particularly threatening because they are linked to an already securitised issue.

3.4 CONCLUSION

The state constructs the use of cyberspace by terrorists and criminals as an existential threat to law and order, which requires huge increases in spending and powerful intelligence capabilities to resist. The DRC constructs state surveillance as an existential threat to freedom, privacy and democracy, which requires the curtailing of state powers, increased enforcement of security measures and resistance by technology companies to government data requests. Hypersecuritisation, everyday security practices, technification, heuristic artefacts and connected securitisations play a major role in each of these securitisations. Whilst these competing securitisations have different goals, their methods are very similar. The parallels between these competing securitisations are highlighted in Table 3.3.

Concept	National Security Threat	State Surveillance Threat
Hypersecuritisation	The threat to national security is huge, escalating and growing in significance. Due to encryption, outdated legislation and blocks by technology companies, the state are unable to combat this threat and this will eventually lead to total insecurity.	The State Surveillance Threat is huge, escalating and growing in significance. Due to state secrecy and a lack of oversight, the public are unable to combat this threat and this will eventually lead to insecurity and a total lack of privacy.
Technification	Cyberspace threats are technical and issues of	Cyberspace threats are technical and issues of

	national security, which should be articulated and combatted by the state, which has access to secret threat information and, through GCHQ, unrivalled technical expertise.	human rights and should be articulated and combatted by digital rights organisations, which have both human rights and technological expertise.
Everyday Security Practices	Cybercriminals affect you, your family and your workplace.	State surveillance affects you, your family and your workplace.
Heuristic Artefacts	Parts of cyberspace are dark and dangerous, which makes it impossible for law enforcement to combat crime and protect the public	Surveillance agencies are dark and dangerous and their secretive nature stops them from being scrutinised and stopped from harming the public
Connected Securitisations	Cyberspace is threating because it facilitates terrorism and risks anarchy	Cyberspace is threatening because it facilitates totalitarianism

Table 3.3: Parallels between Cyberspace Securitisations

Whilst each of these threat constructions may have arisen independently to the other, they are now inextricably linked. The openness of cyberspace is considered a threat to law and order, which results in increased state activity in cyberspace, which is considered a threat and leads to efforts to re-establish its openness, which continues the cycle. There is also no clear start or endpoint to this cycle. As is the case in the security dilemma, moves by one side lead to the other responding with similar measures, producing increased tensions that create conflict, even when no side really desires it. This is coupled with the view that any concession or weakness cannot be tolerated because the threat is just too great. Any vulnerability is a backdoor, and any backdoor is accessible to anyone and therefore threatens us all. All enhanced security measures deny the state the access to communications that they need and will lead to anarchy, which threatens us all.

This hypersecuritising rhetoric appeared to hit a peak during the conflict between Apple and the FBI. If the FBI won then Apple said that this would be as bad as the software equivalent of cancer, and if Apple won then FBI supporters said it would

lead to increases in terrorism, drug trafficking, kidnapping and child pornography. The state was pitched against the world's most valuable brand, technical experts were pitched against technical experts, terrorism was pitched against totalitarianism, and security was pitched against privacy. Examples of these parallel constructions can be seen in Table 3.4 (Cook, 2016; Cook, 2015; Cotton, 2016).

Apple	**Concept**	**FBI**
The implications of the government's demands are chilling.	Hypersecuritisation	Apple is becoming the company of choice for terrorists, drug dealers, and sexual predators of all sorts
For years, cryptologists and national security experts have been warning against weakening encryption	Technification	
The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge	Everyday Security Practices	Apple chose to protect a dead ISIS terrorist's privacy over the security of the American people
The only way to gain access to this phone would be to write a piece of software that we view as the software equivalent of cancer They have asked us to build a backdoor to the iPhone.	Heuristic Artefacts	The Executive and Legislative Branches have been working with the private sector with the hope of resolving the 'Going Dark' problem

The FBI is proposing an unprecedented use of the All Writs Act of 1789 to justify an expansion of its authority. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data.	Connection to the securitised threat of totalitarianism	The problem of end-to-end encryption isn't just a terrorism issue. It is also a drug-trafficking, kidnapping, and child pornography issue

Table 3.4: Parallel threat constructions

Whilst much of the rhetoric surrounding this case was escalatory, each side did also try to counter the other's securitisation. James Comey claimed that all the FBI wanted was access to one phone and Tim Cook argued that Apple had helped the FBI in every way they could.

> We simply want the chance, with a search warrant, to try to guess the terrorist's passcode without the phone essentially self-destructing and without it taking a decade to guess correctly. That's it. We don't want to break anyone's encryption or set a master key loose on the land (Comey, 2016).

> The FBI asked us for help in the days following the attack, and we have worked hard to support the government's efforts to solve this horrible crime. We have no sympathy for terrorists (Cook, 2016).

But within the context of these competing securitisations and headlines warning of software-cancer and terrorism, it is clear that it is far harder to de-securitise an issue than it is to securitise it. How this can be achieved will be discussed throughout Chapters 5-7.

4 THE CYBER SECURITY DILEMMA

Chapters 2 and 3 discuss how cyberspace has become securitised by members of the state and the DRC, who have leveraged their power positions and employed the grammars of hypersecuritisation, everyday security practices and technification, to convince a range of audiences of threats to national security and digital rights. But these parallel threat constructions do not just mirror each other but are also generated and fuelled by each other. The DRC resist state surveillance because they fear the actions of the state, and the state seeks to increase its surveillance capabilities because of resistance to its existing techniques. As each side makes a move, the other makes a counter move. This scenario conforms to the international relations theory of the security dilemma.

This chapter will use the framework of the security dilemma to help understand the securitisation of cyberspace. Using this framework, the characteristics of the CSD will be investigated and the reasons for its intensity will be explored. This chapter will first introduce the concept of the security dilemma before considering its previous applications to cyberspace. It will then consider how well characteristics of the security dilemma match those of traditional security dilemmas, and why the CSD is so intense.

4.1 THE SECURITY DILEMMA

The security dilemma is a term coined by the American scholar John Herz, who used it to describe the predicament of two states who feel they must acquire more and more power to defend against the other.

> Groups and individuals … are concerned about their security from being attacked, subjected, dominated, or annihilated by other groups and individuals. Striving to attain security from such attack, they are driven to acquire more and more power to escape the impact of the power of others. This, in turn, renders the others more insecure and compels them to prepare for the worst. Since none can ever feel entirely secure in such a world of competing units, power competition ensues, and the vicious circle of security and power accumulation is on (Herz, 1950, p. 157).

Independently, the English philosopher Herbert Butterfield also developed ideas on the security dilemma, which he described as the 'absolute predicament and irreducible dilemma' (Butterfield, 1951, p. 19). Butterfield argues that 'the greatest war in history can be produced without the intervention of any great criminals who might be out to do deliberate harm in the world. It could be produced between two powers, both of which were desperately anxious to avoid a conflict of any sort' (Butterfield, 1951, pp. 19-20).

Butterfield describes the security dilemma as a tragedy because it has the power to turn positive intentions into devastating consequences. Butterfield claims that the ultimate source of the security dilemma is fear, whilst Herz describes it as uncertainty and anxiety (Herz, 1950).

> Whether man is 'by nature' peaceful and cooperative, or aggressive and domineering, is not the question ... It is his uncertainty and anxiety as to his neighbors' intentions that places man in this basic [security] dilemma (Herz, 1950, p. 157).

Robert Jervis argues that this uncertainty and anxiety arises from the anarchical structure of international politics. 'The lack of an international sovereign', he explains, 'not only permits wars to occur, but also makes it difficult for states that are satisfied with the status quo to arrive at goals they recognize as being in their common interest' (Jervis, 1978, p. 167). Anarchy refers to the lack of an authority above that of the nation state and, according to Jervis, it is this lack of higher power to enforce the law that discourages states from co-operation. Shiping Tang builds upon the work of Butterfield, Herz and Jervis, (which he terms the BHJ formulation) and introduces three aspects that he considers to be essential to the security dilemma: anarchy which leads to fear and uncertainty, a lack of malign intentions on either side, and some accumulation of power (Tang, 2009).

The security dilemma is often used to explain military arms races and, in its most extreme form, can lead to accidental wars that were brought about by the logics of fear, suspicion and mutual distrust. As with securitization, the existence of an 'objectively real' threat is not a precondition for the existence of a security dilemma. Rather, it suffices that each side believes a threat exists. Two countries may engage in an arms race because they consider their adversary's actions to be offensive in nature, whilst they consider their own actions to be defensive.

4.1.1 Dilemmas and Paradoxes

According to Ken Booth and Nicholas Wheeler, the security dilemma is really comprised of two dilemmas, which together can result in a security paradox, where measures taken by an actor to increase its security ultimately leads to greater insecurity (Booth & Wheeler, 2008). The first dilemma is the dilemma of interpretation; that is, how should one state interpret the actions of another? The second is the dilemma of response; how should an actor respond to the actions of the other?

4.1.1.1 Dilemma of Interpretation

According to Booth and Wheeler, the dilemma of interpretation relates to the difficulty that states face in interpreting the intent, motivation and capabilities of other states. In conditions of unresolvable uncertainty, a state must decide whether the military capabilities of another state are solely defensive or whether they are intended for more offensive purposes. The dilemma is driven by the inability of states to put themselves into the minds of their counterparts and understand their motives and intentions. This difficulty derives from the philosophical problem of 'Other Minds', which addresses the fundamental human inability to know the mind of another (Windsor, 1990; Hollis & Smith, 1990). An additional problem is the inherent ambiguity of weapons and other technologies. Tanks, aircraft and soldiers are largely dual-use in nature, deployable for both offensive and defensive purposes. If a state strengthens its army, how can another state tell whether this is for defensive or offensive purposes?

4.1.1.2 Dilemma of Response

Following the dilemma of interpretation is the dilemma of response; how should a state respond to the seemingly hostile actions of another? Should it provide a show of force to deter the other from attacking or should it signal its benign intentions in an effort to reassure the other side? A state's response to the security dilemma is of utmost importance to its security. Misjudge hostile activity by another state to be benign and defensive and a country risks annihilation; misjudge defensive activity as hostile and a state risks a catastrophic conflict. If each side determines that the other is hostile then a spiral of insecurity may ensue as each seeks to boost their own security whilst simultaneously making the other feel more vulnerable. The result is a security paradox, where an increased focus on security actually results in greater insecurity (Booth & Wheeler, 2008).

The security dilemma is often invoked to help explain negative outcomes in International Relations such as arms races and war, but the existence of a security dilemma does not always lead to a negative security spiral. The Cold War is a classic security dilemma that resulted in an arms race but ultimately ended short of war when each realised the predicament they were in. Insecurity and fear of the other drove the US and the Soviet Union towards a spiralling arms race that initially resulted in greater insecurity for both, but when Mikhail Gorbachev became the leader of the Soviet Union in 1985, he took steps towards ending this harmful spiral. He acted to reassure the US of his peaceful intent and made several conciliatory moves, which created room for negotiation and resulted in reciprocal moves. The disarmament programme following the Good Friday agreement in Northern Ireland is another good example, where each side weakened their own strength through disarmament but ultimately achieved greater security. In both examples, the worst consequences of the security dilemma were avoided, although animosity and distrust were not completely diffused.

The most significant criticism of the security dilemma challenges the idea that insecurity is behind international conflict and suggests instead that greed is the main source of war. States engage in war to change the status quo, and may either seek to gain territory and resources or to eliminate another state, ideology or race. Patrick Glynn, for example, argues that the First World War is best explained by German greed and desire to expand rather than insecurity, as is claimed by others (Glynn, 1992). It is difficult to challenge this idea empirically due to the opacity of the causes of war, but for adherents of the security dilemma the existence of 'greedy states' does not negate the security dilemma, it just becomes less important. As Glaser explains, the dilemma still applies because even greedy states can feel insecure, but 'the security dilemma is of less significance when the state's adversary is greedy' (Glaser, 1997, p. 190).

4.2 Beyond Inter-State Conflict

The conflict between the Digital Rights Community (DRC) and the British state over issues of privacy and surveillance would appear to be far removed from the traditional applications of the security dilemma in international relations, but the concept has proven useful to help understand other sub-state conflicts. In his 'Burglar Paradox' thought experiment, game theorist Thomas Schelling describes how a confrontation between himself and an intruder can escalate into a tragic

outcome because the security measures taken by each side appear threatening to the other (Schelling, 1960).

> If I go downstairs to investigate a noise at night, with a gun in my hand, and find myself face to face with a burglar who has a gun in his hand, there is a danger of an outcome that neither of us desires. Even if he prefers to just leave quietly, and I wish him to, there is danger that he may think I want to shoot, and shoot first. Worse, there is danger that he may think that I think he wants to shoot. Or he may think that I think he thinks I want to shoot. And so on. 'Self-Defense' is ambiguous, when one is only trying to preclude being shot in self-defense (Schelling, 1960, p. 207).

Schelling's Burglar Paradox was later used by Baliga and Sjöström to demonstrate how arms races are inevitable in systems of incomplete knowledge of the preferences of the other (Baliga & Sjostrom, 2004). The burglar paradox is derived from the same issues as Herz's Security Paradox; the ambiguity of defensive/offensive weapons, the difficulty entering the other man's counter fear and the logic that actions taken to increase self-defence can ultimately leave you more vulnerable. Whilst Schelling applies the security dilemma to everyday life, several authors have also extended the concept beyond intrastate conflict and into the domestic political sphere.

Barry Posen was the first to apply the security dilemma to internal problems within states (Posen, 1993). He argues that the security dilemma can be applied to intrastate problems when similar conditions exist to those between states in the international system. Ethnic conflict can be fuelled by the security dilemma when states no longer function effectively. As communities begin to take responsibility for their own security, they can cause anxiety in others, leading to spiralling insecurity and conflict. Stuart Kaufman also applies the security dilemma to ethnic conflict, arguing that once governments have lost control, ethnic groups can take on the attributes of sovereignty.

> Strictly speaking the security dilemma should not apply to contending ethnic groups within a state, because they rarely find themselves in a situation of complete anarchy. Anarchy can be approximated, however, if ethnic groups effectively challenge the governments legitimacy and control over its territory. If anarchy

> reaches the point where the government cannot control its territory effectively enough to protect its people, while ethnic-based organizations can, then the ethnic organizations have enough of the attributes of sovereignty to create a security dilemma (Kaufman, 1996, p. 151).

Philip Cerny takes the concept of intrastate security dilemmas a step further by introducing the concept of the New Security Dilemma (NSD) to replace the Traditional Security Dilemma (TSD) (Cerny, 2000). He argues that the end of the Cold War and the emergence of globalization has increased the likelihood of challenges to the state from non-state, sub-state and trans-state actors.

> The challenges thrown up in the twenty-first century in the form of the New Security Dilemma are likely to significantly reduce the effectiveness of traditional state-based and state-systemic approaches in the stabilization of international politics. Where it is not primarily states that defect[15] from interstate balances of power, but rather a range of transnational and subnational actors and structures, then interstate alliances and other traditional means of re-equilibrating the balance will be insufficient to control those defections (Cerny, 2000, p. 645).

Cerny draws on the historical analogy of neo-medievalism, which suggests that the traditional model of powerful nation states is gradually being replaced by features normally associated with the medieval world. These include competing institutions, fragmented loyalties and identities, and the spread of grey zones - areas and social contexts where the rule of law does not apply. Cerny argues that the emergence of transnational governance from international institutions, policy communities, advocacy coalitions and regulatory bodies, has led to insecurity for the state and conflict between state and non-state actors.

> The notion of a vicious circle inherent in the traditional Security Dilemma is transposed into the New Security Dilemma, but at an entirely different level. To begin with, attempts to address insecurities through traditional forms of state power, especially hegemony, create further insecurities that provoke backlashes.

[15] Cerny uses this term in the game theoretical sense. In game theory players can choose to co-operate to gain mutual benefits or defect to pursue individual gain.

> These backlashes in turn draw both states and nonstate actors farther into the quagmires of ethnic and religious conflict, warlordism, and tribalism, ineffective or collapsed states, and ever-increasing calls on military, political, and economic resources. Such responses simply provoke further resentment, frustration, and hopelessness, and breed endemic low-level conflict. Supposedly hegemonic powers are thus sucked into a widening security gap of their own making (Cerny, 2005, p. 18).

Whilst Cerny applies his concept of the NSD to the issue of terrorism, there are also some clear parallels with cyberspace. Cerny highlights the Internet as one of the factors which helps to undermine traditional identities and his reference to neomedieval grey zones, inaccessible to the rule of law, parallels the concept of the dark web and areas of cyberspace that are inaccessible to the state (Cerny, 2005, p. 19). Digital rights organisations such as the ORG and the EFF are examples of Cerny's advocacy coalitions who undermine traditional state governance and provoke conflict with the state. Cerny also argues that terrorism 'often actually gains sympathy, adherents, and momentum from the attempts of states to repress it' and this can also be seen in cyberspace (Cerny, 2005, p. 19). State efforts to protect National security through state surveillance often creates a backlash and generate sympathy, adherents and momentum for the cause of digital rights.

4.3 The Cyber Security Dilemma

Traditional security dilemmas exist between two equivalent actors (states) who each fear the other, whereas the CSD exists between the state and the DRC. Whilst many within the DRC fear the threat of an authoritarian state, the state does not fear the DRC directly; instead, different elements of the state either fear the undermining of their own authority and legitimacy or fear action by the DRC that could hamper their ability to combat terrorism, organized crime and other threats. Unlike with traditional state-based security dilemmas, the sides are not predetermined or well defined. Instead of geographical separation, the CSD relies on the ideological separation of those who support efforts to improve national security and those who support greater digital rights. These are comprised of a loose collective of civil rights activists, technologists, industry representatives, academics, politicians and members of the public.

As with traditional security dilemmas, opinions on surveillance and digital rights exist across a spectrum, but these opinions coalesce around two strong ideologies that each view the other as threatening. Some privacy-enhancing technologies such as end-to-end encryption are considered threatening to national security, whilst some national security measures such as surveillance are considered threatening to privacy. Whilst each side is focussed on their own security interests, their actions appear threatening to the other, which leads to an escalating arms race between the state and the DRC. The state uses legislation and technical capabilities to maintain and extend its ability to gain access to data, which helps it to protect national security, whilst the DRC uses legislation and technical tools such as encryption to protect individual privacy. As each measure appears threatening to the other, the two sides inadvertently perpetuate a damaging arms race and spiralling insecurity.

4.3.1 Existing Literature

Several authors apply the security dilemma to cyberspace. Ben Buchanan applies the concept to state on state hacking, Nicholas Rueter applies it to cyber warfare and Myriam Dunn Cavelty applies it to the conflict between national security and individual rights.

Ben Buchanan considers the offensive/defensive information problem with regards to state hacking in cyberspace (Buchanan, 2016). He argues that whilst state hacking may appear to be an offensive pursuit, such activity is often driven by defensive requirements. As he puts it: 'two nations, neither of which seeks to harm the other, but neither of which trusts the other, will often find it prudent to penetrate each other's systems' (Buchanan, 2016, p. inside cover). One nation's attempt to secure itself through hacking and learning about the threat from the other results in escalating tensions, increased hacking and less security for all. When discussing solutions to the CSD, Buchanan criticises what he calls the 'mistaken belief that one or two strategic or technological big-ticket innovations will dramatically improve a state's prospects and solve the crisis of the day' (Buchanan, 2016, p. 157). Instead, he suggests that there is no single answer to the CSD, which must be addressed through multipronged efforts that initially establish stability, start to build trust and then begin to minimise the risks of misinterpretation. These include initial efforts to improve the core baseline

defences of each nation, efforts to advance bilateral trust[16] and mutual contributions to system-wide security[17].

Nicholas Rueter considers a similar CSD between states but focusses on the prospect of cyber warfare (Rueter, 2011). He argues that cyberspace is particularly prone to the security dilemma because the offense-defence balance leans towards offense (i.e. it is easier to attack than to defend in cyberspace) and that offense-defence differentiation is extremely difficult (i.e. it is extremely hard to determine whether a state's investment in cyber capabilities is designed for offensive or defensive purposes). This is compounded by the difficulties in gathering intelligence on another state's capabilities, as these generally exist in the virtual world and cannot be physically evaluated in the same way that tank and aircraft numbers can. Whilst describing the situation as grim, Rueter suggests three ways in which the CSD can be improved. The establishment of international institutions and norms could help to facilitate international co-operation in cyberspace and help improve trust between states who currently fear each other's intentions. Technological developments could also help by changing the balance between offence and defence, making it costlier to attack than defend and reducing the fear between states. And finally, states could better signal their offensive or defensive intentions through their doctrine and organisational structures, increased transparency over cyber warfare programs and clear delineation between offensive and defensive units.

Myriam Dunn Cavelty notes that despite huge efforts and vast spending on cybersecurity, the approach is not working and cyberspace appears to be becoming more insecure (Cavelty, 2014). She describes this as a security dilemma between the state and the public. Unlike with traditional conceptualisations of the security dilemma, which place the blame for the emergence of security problems on the inability of two parties to understand the defensive nature of each other's security moves, Dunn Cavelty blames the state for the emergence of the CSD. She cites the militarisation of cyberspace by the state, the weakening of security through state-based malware, state attempts to de-anonymise cyberspace, and the extension of

[16] Buchanan references several Cold War initiatives including the Anti-Ballistic Missile Treaty, the Open Skies Treaty, Strategic Arms Limitation talks and the Intermediate Nuclear Forces agreement.

[17] For example, by bilateral nuclear disarmament or in a cybersecurity by a government declaring zero-days it discovers. This may cost them good intelligence access in the short term but will increase the overall security of the system in the long term.

the notion of national security to cyberspace as evidence of the state's role in reducing both individual and national security. Dunn Cavelty argues that national security and a form of security that is relevant to the people must not be at loggerheads with each other and in cybersecurity, in particular, she claims 'the two can meet' (Cavelty, 2014, p. 703).

In addressing the dilemma between national security and individual freedoms, Dunn Cavelty's work is the most applicable to this thesis. However, Dunn Cavelty only addresses the CSD from the perspective of individual security and human rights, arguing that vulnerability reduction is both the common ground and the solution to the CSD. Dunn argues that reducing vulnerabilities in computer systems protects digital rights by enhancing individual privacy, but also protects national security by reducing the opportunities for hacktivists, criminals and hostile states. But Dunn Cavelty fails to address the fears, held by many states, that totally secure and encrypted communications in cyberspace would increase the threat of crime and terrorism by eliminating the ability of law enforcement to investigate criminal and terrorist activity.

4.3.2 Characteristics of the Cyber Security Dilemma

Security dilemmas have specific characteristics, which create an environment for conflict. Security dilemmas exist in a state of anarchy; they involve actors driven by their own security needs; they are fuelled by fear and certainty; they are exacerbated by the inability to understand the fears of the other; they relate to a scenario where security is not mutually exclusive; they result in actors attempting to accumulate power; and they result in spiralling insecurity and negative outcomes. The following section considers how well each of these characteristics applies to the conflict between the state and the DRC.

4.3.2.1 A State of Anarchy

According to Tang, the ultimate source of the security dilemma is the anarchic nature of international politics (Tang, 2009). Whilst supranational organisations such as the UN or superpowers such as the US can sometimes provide independent nations with some guarantees of security, for the most part they must protect themselves through the accumulation of power, the establishment of alliances and diplomacy.

The conflict between the British state and the DRC is asymmetric as it pits a nation state with legislative authority against a loose collective of individuals and

organisations. Because the British state enacts and executes the law in cyberspace, it could be considered that this creates a state of order that is not conducive to the security dilemma, but the British state's ability to govern cyberspace is actually severely limited. Cyberlibertarians such as John Perry Barlow have long argued that cyberspace is apart from physical space and cannot be subject to state control. This view is sometimes echoed by state actors such as Sir Bernard Hogan-Howe who has argued that cyberspace is becoming anarchic (Barlow, 1996; Hogan-Howe, 2014). The ease of information transit in cyberspace, the public availability of encryption and the rapid pace of technological change all serve to hinder the state's control of cyberspace.

Since the start of the Crypto Wars, activists have attempted to bypass state control of cyberspace by encouraging the use of encrypted systems such as Tor and PGP. In the US, some of the first efforts to control cyberspace through encryption export controls were thwarted by activists who printed banned encryption codes on t-shirts to demonstrate the futility of such policies (Cypherspace.org, n.d.). Following the Snowden disclosures, these efforts became more mainstream and technology companies began to offer greater access to encryption for their customers. The most prominent example comes from Apple, who implemented encryption standards within their products that they described as being able to deny government access to user data even if presented with a court order (Apple Inc, n.d.). Whilst the state could theoretically ban companies from implementing such technology, and they could even ban the use of encryption itself, such legislation would be difficult to pass, relatively easy to bypass and complicated by the international nature of the companies involved. Legislation alone cannot provide the British state with full control over the use of cyberspace in the UK.

Cyberspace is essentially anarchic[18], as neither the state nor actors within the DRC hold complete control and there is no higher authority who can dictate how surveillance is conducted and how encryption is used. This anarchic nature forms the basis for the CSD as without a higher authority the state and DRC are driven to accumulate power to defend their own security interests.

[18] This is not to stay that cyberspace is in a state of chaos or is out of control. A state of anarchy, in this sense, refers to a lack of a higher authority, who can impose decisions on both the state and the DRC.

4.3.2.2 Security Seeking Pre-eminence

Charles Glaser argues that states can be classed as either 'Security Seekers' or 'Greedy States' with respect to their behaviour (Glaser, 1997). Security seekers are only motivated by the desire to preserve their own security, although in doing so they may inadvertently harm the security of the other. Greedy states are motivated to attack others, steal their resources, expand and gain an advantage. The purest form of the security dilemma involves two pure security seekers who end up in conflict due to fear and ignorance; the motivations of each side are benign but the outcome is tragic. If the actors involved have some limited greedy motivations then the security dilemma still applies, as a combination of both aggression and fear can lead to an inflated arms race. However, when one actor is motivated primarily by greed, improving security in self-defence might act as a deterrent rather than fuelling the conflict. As states are comprised of agencies and individuals with different motivations, states can simultaneously display both security seeking and greedy behaviour, which may limit the degree to which the security dilemma can apply.

It is difficult to definitively ascertain whether particular states are security seekers or greedy. Even with hindsight historians disagree over the causes of conflict and the motivations of the actors involved. But as Glaser contests, 'certain actions can communicate valuable information because they are not equally likely to be taken by a greedy state and a pure security seeker' (Glaser, 1997, p. 179). Applied to cyberspace, it is possible to acquire some idea of the degree to which the actors involved are motivated by greed or self-defence.

The British state has always insisted that its surveillance capability is designed to protect the country and its citizens from the threat of terrorism, serious and organised crime, and hostile states (HM Government, 2016). It makes significant efforts in policy documents such as the UK Cyber Security Strategy (UK CSS) to demonstrate its privacy credentials and makes efforts to demonstrate how it is mitigating the potentially intrusive nature of surveillance (HM Government, 2016).

If the British State is the equivalent of a greedy state, then it must be motivated to deliberately harm digital rights. But if this is the case then it is likely that evidence for this would have been uncovered within the hundreds of thousands of documents leaked by Edward Snowden. Whilst it can be argued that the disclosures revealed significant privacy intrusions by GCHQ, they do not show any evidence that GCHQ specifically set out to undermine the public's digital rights. Whilst this

differentiation may not be important for many digital rights advocates, it is a crucial distinction within the security dilemma as it demonstrates security-seeking behaviour that inadvertently threatens the security of others, as opposed to greedy behaviour that deliberately threatens the security of others. It is impossible to disprove the claim, made by some conspiracy theorists, that GCHQ is part of a New World Order plan to control the populace and there has been some past precedent for surveillance capabilities being used for political purposes (The Guardian, 2013). However, it is reasonable to draw the conclusion that, on the whole, GCHQ is motivated to protect the population against terrorism, crime and hostile states rather than to deliberately undermine digital rights (Co, 2014; Campbell & Honigsbaum, 1999).

Members of the DRC frequently state that they do not wish to undermine the ability of the state to fight crime and terrorists, but do acknowledge that national security sometimes had to be compromised to protect individual rights. Whilst some claim that Edward Snowden was working with Russia to compromise American and British national security, there is no evidence to suggest that the DRC is motivated to damage national security (US House of Representatives, 2016). Some cyber-libertarians such as John Perry Barlow view the Internet and encryption as an opportunity to undermine nation states and bring about a new system of governance. It could reasonably be argued that this represents greedy behaviour that goes beyond pure security seeking intention, but whilst the actions of the DRC may be considered a threat to national security, this threat arises as a by-product of actions to protect individual rights and is not what motivates the majority of the DRC.

4.3.2.3 Fear and Uncertainty

The security dilemma is driven by the actors' belief that the other side threatens their own security. This can be derived from a misreading of the other's defensive actions as offensive, a psychological bias against the other, a tendency to respond to the worst-case scenario or a general fear of the unknown.

Security actors within the British state often claims that encryption and other security measures are turning the Internet into a 'dark and ungoverned space', which is in danger of becoming anarchic, whereas the DRC claims that efforts to 'undermine' encryption and advanced security measures represent a threat to digital rights (Muižnieks, 2013; Schneier, 2015; Berners-Lee, 2012; Hogan-Howe,

2014). Technical and legislative moves by the state to ensure that the security agencies maintain their ability to access online communications are met with protest from members of the DRC, who claim that these measures threaten democracy and digital rights. Similarly, the introduction of technical or legal measures to protect technology users from criminal hacking or state surveillance is met by equally loud protest from state representatives, who claims that these measures threaten national security and will lead to terrorism and increased criminality (Rudd, 2017) (Hogan-Howe, 2014).

This level of mistrust is fuelled by uncertainty over the actions and motivations of the other side. When asked about whether he believed there was something sinister about state surveillance, Jim Killock, the Director of the ORG, argued that it was the inability to read the state's intentions that was the real problem.

> There may be [something sinister] but you can never know what the sinister motivations might be because those motivations exist in the heads of people, not necessarily in policy documents and they are not necessarily articulated … the obscurity is where you get the problem, I think (Killock, 2016).

Killock also discusses the difficulties of determining exactly what the threat of state surveillance is, given that intrusion into people's emails, for example, is much less visible than the police entering someone's property and searching through their filing cabinet.

> There' s a silence. It is a difference, not least because it makes it harder for people to understand whether this is a real or ignorable threat, is this something we need to pay attention to? The silence of this monitoring, the fact that it's happening without direct participation or noticing it, that is what makes it quite hard for people to judge (Killock, 2016).

Whilst the motivations of characters such as Edward Snowden[19] and large technology companies[20] can be challenged, there is little to suggest that a significant percentage of the DRC want to threaten national security. Whilst

[19] Many view Edward Snowden's actions to be motivated by revenge, desire for personal fame or due to corruption by Russia or China. See House of Representatives report.

[20] Strong privacy credentials are commercially attractive for technology companies so some believe that actions by some technology companies to display these credentials may be motivated by profit rather than an altruistic desire to protect human rights.

members of the DRC may directly fear the actions of state actors such as GCHQ, the state does not generally view the DRC to be hostile. Instead, it fears that actions taken by the DRC will inadvertently facilitate terrorist and criminal actors. This view was articulated by the former director of GCHQ, Robert Hannigan, who accused technology companies of being in denial about their role in facilitating terrorism.

> To those of us who have to tackle the depressing end of human behaviour on the internet, it can seem that some technology companies are in denial about its misuse (Hannigan, 2014).

The CSD is fuelled by the British state's fears over the consequences of the DRC's actions and the DRC's fears over the consequences of state actions.

4.3.2.4 Failure to appreciate the fears of the other

Within the security dilemma, each side considers their own actions to be defensive in nature and cannot appreciate why others may see them otherwise. Butterfield argues that this inability to understand why the other might see them as threatening is the driving force of the security dilemma (Butterfield, 1951).

> You yourself may vividly feel the terrible fear that you have of the other party, but you cannot enter the other man's counter fear, or even understand why he should be particularly nervous. For you yourself know that you mean him no harm, and that you want nothing from him save guarantees for your own safety; and it is never possible for you to realise or remember properly that since he cannot see the inside of your mind, he can never have the same assurances of your intentions that you have (Butterfield, 1951, p. 21).

In the CSD, the British state considers surveillance to be defensive in nature, designed to prevent terrorists and criminals from attacking both the state and the population. This is a view that was repeatedly put forward during interviews with GCHQ staff such as Matt.

> In terms of the threat to privacy. This is not from us. With GCHQ we have a mandate, done through an elected government, under law and with safeguards and oversight. Other people are intruding without a mandate or safeguards. Criminals don't have a mandate, oversight or safeguards. This is criminals against individuals. It's a

> completely different nature of intrusion. The aims are different; the purpose is different. We can only use surveillance for national security, serious crime and the economic wellbeing of the UK (Matt, 2016).
>
> If you consider that if somewhere in our building there being some information on you is a breach of privacy, then companies do the same. It's not the state that gathers the data. We use it for national security purposes (Matt, 2016).
>
> In terms of threats to liberty, privacy and freedom we're here to defend liberty and freedom. The freedom to be safe, the freedom delivered through economic wellbeing, keeping the UK safe. Globally we have much greater freedoms and privacy then many other countries and we are actively promoting this around the world (Matt, 2016).

But there is also frustration that others do not understand this point of view and there is exasperation that GCHQ could be viewed as some form of totalitarian force.

> Part of this is a trust issue. A misunderstanding of what we do and how. Not understanding we're real people drawn from the public. It's frustrating to have the 'mass surveillance' myth pedalled (Matt, 2016).
>
> We don't like this [the term mass surveillance]. It sounds 1984 and it's not true. It suggests a totalitarian regime where every move is watched and scrutinised and has possible repercussions. How can people actually think we live like this? (Fiona, 2016).

For GCHQ, the task of persuading others of their benign nature is hampered by issues of secrecy, the lack of a human face and the complexity of the technology and laws that govern the organisation.

> We have one arm tied behind our back because we can't talk about specific cases. Identities are also sensitive therefore it is very difficult to put a human face on the organization. This is difficult as we only have a handful of faces we can show. It's a problem because some of the allegations of 'mass surveillance' and extreme forms of 'those people must be evil' would be an untenable

> position if you see the actual people who work here. The complexity of the work, the laws that cover us and the technology, which are all difficult to understand is also a problem (Matt, 2016).
>
> The legislation that currently exists and proposed new legislation is really complex. Even those who track and follow it observe that a large proportion of people struggle to understand. So explaining to the public is very challenging (Emily, 2016).

For GCHQ staff this communication problem was compounded by Snowden's disclosures, which they believe presented an inaccurate picture of the organization.

> One of the things that Snowden did was to make the public think that we weren't on their side. That we had somehow slipped into 1984. It is on us to communicate our value. That we aren't how we are portrayed, that we don't care about their email and are not reading it and we are focused on threats to the UK (Fiona, 2016).

GCHQ staff also highlight how difficult it is to reverse these perceptions, given their inexperience in communicating with the public.

> It's like turning the Titanic. We're a Signals Intelligence agency, not an experienced crisis management agency. Previously we were used to just speaking to the Gloucester Echo and the biggest story was that a dead pigeon had been found with a WW2 code attached to it and GCHQ couldn't decrypt it. So the organisation struggled to react to Snowden in a way. We were previously secret with no public face. When the news broke we didn't know how bad it would be. By the time we realised what had happened and were ready to react the horse had already bolted. The reaction was slow and coated in fear. We tried to starve the story of oxygen by not commenting on it but then when we realised that was not working we started to engage but it has taken a long slog to build up relationships and get to the situation we are in today, which isn't perfect. But so much damage was done by not commenting. Someone else had told our story. The headlines were sensational. It was compelling but it was wrong (Fiona, 2016).

The DRC also consider their own actions to be defensive, not just of digital rights but also of national security. But one of the major allegations that the DRC must frequently counter is that their efforts aid terrorists and harm national security (Cotton, 2016). Edward Snowden, for example, claims that his actions are designed to improve the NSA and Bruce Schneier, amongst many others, argues that strong encryption is essential for national security (Snowden, 2013; Schneier, 2016).

> I am not trying to bring down the NSA, I am working to improve the NSA. I am still working for the NSA right now. They are the only ones who don't realize it (Snowden, 2013).

> The FBI paints this as a trade-off between security and privacy. It's not. It's a trade-off between more security and less security. Our national security needs strong encryption (Schneier, 2016).

But many within the DRC are frustrated by the lack of understanding of their position. When asked why GCHQ does not understand the DRC's point of view, ORG Policy Director Javier Ruiz claims that 'to a hammer every problem looks like a nail', continuing to explain that GCHQ can only think of surveillance as the solution to national security problems because this is the nature of the organisation. He also claims that public understanding of the issues is limited by the complexity of the technology involved (Ruiz, 2016).

> [public understanding is] not good at all. What you get every now and then is that people have a gut feeling for something but they don't know how to express that and they don't really understand the technology and then they don't complain (Ruiz, 2016).

Both the British state and the DRC believe that their own actions are defensive in nature and are motivated by a desire to improve security, freedom and liberty for the populace, but each is also frustrated by what they would consider the inability of others to understand their position. Whilst some within the government and DRC may be better at understanding the fears of the other, each side is largely fixated on their own security concerns. As Butterfield puts it 'neither side sees the nature of the predicament that he is in, for each only imagines that the other party is being hostile and unreasonable' (Butterfield, 1951, p. 21).

4.3.2.5 Compatible Security

The security interests of two different parties can broadly be described as compatible or incompatible. If compatible, then the security interests of each can be achieved through either independent efforts or through the establishment of an alliance. If security interests are incompatible, then any advancements in the security of one party will reduce the security of the other, and as it is impossible for both to simultaneously achieve security, conflict is inevitable.

One of the most significant arguments against the existence of a CSD is the belief that national security and digital rights are incompatible security models. National security can only be achieved by reducing digital rights and digital rights can only be achieved at the expense of national security, so solutions should focus on striking a balance between these 'competing' notions.

But the need for balance is challenged by several authors including Mark Neocleous, who argues that the notion of balance is a substitute for real argument (Neocleous, 2007). Neocleous argues that 'the myth of a "balance" between security and liberty opens the (back-) door to an acceptance of all sorts of authoritarian security measures; measures which are then justified on liberal grounds' (Neocleous, 2007, p. 133). By ceding that balance is required, illiberal security measures must be accepted in its name. Jeremy Waldron also opposes the concept of balance, but suggests that the idea of balance is based on the false assumption that security and liberty are in a zero-sum game (Waldron, 2003). Waldron's arguments against a balance include the rejection of consequentialism by civil rights activists and the existence of imbalances in security and liberty throughout society. Waldron also suggests that actions taken to improve individual security (at the expense of liberty), by boosting the state's powers, might actually diminish the security of the individual due to the new threat posed by the state itself. This is a common argument made by the DRC, who claim that the powers accumulated by organisations, such as GCHQ, to fight terrorism, can equally be used against the populace.

Kenneth Boulding argues that alongside 'real' incompatibility we should also be considering another type of incompatibility which he describes as illusory.

> The other form of incompatibility might be called 'illusory' incompatibility, in which there exists a condition of compatibility which would satisfy the 'real' interests of the two parties but in which the dynamics of the situation or illusions of the parties

> create a situation of … misunderstandings, with increased hostility simply as a result of the reactions of the parties to each other, not as a result of any basic differences of interests (Boulding, 1959, p. 130).

The belief that national security and digital rights are incompatible is a result of years of competing securitisations and the polarization of the cybersecurity debate. As discussed in Chapter 3, this debate has become entrenched in issues of encryption, backdoors and the concept of 'Going Dark'. It is framed as a choice between encryption and digital rights, on the one hand, and backdoors and national security on the other.

A universal application of unbreakable encryption, where the decryption keys are held securely and solely by the communicating parties, does appear to be incompatible with the state's desire to be able to access all online communications, but encryption and surveillance do not constitute the real security interests of the state and the DRC. Encryption does not guarantee digital rights and digital rights do not rely on encryption. Likewise, access to all communications does not guarantee national security and national security does not rely on access to all communications. As Andrew Keane Woods suggests in his description of Encryption Substitutes, there are many ways that the DRC can achieve security without the need for encryption, and there are many ways for the state to achieve national security without gaining access to encrypted data (Woods, 2016).

Recently there has been some movement away from the view that national security and digital rights must be balanced. Whilst the 2011 UK Cyber Security Strategy discusses 'balancing security with freedom and privacy', the 2016 National Cyber Security Strategy debates 'reconciling national security with individual rights and freedoms', and the Investigatory Powers Act 2016 claims to 'protect both the privacy and security of the public' (HM Government, 2016; HM Government, 2016; HM Government, 2011). In 2014, FBI Director James Comey claimed that law enforcement worked to provide security that enhances liberty.

> Some have suggested there is a conflict between liberty and security. I disagree. At our best, we in law enforcement, national security, and public safety are looking for security that enhances liberty. The people of the FBI are sworn to protect both security and liberty. It isn't a question of conflict (Comey, 2014).

Whereas many in the DRC, such as Bruce Schneier, claim that encryption is essential to national security.

> The FBI paints this as a trade-off between security and privacy. It's not. It's a trade-off between more security and less security. Our national security needs strong encryption (Schneier, 2016).

Many policies designed to improve national security are considered detrimental to digital rights, and many efforts to improve digital rights are considered detrimental to national security, but the two are not incompatible because ultimately each side wants both national security and digital rights.

4.3.2.6 Power Accumulation

Due to uncertainty and fear about the intention of others, states often believe that they have no choice but to accumulate power to protect their own security. This power accumulation may take the form of military might, economic power, political alliances or forms of soft power such as cultural influence. The British state attempts to accumulate power in cyberspace through both legislation and the development of technical capabilities, particularly at GCHQ. These efforts are designed to provide the state with the capability to access any electronic communication if deemed necessary to protect national security and to deny 'safe spaces' for terrorists to communicate online (May, 2015). The Telecommunications Act 1984 was the first major piece of legislation providing surveillance powers to the British intelligence services. It allowed the collection of bulk phone data and authorised the Secretary of State to order telecoms providers to provide secret assistance to the state in the interests of National security.

Following advances in technology, the Regulation of Investigatory Powers Act 2000 (RIPA) provided the state with further powers, including the ability to intercept the content of phone and internet communications, the power to demand that an ISP provides access to an individual's communications in secret and the power to engage in bulk collection of communications data whilst in transit. Following the re-emergence of terrorism in the UK and the use of the Internet for serious and organised crime, the Investigatory Powers Act 2016 provided further powers to the state including the right to access Internet collection records for up to 12 months and the creation of Technical Capability Orders, which allow the state to order technology companies to adapt their products to facilitate access to information. This legislation is designed to both help ensure that the state can combat crime and

terrorism, but also to enable it to mitigate new technologies, such as encryption, that have reduced the state's capability to operate in cyberspace.

The state has also sought to improve its capability to conduct cyberspace surveillance through the development of new technical capabilities. The Snowden disclosures reveal that in around 2007, GCHQ embarked on a programme dubbed 'Mastering the Internet' (MTI) which was designed to provide the agency with vast amounts of intelligence from cyberspace. The programme was designed to intercept and exploit as much Internet traffic as possible, and an internal report from 2011 indicates that in a single day the agency collected 39 billion separate pieces of information (The Guardian, 2013). In recent years GCHQ has also developed capabilities to hack into individual computers, rig online polls, intercept live webcam footage, read individual emails and intercept web-based phone calls (The Guardian, 2014; The Guardian, 2014). GCHQ has also increased its funding and staffing; it received the majority of money from the 2011 Cyber Security Programme and, in 2015, the government announced that 1000 extra staff would be employed at GCHQ, MI5 and MI6 (The Telegraph, 2015).

Efforts within the DRC to develop and spread security technologies and influence legislation can also be viewed as an attempt to accumulate power to defend their own security interests. Technologies such as PGP and Tor are actively promoted by members of the DRC, and organisations such as the ORG organize and promote events such as 'Crypto Parties' which are designed to increase the uptake of good encryption (Open Rights Group, n.d.). As discussed in Section 3.3.2, technology companies such as Apple and Facebook have also increased their security provision, providing to users both end-to-end security for communications and full-disk encryption for data at rest (Apple Inc, n.d.).

Members of the DRC have also been active in restricting the state's surveillance powers through political campaigning and participation in the drafting of legislation. During the consultation period for the IPA, a large range of digital rights organisations and supporters, including the ORG, EFF, Privacy International, Human Rights Watch, Liberty and Amnesty International[21] provided written and oral evidence to the Investigatory Powers Committee making the case to limit state surveillance powers and provide better oversight and accountability mechanisms.

[21] See https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf for a full list

Provisions such as a new Investigatory Powers Commissioner, the creation of new offences for the misuse of Investigatory Powers and the requirement for warrants issued by the Secretary of State to be signed off by a senior judge, were all achieved in response to campaigns by the DRC (HM Government, 2016).

The development of technologies and legal powers by both the state and the DRC reflect efforts to accumulate power in the interests of security. The state continuously develops new capabilities to defend national security and counter the more difficult technological landscape, whilst members of the DRC continuously seeks new capabilities to counter increasingly intrusive state surveillance measures (Apple, 2017; Electronic Frontier Foundation, n.d.; HM Government, 2017)

4.3.2.7 Spiralling Insecurity

When the security dilemma is established it leads to an arms race of competing security spending as each side tries to keep up with the other but is ultimately left feeling even more insecure.

> [states are naturally] concerned about their security from being attacked, subjected, dominated, or annihilated by other groups and individuals. Striving to attain security from such attack, they are driven to acquire more and more power to escape the impact of the power of others. This, in turn, renders the others more insecure and compels them to prepare for the worst. Since none can ever feel entirely secure in such a world of competing units, power competition ensues, and the vicious circle of security and power accumulation is on (Herz, 1950, p. 157).

Figure 4.1 demonstrates how this spiralling arms race is evident in the CSD as both the state and the DRC react to the other's security efforts by making additional security moves of their own.

State
Fear: Cyberspace is enabling criminality and terrorism Action: Legislation to enable the intelligence agencies to conduct surveillance and the development of a surveillance capability

DRC

Fear: The **s**tate's surveillance capability is a threat to digital rights

Action: The development and promotion of encryption and other security technologies to protect digital rights and defend against state surveillance.

⇩

State

Fear: Encryption is threatening the state's ability to enforce the rule of law and counter threats to national security

Action: Efforts to undermine encryption, efforts to break into encrypted products and legislation to help gain access to encrypted communications

⇩

DRC

Fear: 'Breaking' Encryption undermines security and digital rights

Action: Opposition to state efforts to gain access to encrypted communications and resistance to court orders by technology companies such as Apple.

Figure 4.1: The spiralling arms race

Whilst the diagram indicates a start and end to the conflict, in reality it is a spiral with no defined start or end. Whilst any of the actions that are taken could be considered positive in isolation, the result of the spiral as a whole is greater insecurity. The result of this spiralling arms race between the state and the DRC is a greater insecurity for both parties, which is demonstrated by claims from each side that their security is under greater threat than ever. Following enactment of the IPA in 2016, Jo Glanville, Director of the freedom of expression advocates, English PEN, described it as 'unprecedented' and more chilling than the Snowden revelations, Bella Sankey, the policy Director of Liberty, claimed that 'the state has achieved totalitarian-style surveillance powers' and Jim Killock, director of ORG, said that the act granted the state unprecedented powers 'more suited to a dictatorship than a democracy' (Don't Spy On Us, 2016). In 2016, new government terror watchdog Max Hill claimed that the terror threat was the greatest it had been for 40 years, Head of MI5 Andrew Parker said that the cyber threat from hostile states was growing and, at the opening to the new NCSC, Chancellor Phil Hammond

claimed that 'the cyber attacks we are seeing are increasing in their frequency, their severity, and their sophistication' (Hammond, 2017; Parker, 2016; Hill, 2017).

The case of Apple vs the FBI can be used to demonstrate how efforts to improve security can paradoxically result in greater insecurity for both sides. From a digital rights perspective, security was reduced because not only did the FBI end up with the ability to break into all iPhone 5Cs, but the existence of a major vulnerability became public knowledge and their appeared to be no guarantee that the vulnerability would not be disclosed to others. In a lawsuit filed by the Associated Press, USA Today and Vice Media, the claimants argued that dangerous technology was now in the hands of this unidentified vendor.

> The FBI's purchase of the technology – and its subsequent verification that it had successfully obtained the data it was seeking thanks to that technology – confirmed that a serious undisclosed security vulnerability existed (and likely still exists) in one of the most popular consumer products in the world. And in order to exploit that vulnerability, the FBI contracted with an unidentified third-party vendor, effectively sanctioning that party to retain this potentially dangerous technology without any public assurance about what that vendor represents, whether the vendor has adequate security measures, whether the vendor is a proper recipient of government funds, or whether it will act only in the public interest (Associated Press, USA Today, Vice Media, 2016).

Apple could have hacked the iPhone in a controlled environment before providing the data to the FBI and destroying the software they had created but, by opposing this option on security grounds, the FBI acquired a method for accessing iPhones which they could use to bypass Apple altogether.

From the FBI's perspective, the outcome also damaged security. When speaking at the Aspen Security Forum in London, FBI Director James Comey indicated that the zero-day had cost the FBI more than his wages for the next seven years, which roughly equated to $1.3 million USD (The Guardian, 2016). Spending such large amounts each time they have trouble accessing data would not be feasible and would reduce the funds available for other counter-terrorism work. By pursuing the case, the FBI also angered a coalition of other technology companies including

Google and WhatsApp, who all backed Apple's stance (Financial Times, 2016) and are increasingly resistant to attempts by the US state to access user data.

The CSD has led to spiralling security efforts and spiralling insecurity for both the state and the DRC.

4.3.2.8 Negative Outcomes

The dynamics of the security dilemma have led to countless wars and ethnic conflict, resulting in tragic loss of life as well as standoffs that encourage massive military spending and hinder mutually beneficial co-operation.

When security rivalries emerge from security dilemmas it is natural for each side to blame the other as each side 'knows' that their own actions are only meant to protect their security and 'each only imagines that the other party is being hostile and unreasonable' (Butterfield, 1951, pp. 19-20). After the Cuban Missile Crisis, for example, the US blamed the USSR as they had positioned threatening weapons adjacent to the US, but the USSR blamed the US for they were only responding to US missiles in Italy and Turkey and the botched CIA operation to overthrow their ally in Cuba. Viewed through the lens of the security dilemma, each side was driven by their own compatible security interests, but by taking action that threatened the other they almost provoked a nuclear war.

A similar scenario is evident in the case of WannaCry, the malware that caused substantial damage to computer networks around the world and crippled some parts of the NHS. The DRC blame the CIA for creating the malware that was stolen and used within the WannaCry attack, but the CIA and NSA could claim that if the DRC hadn't opposed their efforts to gain access to computer networks then they wouldn't have to resort to malware (The Guardian, 2017). Likewise, the British state could accuse social networks of facilitating terrorist attacks such as the murder of Lee Rigby, but Facebook and others could argue that they had to limit co-operation with law enforcement due to the targeting of technology companies by US and UK intelligence agencies.

Whilst the state and DRC can blame each other for security incidents, it is more useful to consider the impact of the CSD as a whole. This includes the increasing use of cyberspace by cyber criminals and terrorists, frequent data leaks involving the private information of citizens, an increasingly difficult online environment for law enforcement, substantial surveillance by domestic and foreign intelligence agencies, and the ease of access to illegal material through encrypted services such

as Tor. These outcomes demonstrate the tragedy of the Crypto Wars of the 1990s and 2010s, which resulted in time and resources being spent on an arms race between the state and the DRC, whilst attacks by hackers, cyber criminals, terrorists and foreign states were harming both digital rights and national security.

4.4 Intensifying the Security Dilemma

The previous section demonstrates how the CSD has the characteristics of traditional security dilemmas, but it also has particular properties that intensify its effects. Within Jervis's conceptualization of the security dilemma, a state's behaviour can be described as either defensive or offensive; defensive behaviour is designed to protect an actor's own security interests, whilst offensive behaviour is designed to disrupt the status quo in favour of the attacker (Jervis, 1978). But it is often difficult to determine whether behaviour is defensive or offensive in nature. In cyberspace, the defensive or offensive nature of activities such as surveillance can be judged by considering the purpose of this activity. From the DRC's perspective, state surveillance can be considered to have either defensive or offensive purposes:[22]

Defensive Purposes

- Prevention and investigation of crime.
- Intelligence gathering against hostile states.
- Prevention of terrorism.
- Counter-espionage against foreign intelligence agencies.

Offensive Purposes

- Falsifying intelligence to gain public support for war or other such action.
- Using surveillance to spy on, control or manipulate citizens or the media.
- Spying on opposition parties to support the party in government.
- Covering up wrongdoing by the intelligence agencies or the state.
- Conducting intrusive and unwarranted surveillance against the whole population.

[22] Individuals within the DRC would likely disagree about whether some of the 'defensive' purposes are legitimate as they rely on the state defining who is a hostile state or terrorist group but the wider point is that most members of the DRC would consider some uses of surveillance to be defensive in nature and therefore justified.

From the British State's perspective, security technologies such as encryption can also have defensive or offensive purposes.

Defensive Purposes

- Protection of individual privacy.
- Protection of freedom of speech.
- Protection of journalism.
- Protection of the identity of vulnerable people such as political dissidents.

Offensive Purposes

- Facilitation of criminal acts such as terrorism or the sharing of child abuse imagery.
- Prevention of lawful investigation into criminals and terrorists.

According to Jervis (1978), the magnitude of the security dilemma depends on two main conditions; offence-defence differentiation and offence-defence balance. I.e. how easy is it to determine whether capabilities are designed for defensive or offensive purposes, and how easy is it to use capabilities offensively rather than defensively?

4.4.1 Defence/Offence Differentiation

To solve the dilemma of interpretation states must be able to judge whether the actions of another are motivated by defensive or offensive intent. Has a military build-up been ordered out of fear (perhaps enhanced by poor intelligence) or out of a desire to attack? States can make this assessment by considering several factors, including the other side's military doctrine, culture, training programme, alliances, arms development, political statements, past behaviour and command structure. When offensive and defensive behaviour is difficult to distinguish, the security dilemma intensifies but when offensive and defensive behaviour is easy to distinguish, the security dilemma diminishes as each side can invest in their own defence without threatening the other.

4.4.1.1 DRC Perspective

GCHQ is split into an intelligence collection element and a cybersecurity element, the NCSC. Whilst the NCSC is evidently designed for defensive purposes (i.e. to promote UK cybersecurity and protect the country's infrastructure), the function of the intelligence collection element is more obscure. To determine whether GCHQ's intelligence capabilities are designed for defensive or offensive purposes, members

of the DRC may consider their technical capability, their motivation and their past behaviour.

From a purely technical perspective, it is extremely difficult to differentiate whether the technologies employed by agencies such as GCHQ are designed for offensive or defensive purposes. For example, GCHQ has the capability to intercept the emails of criminals and terrorists, but this same technology can also be used against political opponents or the public. GCHQ also has the capability to manipulate information online, change the outcome of online polls and boost traffic to websites or views on YouTube (*The Guardian*, 2014). These techniques can be used to undermine terror networks and reduce their support but, technically, they could also be used to manipulate public opinion or cover up wrongdoing. Intuitively, GCHQ's ability to manipulate information appears more threatening to democracy and individual rights, compared to their ability to passively collect data. An ORG report on GCHQ's 'offensive capabilities' expressed concern about the 'potentially horrific' implications of these capabilities given the lack of oversight (Open Rights Group, n.d.).

> The problem however with GCHQ controlling these offensive capabilities is that they are highly secretive and are not subject to the same levels of public oversight we would normally expect. Parliament would normally examine the ethical, legal and strategic questions associated with our offensive weaponry (Open Rights Group, n.d.).

The differentiation problem is exacerbated by vastly differing perceptions of GCHQ's data collection, with GCHQ arguing that 'bulk collection does not equal bulk surveillance' and the ORG claiming that 'the bulk collection of communications data without targeted suspicion *is* mass surveillance' (Hannigan, 2016; Open Rights Group, n.d., p. 172). GCHQ often cite an investigation by the Investigatory Powers Tribunal which rejects the assertion that they carry out 'Mass Surveillance', but the DRC claims that considering everyone's data a threat is still mass surveillance (GCHQ, 2014).

> I think for us it is the whole apparatus of collect, analyse, store, reanalyse, flag, that is a process of mass surveillance because you are treating everyone's data as potentially indicative of threat. You analyse it all to find what might be a threat (Killock, 2016).

During his leaving speech, GCHQ Director Iain Lobban claimed that 'the people who work at GCHQ would sooner walk out the door than be involved in anything remotely resembling "mass surveillance"' (Lobban, 2014). And during interviews with GCHQ staff, including Emily, Adrian and Fiona, it was evident that this view is embedded deep within the organisation.

> I recognise the phrase [mass surveillance], its widely used. If individuals think that we are looking at everything then this is completely and utterly wrong. The Anderson, RUSI and ISC reports all disprove this notion (Emily, 2016).

> It's not mass surveillance. We have the powers to undertake bulk collection. We use bulk collection authorities to investigate and prevent crimes. We do not surveil the whole UK to do that. There is a difference between how we collect and analyse, rather than an analyst looking at every aspect of data in the UK (Adrian, 2016).

> We don't like this. It sounds 1984 and it's not true. It suggests a totalitarian regime where every move is watched and scrutinised and has possible repercussions. How can people actually think we live like this? We have powers, legal authority and the rules of proportionality to look for threats. This needs bulk collection but most of the data won't be touched (Fiona, 2016).

Some GCHQ staff also argue that it would be impossible to conduct mass surveillance given the number of lawyers that would be required to authorise such action, the analytical manpower required, and the fierce resistance that GCHQ staff would put up themselves if they were asked to conduct such work. This was evident throughout interviews with GCHQ staff.

> It's a problem because some of the allegations of 'mass surveillance' and extreme forms of 'those people must be evil' would be an untenable position if you see the actual people who work here. It's frustrating to have the 'mass surveillance' myth pedalled. It's interesting that many people believe the myth of mass surveillance but don't care. They think that if that's what's necessary then it's fine. But that's bad for people here as they wouldn't want to work here if it really was like that. It's very

> worrying for GCHQ staff because they care about civil liberties (Matt, 2016)

> I don't recognise it. You need to look at a lot of data as there's lots out there. Surveillance is very specific in law and warranty on it is very rare. Conflating mass with surveillance. It's impossible due to the numbers of lawyers who would need to sign it off. How would you go about doing that? The Home Secretary signing off a warrant versus everyone? It's a ridiculous argument (David, 2016).

For GCHQ, these limitations put technical restraints on the organisation's ability to conduct mass surveillance, thus ensuring that their capabilities are used for defensive purposes only, but these arguments are rejected by groups such as ORG who argue that they don't 'detract from the gigantic scale and breadth of the agencies' activities' (Open Rights Group, n.d., p. 26).

Whilst technical capabilities may be dual use, the nature and history of institutions who wield power can also provide clues as to whether they are designed for offensive or defensive purposes. Since the 2001 terrorist attacks in New York and the 2005 terrorist attacks in London, GCHQ has played an increasing role in domestic operations, including the 'War on Terror', and has been given a greater role in tackling online crime, especially child sex exploitation. Documents released by Edward Snowden reveal that, in 2009, GCHQ's JTRIG unit conducted the organisation's 'first serious crime effects operation' against a website that was identifying police informants (The Intercept, 2011; Dhami, 2011). JTRIG has also conducted work for several domestic agencies, including the Metropolitan Police, Border Agency, HMRC and the National Public Order and Intelligence Unit (NPOIU). This work has involved the monitoring of domestic extremist groups', online work to 'deny, deter and dissuade' criminals and work to 'deter and disrupt online consumerism of stolen data or child porn, including the use of psychological methods (The Intercept, 2011; Dhami, 2011). A formal collaboration between the new National Crime Agency (NCA) and GCHQ was announced in 2015 with the establishment of the Joint Operations Cell (JOC), which is designed to 'identify and stop serious criminals, as well as those involved in child sexual exploitation and abuse online' (National Crime Agency, 2015).

If GCHQ's JTRIG uses psychological methods to influence criminals and terrorists in the UK then these techniques can also be used for more offensive actions, such as

the manipulation of the public. Whilst GCHQ's increasing role in domestic affairs can be considered a more effective use of its unique capabilities, the blurring of its domestic and foreign responsibilities makes it harder for outsiders to determine whether its capabilities are being used defensively or offensively.

Another means to judge the offensive or defensive nature of GCHQ's capabilities is to consider how they have been used in the past. Whilst there is no evidence of wide-ranging abuse of GCHQ capabilities, there is evidence that they have previously engaged in behaviour that could be considered offensive in nature. For example, in 2003, an ex-GCHQ staff member leaked documents that suggested the UK was planning to use its surveillance capabilities to spy on six countries at the UN who were key to passing a second UN resolution on Iraq (The Guardian, 2013). In 2013, leaked documents from Edward Snowden indicated that GCHQ was engaged in several controversial programmes, including the capability to access 1.8 million webcams and in 2016, the Investigatory Power Tribunal found that GCHQ's collection and use of Bulk Communications Data was illegal (The Guardian, 2014) (Investigatory Powers Tribunal, 2016). Whilst some may consider these cases to be exceptions, others will see them as the tip of the iceberg and evidence of widespread abuses of power.

It is extremely difficult for the DRC to determine whether the state's vast surveillance capabilities are designed for offensive or solely defensive purposes. The combination of a huge and previously hidden surveillance programme, inadequate oversight, increasing focus on domestic issues and past evidence of abuse, leads many within the DRC to conclude that the state is offensively minded and uses its surveillance capabilities to cover up wrongdoing, justify unjust wars and control the population (Open Rights Group, n.d.; GCHQ Lawyer, 2013; The Guardian, 2013).

4.4.1.2 State Perspective

To determine whether the capabilities of members of the DRC are designed for defensive or offensive purposes, the state can consider their technical capability, their motivation and their past behaviour.

Encryption is critical to the functioning of the Internet but, from a purely technical perspective, it is impossible to determine whether technologies such as encryption are defensive or offensive in nature. As Moore and Rid explain, individuals now have the capability to encrypt their own communications to protect their privacy,

but the same technology can be used by criminals and terrorists to support more nefarious activities.

> The power of ciphers protects citizens when they read, bank and shop online – and the power of ciphers protects foreign spies, terrorists and criminals when they pry, plot and steal. Encryption bears directly on today's two top threats, militant extremism and computer-network breaches yet it enables prosperity and privacy (Moore & Rid, 2016, p. 7).

This dual use nature of encryption creates a significant problem for both the state and the DRC. Studies show that sophisticated encryption technologies such as Tor are used primarily for illicit purposes, but they are also widely valued for their protection of personal freedoms and individual privacy (Moore & Rid, 2016). Before encryption became widespread and was implemented by default on services such as WhatsApp, intelligence agencies considered the personal use of encryption to be suspicious, but as encryption has become more mainstream the defence/offensive balance has blurred.

> Previously, as an analyst, if someone used encryption then this would be suspicious behaviour but this is no longer the case (Fiona, 2016).

Whilst the state often comments on the benefits of encryption, it is also frequently blamed for crime and terrorism, such as in the wake of the Westminster terror attacks.

> To be very clear – Government supports strong encryption and has no intention of banning end-to-end encryption. But the inability to gain access to encrypted data in specific and targeted instances – even with a warrant signed by a Secretary of State and a senior judge – is right now severely limiting our agencies' ability to stop terrorist attacks and bring criminals to justice (Rudd, 2017).

The Intelligence and Security Committee (ISC) Report into the murder of Fusilier Lee Rigby indicated that GCHQ's inability to access the communications of two of the perpetrators contributed to the attack not being stopped. The report noted that 'encryption is increasingly being used by CSPs to prevent criminality' but suggested that for law enforcement 'the growing use of increasingly sophisticated encryption

is challenging' (Intelligence and Security Committee of Parliament, 2014, p. 147). Former head of the Metropolitan Police Service, Sir Bernard Hogan-Howe, has also previously warned that encryption 'is in danger of making the Internet anarchic' (Hogan-Howe, 2014).

For the DRC, encryption is often considered to be inherently good, and crypto-anarchists such as Julian Assange consider cryptography to be a means by which a better world can be achieved. Apple CEO, Tim Cook claims that 'encryption is inherently great and we would not be a safe society without it' (Cook, 2016). Borrowing and adapting from Thomas Jefferson, Edward Snowden claimed that cryptography is the only way to stop mankind from doing wrong.

> Let us speak no more of faith in man, but bind him down from mischief by the chains of cryptography (Greenwald, 2014, p. 24).

And Julian Assange claims, quite simply, that 'the universe believes in encryption' (Assange, 2013).

This dedication to cryptography has been noted by authors such as Rid and Moore, who consider that 'too many activists treat cryptography as if it were a godlike force for good' and describe Julian Assange's book as a celebration of the 'cult of crypto' (Moore & Rid, 2016). Indeed, some anti-religious websites such as antispirituality.net' list cryptography as a cult and claim that 'the fundamental belief of cryptography cultists, is the conviction that Cryptography is the only thing that matters in the universe' (Antispirituality.net, n.d.).

The dual-use nature of encryption makes Jervis's offence/defence differentiation extremely difficult and this consequently fuels the security dilemma. The DRC promote encryption for its defensive properties, whilst the state opposes some of its uses due to its offensive potential. There is no way to determine whether new encryption technologies will be used in ways which are viewed as defensive or offensive by the state. This problem is exacerbated by the different views taken towards encryption, with the Digital Rights Movement viewing it as solely defensive and a guarantor of individual security and privacy, and much of the state considering it to be potentially offensive and a threat to their ability to enforce law and order.

The state is unlikely to accuse the DRC of deliberately aiding terrorists and criminals, but it does question whether the DRC's motivations are completely defensive

minded. When technology companies challenge attempts by the state to gain access to user data, there is often disagreement over their motivations and suggestions that they are inadvertently aiding terrorists by pursuing commercially lucrative strategies. As discussed in Chapter 3, Apple's refusal to comply with a court order to unlock a terrorist's iPhone was described as a 'marketing strategy' by the US Justice Department despite Apple's insistence that it was taking a stand to defend digital rights (US Justice Department, 2016). A genuine concern for digital rights could be seen by the state as defensive behaviour, deliberately thwarting terrorist investigations to gain a reputational and economic advantage would be considered an abuse of power. Likewise, as discussed in Section 2.3, the motivation of whistle-blowers is also questioned. Many see Snowden as a serial exaggerator and fabricator, motivated by a desire for revenge, an inflated sense of his own self-importance and potential influence from the Russian intelligence agencies (US House of Representatives, 2016).

For the most part, the DRC is considered to be motivated by a desire to defend digital rights, which can become dangerous for the state when this promotes behaviour that is considered detrimental to national security. But, in some instances, it may be unclear whether more offensive motivations are behind the DRC's actions.

The DRC's past behaviour could give some indication of whether their capabilities are designed for defensive or offensive purposes. From the state's perspective, Apple's conflict with the FBI gives an indication that some technology companies will take all measures they can to prevent their user data from being accessed by the state. Twitter's decision to block British intelligence agencies from accessing some Twitter data, even whilst allowing access to others, can be considered further evidence of this hostility (The Telegraph, 2017; Twitter, 2016).

Large technology companies possess the capability to significantly disrupt the state's ability to investigate and prevent crime and terrorism and there are also suggestions that some companies act against state surveillance to boost their popularity or absolve themselves from the ethical responsibility of handing over decryption keys. There is also concern that whistle-blowers speak out for their own selfish or egotistical reasons but, overall former GCHQ Director Robert Hannigan sums up the state perspective when he states that he has 'never doubted the shared good intentions of all concerned' but is 'puzzled by the caricatures in the

current debate' and believes there is 'confusion' over this 'highly-charged and technically complex area' (Hannigan, 2016).

4.4.2 Defence/Offence Balance

Defence/offence balance describes the ease by which territory can be taken by force, compared to the ease by which territory can be defended. If territory is easy to defend but hard to attack then the security dilemma will diminish because states will feel more secure, but if territory is difficult to defend and easy to attack then states are likely to feel more insecure and will seek to accumulate power to defend their security interests. Jervis uses a simple economic analogy to explain the balance.

> Does the state have to spend more or less than one dollar on defensive forces to offset each dollar spent by the other side on forces that could be used to attack (Jervis, 1978, p. 188).

Jervis argues that if the offence/defence balance favours offence then war will be much more likely. State's will feel more insecure, so may attack to defend their interests; war will be quick and decisive, and therefore profitable; striking first will be more advantageous, therefore increasing the probability of crises escalating via pre-emptive attacks; and because wars are likely, arms races will be more intense.

4.4.2.1 DRC Perspective

The Defence-Offence balance for the DRC relates to how easy it is for the state to use its surveillance capabilities offensively (i.e. abuse them), compared to how easy it is for the public to defend against these abuses. This depends on the capability of the state to conduct intrusive state surveillance, compared to the capability of the public to defend against it. It also depends on the degree to which the law facilitates or protects against intrusive state surveillance, and the degree to which oversight and accountability mechanisms can restrict intrusive state surveillance.

Capability

Television, film and the print media often portray state surveillance capabilities as omnipotent. In the television shows and films of James Bond, Jason Bourne and Jack Bauer, state intelligence agencies can access CCTV anywhere virtually instantly, they hack computers at will, have immediate access to targets' emails and online communications, and can tap phone calls on demand. This fantastical view of

surveillance is re-enforced by the secret nature of organisations such as GCHQ, which makes it difficult for surveillance myths to be dispelled.

For many members of the DRC, the Snowden disclosures are evidence that the state does indeed possess a massive surveillance capability (Open Rights Group, n.d.). The PRISM programme, reportedly provided GCHQ and NSA with direct access to the online lives of everyone in the UK and US, through backdoor access to the systems of the world's largest internet companies, including Google Facebook, Microsoft, Apple, Yahoo and Skype. An investigation by the US Privacy and Civil Liberties Oversight Board debunked this claim, ruling that PRISM was legal and that its function was to better manage the data passed to the NSA from internet service providers in response to specifically targeted requests against individuals based outside of the US. In the UK, an investigation by the Intelligence and Security Committee came to a similar conclusion, reporting that only a tiny fraction of Internet traffic was ever looked at by GCHQ analysts.

> GCHQ's bulk interception systems operate on a very small percentage of the bearers that make up the internet. We are satisfied that they apply levels of filtering and selection such that only a certain amount of the material on those bearers is collected. Further targeted searches ensure that only those items believed to be of the highest intelligence value are ever presented for analysts to examine: therefore only a tiny fraction of those collected are ever seen by human eyes *(Intelligence and Security Committee of Parliament, 2015, p. 2)*.

There are many means through which it is possible for the public to protect themselves against state surveillance, including using end-to-end encryption provided by services such as WhatsApp and Apple Messenger, using Virtual Private Networks (VPNs), using full disk encryption, and using services such as Tor. Mathematically the advantage is also with the defender rather than the attacker as, despite the huge resources of GCHQ and the NSA, it is far less data intensive to encrypt data than it is to break that encryption. However, the secrecy of intelligence agency techniques, the huge range of potential attack vectors, constant reporting of new vulnerabilities and hints that services such as Tor have been compromised, mean that the public can never be sure of their own security (*ArsTechnica*, 2017). In 1993, Oscar Gandy proposed that modern communication techniques were creating a modern panopticon and this concept has since been applied several

times to GCHQ and NSA surveillance (Gandy, 1993; Sullivan, 2013). For the DRC, the offensive/defensive balance may always seem to be in favour of the state because they never actually know if they are being watched.

Legality

Prior to the passing of the IPA in January 2017, many within the DRC felt that the opaque nature of laws governing investigatory powers had enabled agencies such as GCHQ to engage in activities that threaten digital rights. But when these laws were rewritten and consolidated within the IPA, there was dismay that the state's powers had been expanded rather than restricted. Edward Snowden claimed that 'the UK has just legalised the most extreme surveillance in the history of western democracy' and ORG director Jim Killock claimed that '…the Bill will mean the police and intelligence agencies have unprecedented powers to surveil our private communications and Internet activity, whether or not we are suspected of a crime' (Snowden, 2016; Killock, 2016).

The state contests these allegations and claims that the IPA prevents the abuse of surveillance powers through measures such as tough sanctions against those misusing surveillance powers and the requirement for approval by the Secretary of State and a senior judge before intrusive powers are used (HM Government, 2016). Whilst welcoming some privacy-enhancing aspects of the act, the DRC fear that the IPA allows for the offensive use of surveillance powers, including mass surveillance and the targeting of those not suspected of a crime.

Oversight and Accountability

The DRC has often been critical of the oversight and accountability of UK intelligence and security agencies and has argued that legislation has not been strong enough to ensure that GCHQ's activities are legal and proportionate. The Intelligence and Security Committee, which oversees their activity, is often described as inadequate and ORG director Jim Killock has claimed that their activity 'is not an oversight: it is a policy of trust us, we know what we're doing' (Killock, 2015). Concern over insufficient oversight was strengthened by evidence from the Snowden disclosures, which revealed that in guidelines to the NSA, a GCHQ lawyer stated that 'we have a light oversight regime compared with the US', which was widely reported as GCHQ having boasted about its lack of oversight (GCHQ Lawyer, 2013).

Before the enactment of the IPA, the government acknowledged that surveillance powers required greater oversight, but Theresa May claimed that the 'Bill will establish world-leading oversight to govern an investigatory powers regime which is more open and transparent than anywhere else in the world' (May, 2015). The government claims that the IPA includes 'world-leading oversight', provided by a powerful new Investigatory Powers Commissioner who oversees the use of surveillance powers, which are subject to strict safeguards (HM Government, 2016).

Despite fierce criticism of the act, the ORG has welcomed the improvements it has made to surveillance oversight.

> A simplified oversight regime is positive and the Bill states that it will have dedicated legal, technical and communications support. Even if independent serving judges were responsible for signing warrants, an independent commissioner could help with technical issues and improve compliance, transparency and accountability (Open Rights Group, n.d.)

Whilst a simplification to the oversight regime is viewed positively, the ORG still consider this oversight to be too limited to adequately protect against abuses of state surveillance powers.

4.4.2.2 State Perspective

The defence-offence balance for the state relates to how easy it is for criminals and terrorists to use encryption to protect themselves, compared to how easy it is for the state to access their communications. This depends on the capability of the state to access online communications, the legal powers that facilitate this and the degree to which technology companies co-operate with the state to facilitate access to user data.

Capability

The police and intelligence agencies claims that security technologies such as encryption are becoming so powerful that terrorists and criminals are now better able to hide their activities from the authorities; the intelligence agencies are 'Going Dark' and the Internet is in danger of becoming anarchic (Comey, 2014).

> The levels of encryption and protection that we are seeing in the devices and methods used to communicate are frustrating the

> efforts of police and intelligence agencies to keep people safe. In a democracy we cannot accept any space - virtual or not to become anarchic where crime can be committed without fear. Yet this is in danger of happening (Hogan-Howe, 2014).

Following the Westminster terror attacks, Home Secretary Amber Rudd also complained about the inability of the intelligence agencies to access encrypted WhatsApp messages, calling the situation 'unacceptable' (Rudd, 2017). She used the analogy of steaming open envelopes and listening in to phone calls to re-enforce her case that the ability of terrorists and criminals to evade monitoring is greater than in the past.

Many within the DRC disagree with this assessment and claims that the state has access to more data on citizens and their activities than ever before. The Berkman Centre's report on the 'Going Dark' problem suggests that whilst the state might be losing access to some vectors of information, others are emerging to take their place.

> As data collection volume and methods proliferate, the number of human and technical weaknesses within the system will increase to the point that it will overwhelmingly likely be a net positive for the intelligence community … The label is "going dark" only because the security state is losing something that it fleetingly had access to, not because it is all of a sudden lacking in vectors for useful information (The Berkman Centre, 2016, p. 3 (appendix a)).

But this view is not shared by state actors such as Theresa May and Amber Rudd, who consider the capabilities provided by tools such as WhatsApp to be extremely detrimental to the ability of law enforcement to prevent and investigate crime and terrorism.

Legality

Following the enactment of the IPA, the British state and the DRC tend to agree that the intelligence agencies have significant legal authority to use their surveillance capabilities. The state views these powers as essential to combat terrorism and crime, whereas the DRC views them as threatening.

> The Investigatory Powers Act 2016 will ensure that law enforcement and the security and intelligence agencies have the

> powers they need in a digital age to disrupt terrorist attacks (HM Government, 2016).
>
> Amber Rudd says the Investigatory Powers Act is world-leading legislation. She is right, it is one of the most extreme surveillance laws ever passed in a democracy… The Bill will mean the police and intelligence agencies have unprecedented powers to surveil our private communications and Internet activity (Killock, 2016).

However, following the 2017 terrorist attacks in Manchester and London, the state has argued that, despite these powers, technology companies are still thwarting the ability of the intelligence agencies to access the data they need.

Co-operation

In the past few years, the British state has increasingly complained about efforts to resist state surveillance that have been undertaken by some technology companies. After the Westminster terrorist attack in March 2017 and reports that the perpetrator had communicated using WhatsApp shortly before the attack, Home Secretary, Amber Rudd voiced the state's frustration at being denied access to data due to the implementation of encryption and non-co-operation by technology.

> You can't have a situation where warranted information is needed, perhaps to stop attacks like the one last week, and it can't be accessed (Rudd, 2017).

Amber Rudd suggested that technology companies feel that they are different and do not need to comply with the law.

> We do want them [technology companies] to recognise that they have a responsibility to engage with government, to engage with law enforcement agencies when there is a terrorist situation. We would do it all through the carefully thought through legally covered arrangements, but they cannot get away with saying we are different. They are not (Rudd, 2017).

Rudd even questioned whose side technology companies are on.

> Where there are ongoing investigations with terrorists – these people have families, have children as well, they should be on our side (Rudd, 2017).

Technology companies deny that they facilitate terrorism, claim that they always comply with the law and report that they engage in extensive work to protect their users. In a response to Amber Rudd's comments, Facebook (the owner of WhatsApp) released a statement detailing much of the work they do to counter terrorism online.

> There's no place on Facebook for terrorism … When we receive reports of potential terrorism posts, we review those reports urgently and with scrutiny …. We believe technology, and Facebook can be part of the solution (Facebook, 2017).

Despite the view from technology companies that they make significant efforts to combat criminal and terrorist use of their networks and technologies, elements of the state still fear that their actions are serving to tip the offence-defence balance towards offensive (Rudd, 2017).

Despite the objections of the DRC and technology companies and new legal powers from the IPA, the state still fears that new technologies such as encryption are hampering its ability to defend against crime and terrorism. This notion that the offence-defence balance is tipping towards offence, serves to fuel the state's fears and serves to heighten the security dilemma.

4.5 Conclusion

The conflict between the DRC and the state is often viewed as binary, caused by either overzealous efforts by the state to fight terrorism and crime through surveillance, or by a lack of appreciation by the DRC of the scale of the threat to national security and the importance of data to the intelligence and security agencies. The conflict bears many of the hallmarks of a security dilemma, which has been made more intense by the pace of technological and political change. Limitations on the state's ability to govern cyberspace creates a state of anarchy between the state and the DRC, where neither can exert full authority and there is no mechanism to resolve disputes. Each side is focussed on their own security concerns but, fearing the actions of the other, takes measures to defend their own interests, creating an insecurity spiral that has resulted in the Crypto Wars. The CSD has been intensified by the difficulty in differentiating between defensive and offensive capabilities, with the defence/offence balance seemingly tilted towards offence.

The framing of the debate as surveillance versus encryption or encryption versus insecurity has created the illusion of incompatibility between national security and digital rights, but the security interests of the state and DRC are not necessarily in opposition to each other. The following chapters will discuss how this dilemma might be resolved.

5 RESPONDING TO CYBERSPACE SECURITISATION

Chapters 2 and 3 analysed the relationship between different securitising actors and how they use speech acts to securitise cyberspace, and Chapter 4 discussed how this securitisation has led to a CSD, which has created spiralling insecurity for both sides.

This chapter considers two further questions which arise from the previous chapters, each of which is related to the question of how we should respond to the securitisation of cyberspace and the creation of the CSD. Whilst the content of Chapter 4 would appear to support the conclusion that the desecuritisation of cyberspace is extremely desirable, it is not immediately obvious if this would be either ethical or effective. The first part of this chapter considers different approaches to the question of whether an issue should be desecuritised or not. These approaches are then applied to cyberspace to address the question of whether cyberspace should be desecuritised. The second part of this chapter then addresses the question of how cyberspace could be desecuritised using existing desecuritisation methodology. The chapter concludes by highlighting the limitations of desecuritisation and proposing a different approach. This approach is then discussed in Chapter 6.

5.1 APPROACHES TO SECURITISATION

Whilst the Copenhagen School refer to securitisation as undesirable, Securitisation Theory itself does not address the normative implications of securitisation and does not provide the tools by which a security analyst can determine whether an act of securitisation is desirable, undesirable, harmful or necessary. This weakness has led to significant criticism of the usefulness of the concept. McSweeney calls it 'sociologically untenable' and Erikson highlights the problem of 'adopting a securitization perspective and not acknowledging one's own responsibility for widening the security agenda' (McSweeney, 1996, p. 89; Erikson, 1999, p. 315). Michael Williams suggests that this problem has

> led many to ask whether despite its avowedly ''constructivist'' view of security practices, securitization theory is implicitly committed to a methodological objectivism that is politically irresponsible and lacking in any basis from which to critically evaluate claims of threat, enmity, and emergency (Williams, 2003, p. 521).

But there are several theoretical frameworks through which a security analyst can attempt to assess the positive or negative implications of any act of securitisation. Catherine Charrett categorises these responses to the normative dilemma as 'The Copenhagen School's Response', 'The Discursive Ethical Response' and the Consequentialist Response' (Charrett, 2009).

5.1.1 Copenhagen Approach

The Copenhagen School generally consider securitisation to be undesirable and insist that security should be viewed as a failure of politics (Busan, et al., 1998). Desecuritisation is considered 'the optimal long-range option', since it results in issues not being framed as 'threats against which we have countermeasures but moves them out of this threat-defence sequence and into the ordinary public sphere' (Waever, 1995, p. 29). However, the Copenhagen School also contend that securitisation can have its uses and may be unavoidable in the face of a 'barbarian aggressor'. It can also have 'tactical attractions … for example, as a way to obtain sufficient attention for environmental problems' and can be desirable if it is the only way to raise a depoliticised issue onto the political agenda (Busan, et al., 1998, p. 29).

> When considering moves such as "environmental security" or a "war on crime," one has to weigh the always problematic side effects of applying a mind-set of security against the possible advantages of focus, attention and mobilization. Thus, although in the abstract desecuritization is the ideal, in specific situations one can choose securitization *(Busan, et al., 1998, p. 29)*

This stance by the Copenhagen School makes uncomfortable reading because the contention that some threats are significant enough to be justly securitised is at odds with the central contention of Securitisation Theory – that threats are social constructions. The Copenhagen School claim that the concept of securitisation allows for the 'problematizing of both actual securitisation and the absence of securitisation' but it does not provide the tools by which to judge whether an issue suffers from too much or too little securitisation (Busan, et al., 1998, p. 40). This is left open for the security analyst to determine through their own means.

The CS's overarching view that securitisation is generally a negative process and that desecuritisation is generally preferable is widely reflected within the securitisation literature (Georgieva, 2015; Kingsmith, 2013; Lazaridi, et al., 2015; Hughes, 2007). The only significant issue where the necessity for securitisation is widely debated in academic literature is that of environmental security. Rita Floyd,

for example, provides a good overview of arguments for and against the securitisation of climate change, addressing arguments that securitisation can raise climate change onto the agenda. But she concludes that 'the securitisation of climate change is a double-edged sword' as it can lead to negative effects on the most disadvantaged members of international society (Floyd, 2008, p. 63).

Whilst some agree with the Copenhagen School that some instances of securitisation may be beneficial, others including Claudia Aradau, argue that securitisation is, at its heart, a negative concept because it bypasses good political processes, delivers unethical outcomes and relies on a Schmittian politics of enmity[23] (Aradau, 2004; Schmitt, 1932). Aradau argues that securitisation is bad for democracy as it creates states of exception and urgency which inhibit the processes of normal political debate. 'The speed required by the exceptional suspends the possibilities of judicial review or other modalities of public influence upon bureaucratic or executive decisions' (Aradau, 2004, p. 392). Groups such as the ORG reflect Aradau's concerns about rushed decision making and legislation relating to cybersecurity. In 2014, following the introduction of emergency legislation, the 'Data Retention and Investigatory Powers Bill' completed its passage through parliament in one day. Several groups complained about the lack of scrutiny that it had received.

> The Government announced legislation this morning forcing Internet Service Providers and phone networks to carry out blanket retention of your phone calls, your texts, and your Internet browsing history … they're pushing this legislation through with hardly any debate in Parliament ... Rushing through legislation that is so controversial should never be done (Open Rights Group, 2014).

The ORG also responded in a similar fashion to news of the progression of the Investigatory Powers Bill in 2017 claiming that 'the Home Office is treating the British public with contempt if it thinks it's acceptable to rush a Bill of this magnitude through Parliament' (Killock, 2016).

Aradau also argues that securitisation creates 'us/them, 'friend/enemy' politics, which generates winners and losers based upon the acceptance or not of a

[23] Based upon Carl Schmitt's focus on a friend/enemy dichotomy where an enemy can be anyone for whom there is enmity towards.

particular act of securitisation. This is demonstrated in the court case between Apple and the FBI, where only one side could emerge victorious.

Other authors have challenged the view that securitisation must always deliver negative outcomes. Paul Roe argues that whilst securitisation may lead to the expedition of legislation, it does not result in the abandonment of political practices altogether. 'While the legislative process is surely accelerated, a degree of scrutiny and oversight nevertheless remains' (Roe, 2012, p. 260). It can also be argued that in specific scenarios, the ability to fast-track emergency legislation is necessary, even if that may lead to less scrutiny than is desirable. This point was made by the then Home Secretary Theresa May following the passage of the emergency 'Data Retention and Investigatory Powers Bill', which was passed as an emergency stopgap after previous legislation was about to expire.

> If we delay we face the appalling prospect police operations will go dark, that trails will go cold, that terrorist plots will go undetected. If that happens, innocent lives may be lost (May, 2014).

In what he calls the securitisation of securitisation Michael Williams engages with the negative role that fear plays in driving securitisation, but argues that this force can be harnessed to inhibit processes of securitisation instead (Williams, 2011). If actors fear making securitising moves or audiences are fearful of securitising moves then this fear can prevent an issue from becoming securitised in the first place. Williams' securitisation of securitisation can be seen within the cybersecurity discourse. Members of the DRC, for example, attempt to securitise state securitisation of terrorism by arguing that surveillance measures are worse than terrorism.

> We've been asked to sacrifice our most sacred rights for fear of falling victim to [terrorism] (Snowden, 2013).

State actors make a similar claim about privacy, arguing that the DRC's securitisation of state surveillance is more threatening than state surveillance itself.

> Privacy is important, but … the levels of encryption and protection that we are seeing in the devices and methods used to communicate are frustrating the efforts of police and intelligence agencies to keep people safe (Hogan-Howe, 2014).

The major problem with the Copenhagen School approach is that whilst it provides a good case for why securitisation is generally desirable, it also suggests that this may not always be the case, without providing the tools to judge when this might be. Alternative approaches attempt to address this deficiency.

5.1.2 Discursive Ethical Approach

Authors including Michael Williams and Wyn Jones advocate for a 'Discursive Ethical Approach' to securitisation, which includes a process of legitimisation that helps to determine whether securitising claims are true or false. Speech acts should be challenged and scrutinised, thereby facilitating the refutation and rejection of negative acts of securitisation or the acceptance of acts that are based upon truthful and accurate claims.

Whilst the approach is appealing, it has several limitations, some of which are highlighted by Wyn Jones and Williams themselves (Williams, 2003; Jones, 1999). The first limitation is that a security analyst cannot ensure that speech acts will be scrutinised for validity given the power relations at play within the securitisation process. An analyst may refute a securitising claim, but unless they have the authority and reach to convince an audience of their case, then they are powerless to stop the issue from becoming securitised. The deployment of discursive ethics 'does not mean that securitisations will always be forced to enter the realm of discursive legitimization' (Williams, 2003, p. 524). Another problem with the discursive ethical approach is the issue of who should make the judgement about the validity of the securitising actor's claims, and what tools does an analyst or the audience possess to ensure that they can scrutinise the claim free of their own internal biases?

The final limitation is the requirement for an analyst to assess the validity of a securitising act by assessing whether the threat is or isn't real. This clashes with the primary claim of the Copenhagen School that threats are constructed rather than based on objective reality. If threats are constructed by speech acts, then a security analyst has no means within the constructivist approach to enable them to determine the validity of these threats.

5.1.3 Consequentialist Approach

The Consequentialist approach judges an act of securitisation by its outcome rather than its processes. If an act of securitisation is well intended and results in appropriate security responses, then it can be considered ethical, otherwise it is

unethical. The ethics of securitisation and security are considered to be issue dependent rather than black and white. Rita Floyd takes a consequentialist approach to the normative dilemma of securitisation by drawing on 'Just War Theory' to formulate a 'Just Securitisation Theory' (Floyd, 2011). Floyd proposes the introduction of three criteria, which if met would render an act of securitisation morally legitimate;

1.) There is an objective existential threat;
2.) The referent object of security is morally legitimate;
3.) The security response is appropriate to the threat in question.

To achieve this Floyd extends the scope of Securitisation Theory beyond the acceptance or not of a threat, to include the security response to this threat as well. She admits that the Copenhagen School would 'be deeply uncomfortable with all parts of the analysis' because it requires threats to be considered as objectively real rather than constructed, but she also argues that her work simply extends the Copenhagen School approach into ethics (Floyd, 2011, p. 437). 'Setting criteria that determine the moral rightness of securitisation is akin to the Copenhagen School setting criteria that determine both the existence of securitisation and its success' (Floyd, 2011, p. 436). Securitisation Theory applies a formulaic process to help determine how threats are constructed and Floyd argues that she simply extends this formulaic process to include judgements as to whether the securitisation is moral or not. Floyd's approach is appealing because, by including ethical considerations, it broadens the potential usage of Securitisation Theory. It could also bring together traditionalists and critical security studies proponents because it considers threats to be both objective and constructed.

Just War theory is subject to substantial criticism, which could equally be applied to Just Securitisation Theory, including the criticism that no theory can be considered ethical if it ever justifies war/securitisation. The main issue with Just Securitisation Theory, however, is deciding who can make the judgement as to the ethics of an act of securitisation. Those with the authority and reach to determine the justness of an act are likely to be the same actors who have the power and authority to securitise an issue in the first place. In addition, by calling for an assessment as to whether the 'security response is appropriate to the threat in question' Floyd undermines the need for Securitisation Theory at all (Floyd, 2011, p. 427). If we can simply make an ethical assessment of the appropriateness of

security measures then we do not need to question their origins, simply whether they are appropriate or not.

5.2 SHOULD CYBERSPACE BE DESECURITISED?

Desecuritisation is the process by which an issue is removed from the security sphere and is no longer considered to be an urgent threat, requiring exceptional measures to counter. For the Copenhagen School, 'it means not to have issues phrased as "threats against which me have countermeasures" but to move them out of this threat-defense sequence and into the ordinary public sphere' (Busan, et al., 1998, p. 29).

But desecuritisation is difficult to achieve once an issue has been accepted as threatening and desecuritisation does not guarantee than an issue will become re-politicised and re-open to public debate. If securitising moves are rejected forcefully enough, then issues can become both de-securitised and de-politicised (See Figure 5.1). This means that not only are the issues considered non-threatening, but they are also closed for discussion. Islamic extremism and

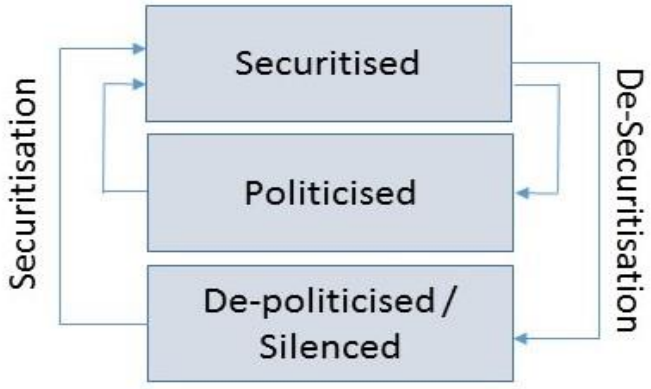

Figure 5.1: Securitising and Desecuritising

immigration are issues that are often difficult to discuss in a political environment because they are either securitised as existentially threatening or de-politicised because the responses to them are considered threatening, racist or intolerant.

Cyberspace scholars are in general agreement that cyberspace securitisation has mainly negative consequences. Kingsmith, for example, discusses the negative consequences that emerge from moves by states to securitise internet content.

> Considering these securitising moves … the more that filtering practices are withheld from public scrutiny and accountability, the more tempting it is for framing authorities to employ these tools

> for illegitimate reasons such as the stifling of both opposition and civil society networks (Kingsmith, 2013, p. 1).

Deibert also highlights the negative consequences of the securitisation of cyberspace, including the resultant threats to basic freedoms.

> There has been a growing recognition of serious risks in cyberspace. The need to manage these risks has led to a wave of securitization efforts that have potentially serious implications for basic freedoms (Deibert & Rohozinski, 2010, p. 49).

Whilst arguing that the securitisation of cyberspace is negative and inevitable, Deibert also contends that the form of this securitisation can be influenced. 'The securitization of cyberspace may be inevitable, but what form that security takes is not' (Deibert, 2012, p. 274). He suggests that it is better to securitise threats to human rights than to securitise threats to national security. Mariya Georgieva takes this further, citing the Snowden disclosures as an example of the securitisation of digital rights, arguing that Snowden had 'successfully shifted the focus of the securitisation of cyberspace from values such as the survival of the state and effective national security to the survival of privacy and personal choice' (Georgieva, 2015, p. 44). Whilst she celebrates this shift she does not explain why it is better to securitise privacy rather than national security. Helen Nissenbaum is one author who does take a more consequentialist approach to cyberspace securitisation, arguing that it might be justified when the threat is as extreme as its proponents claim.

> If those who subscribe to a conception of security as cybersecurity are right, particularly if the magnitude of threat is as great as those on the extremes claim, then an extraordinary response is warranted despite its chilling effects (Nissenbaum, 2005, p. 73).

However, this approach is rare and most literature is either critical of state surveillance and the securitisation of cyberspace, or is complimentary of Edward Snowden and supportive of the securitisation of individual privacy. Given that a narrow majority of the British public support greater efforts to protect national security it is surprising that academic literature is weighted so strongly towards criticisms of state surveillance and the securitisation of national security (Pew Research Centre, 2016). Even when cyberspace securitisation by non-state actors is addressed, such as in Georgieva's work on Snowden as an alternative securitising

actor, these forms of securitisation are considered positive because they support human rights. In the US and UK, academics have also been politically active in opposing state surveillance. In 2014 over one thousand scholars from a wide range of disciplines formed the 'academics against surveillance' campaign, which published an open letter criticising state surveillance (Electronic Frontier Foundation, 2014).

Whilst there is disagreement over whether desecuritisation is always best and what types of securitisation should be reversed, there are a variety of means through which desecuritisation can be achieved.

5.3 How might we desecuritise cyberspace?

Desecuritisation can be achieved through replacement, counter-securitisation, silencing, de-escalation or rearticulation of the problem. These can be applied separately or in combination with each other.

5.3.1 Replacement (Competing Securitisation)

Replacement occurs when one act of securitisation is replaced by another that relates to a greater threat, requiring a more urgent and substantial response. One example is attempts to replace the securitisation of state surveillance with the securitisation of the activities of technology companies. MP Ben Wallace attempted to achieve this when he argued that technology companies are a greater privacy threat than the state.

> The big capitalist companies in America … harvest our data without your leave, sell it on to intermediaries on and on and on. They make millions, billions of pounds … and that's the area that needs regulating and protection… I'd rather have the state than the private sector all over the world grooming through my internet capabilities (Wallace, 2013).

Others, such as Estonian MP Indrek Tarand, have suggested that state hacking from Russia and China[24] is a greater threat than state surveillance by the UK and US.

> For me, US spying cannot be a bigger problem than Chinese or Russian spying. And, here in the Parliament, unfortunately, we

[24] For example, hacks on the DNC and New York Times

> always speak about the US but tend to forget that other big powers are doing the same (Tarand, 2014).

Replacement does not necessarily aim to debunk the original threat construction, but this threat becomes replaced in the audience's minds by an even more significant one.

5.3.2 Counter-Securitisation

An issue is counter-securitised when the consequences of securitisation are deemed more threatening than the original threat. Counterterrorism measures, for example, are often argued to be a greater threat to freedom and liberty than terrorism itself (Ogilvie, 2016).

Counter securitisation is prevalent in cybersecurity discourse because measures to promote digital rights and national security are often considered to be threatening to the other side. Individuals such as Edward Snowden argue that the securitisation of terrorism has led to state surveillance, which is more dangerous than the terrorist threat itself.

> It may be that by watching everywhere we go, by watching everything we do, by analyzing every word we say, by waiting and passing judgment over every association we make and every person we love, that we could uncover a terrorist plot, or we could discover more criminals. But is that the kind of society we want to live in? (Snowden, 2014).

Conversely, state actors argue that the securitisation of state surveillance has led to an increased roll-out of encryption and other enhanced security measures, which are now the greater threat.

> Privacy is important, but in my view the security of communications methods and devices is growing beyond what any genuine domestic user could reasonably require. The levels of encryption and protection that we are seeing in the devices and methods used to communicate are frustrating the efforts of police and intelligence agencies to keep people safe (Hogan-Howe, 2014).

Counter-securitisation does not address the issues of securitisation but merely focusses attention in a different direction.

5.3.3 Silencing

Silencing occurs when an issue is not only de-securitised but is also eliminated from political discourse. This can occur when the issue at hand is considered so toxic that it is no longer open for public debate, the securitising actor is widely discredited or the securitising move is somehow suppressed.

Examples of toxic issues include the concepts of backdoors, key escrow and weakened encryption, which are considered by many members of the DRC and much of the technology community to be inherently threatening and closed to debate (Schneier, 2015; Abelson, et al., 2015).

Individuals or institutions can be silenced by undermining their qualifications to speak security, undermining their trustworthiness and motivations, and denying them a platform from which to speak. This may involve dehumanising the securitising actor, portraying them as evil or ignorant, or making it difficult for others to associate with their cause. The use of the term 'snoopers' charter' to refer to the Investigatory Powers Bill implies that the beneficiaries of the bill are motivated by a desire to pry into other people's business. It discredits them and therefore seeks to silence their arguments. A similar concept applies to Edward Snowden, who was widely labelled as a traitor when he disclosed material from the NSA and GCHQ**.** The official US House of Representatives report into Snowden's disclosures described Snowden as 'a serial exaggerator and fabricator' saying that he had demonstrated a 'pattern of intentional lying' throughout his career and following the disclosures (US House of Representatives, 2016, p. iii).

Attempts can also be made to silence an issue by denying it attention. GCHQ describe how they attempted to silence the Snowden revelations by starving them of oxygen.

> The organisation struggled to react to Snowden in a way. We were previously secret with no public face. When the news broke we didn't know how bad it would be. By the time we realised what had happened and were ready to react the horse had already bolted. The reaction was slow and coated in fear. We tried to starve the story of oxygen by not commenting on it (Fiona, 2016).

But silencing does not always work. Having initially attempted to silence the issue by not commenting, GCHQ eventually realised that they had instead only silenced themselves.

> …but then when we realised that was not working we started to engage but it has taken a long slog to build up relationships and get to the situation we are in today, which isn't perfect. But so much damage was done by not commenting. Someone else had told our story. The headlines were sensational. It was compelling but it was wrong (Fiona, 2016).

Attempts to silence issues can be high risk because, whilst speakers can be silenced and concepts can be removed from public debate, this can result in ideas becoming repressed and emerging later in more extreme forms.

5.3.4 De-escalation

De-escalation involves the securitising actor or other influential force reducing the claimed likelihood, imminency or impact of a threat so that it can be dealt with through ordinary means. There have been several attempts to de-escalate cyberspace threats relating to both surveillance and national security. The Berkman centre report on the 'Going Dark' threat attempts to de-escalate the issue by highlighting the vast volumes of information that law enforcement have access to (The Berkman Centre, 2016). During the conflict between Apple and the FBI, Tim Cook also made a similar effort to de-escalate the 'Going Dark' threat.

> We shouldn't all be fixated just on what's not available. We should take a step back and look at the total that's available. Because there's a mountain of information about us (Cook, 2016).

Edward Snowden has also attempted to de-escalate the 'Going Dark' threat by referencing a case where the FBI had gained access to a Dark Web drug dealer's encrypted laptop by following him and seizing the laptop when it was logged on (Snowden, 2016). He argued that normal policing could be used to counter encryption, therefore the 'Going Dark' problem is not as significant as claimed.

The state has also attempted to de-escalate the threat that it poses to digital rights. The National Cyber Security Strategy, for example, contains a whole section titled 'balancing security with freedom and privacy', which explains how the state will preserve 'UK citizens' rights to privacy and other fundamental values and freedoms' (HM Government, 2011, p. 22). Whilst making speeches warning of cyberspace threats, state representatives also frequently claim that they protect digital rights rather than threaten them. In speeches about cyber threats, Sir Bernard Hogan-Howe agreed that 'privacy is important', former Head of GCHQ, Robert Hannigan,

claimed that ‘we have a good story to tell about privacy’, and former Head of MI5, Jonathan Evans claimed that ‘any suggestion that the [Investigatory Powers Acts] powers will be used to ‘snoop’ on the innocent activities of ordinary people is absurd’ (Hogan-Howe, 2014; Hannigan, 2014; Evans, 2016).

Whilst de-escalation is often a useful tool, it can be difficult to achieve because it is far easier to talk a threat into existence than to talk it out of existence.

5.3.5 Re-articulation

Re-articulation occurs when a securitised issue is recast in entirely new terms. An issue may still be accepted as real but is no longer viewed in security terms. Re-articulation is arguably the most difficult form of de-securitisation to achieve, since it involves a fundamental shift in how people conceptualise security, but it can have profound effects, as demonstrated by the peace process in Northern Ireland. During the troubles, Sinn Fein was considered the political arm of the IRA and constructed as a threat to the integrity of the UK, but since the signing of the Good Friday agreement in 1998, their increased role in Northern Irish politics has been rearticulated as a positive sign of a developing peace. Whilst many still consider Sinn Fein to represent terrorism, many others who originally considered them a threat now see them as part of the solution.

Re-articulation of threats to national security and digital rights would see the DRC consider GCHQ as an ally in their efforts to protect digital rights, and the state consider the DRC as essential to the provision of good cybersecurity.

5.4 The Limitations of Desecuritisation

One of the main reasons that cyberspace is difficult to desecuritise is that securitisation is now well established, constantly re-enforced, and the audiences which accept these securitisations have become entrenched in their views. As the preceding chapters have demonstrated, securitisation has been achieved through hyper securitising rhetoric that portrays surveillance and national security threats as existentially threatening, and this rhetoric is strengthened with linkages to fears of authoritarianism, totalitarianism, anarchy and terrorism.

Audience acceptance of threats is also influenced by political ideology, with those fearful of the state placing much greater trust in the securitisations of whistle-

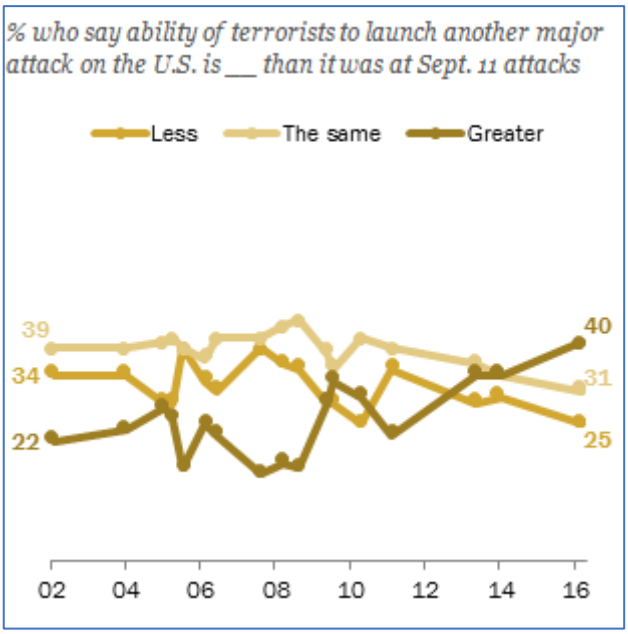

Figure 5.2: American views on terrorist threat

blowers[25] such as Edward Snowden and those more fearful of external threats, such as terrorism, placing far greater trust in the securitisations of the state. In addition, cyberspace securitisations are constantly re-enforced by daily events, with instances of terrorism or cyber breaches re-enforcing the national security threat, and daily reports on the state's surveillance powers re-enforcing the state surveillance threat.

It is also far easier to securitise an issue than it is to desecuritise it. Once an audience has accepted the existence of an existential threat, it is difficult to convince them that this threat does not exist, or is far less dangerous than first thought. This is most evident in reactions to terrorism and the war on terror, although can be applied equally to cyberspace. In 2010, 25% of the British population believed that the threat of terrorism had grown in the past five years compared to 17% who believed it had shrunk. By 2016, the percentage of people believing that the threat had grown was 74% compared to only 1% who believed it had shrunk (YouGov, 2016) (see Figure 5.3). Supporters of all political parties believed that the terror threat had increased, but this belief was stronger on the right of British politics (Conservative -84%, UKIP – 83%, Labour – 71%, LibDem – 74%). In the US, when

[25] For his supporters, Snowden is a whistle-blower, but for his detractors he is a criminal who has illegally disclosed millions of classified documents.

asked how they would rate the chances of themselves or a member of their family or a good friend being killed or wounded in a terrorist attack, 12% of people responded with 'Very high' or 'Fairly High'. This belief appears at odds with the fact

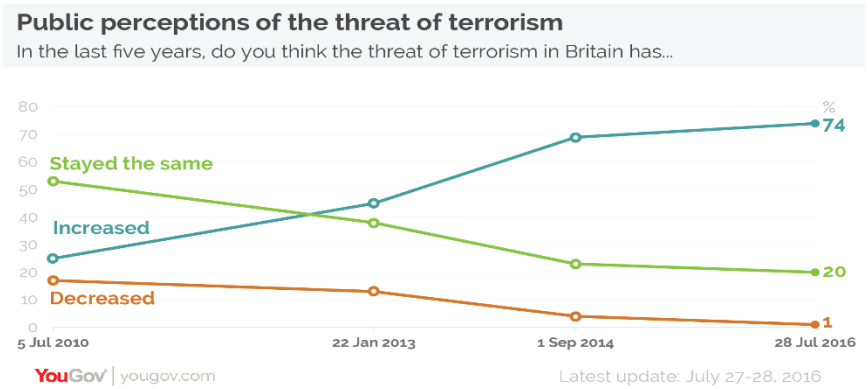

Figure 5.3: British view on terrorist threat

that the US had not suffered a mass casualty terrorist attack since 2001.

There have been several attempts to explain the discrepancy between the fear of terrorism and the actual risk of being affected by it (Nellis, 2009; Altheide, 2016; Braithwaite, 2013). These demonstrate how the visceral images of terrorist attacks such as 9/11, the constant re-enforcing of the threat, hatred of 'the other' and the uncertain nature of the threat, combine to create an emotional response to terrorism. Studies have also demonstrated that it is not necessary to have been present at a terrorist attack or to have been directly affected by one, to experience significant symptoms of anxiety and stress in otherwise healthy citizens (Collins, et al., 2001).

This emotional response to the threat of terrorism renders logical arguments against it less effective and psychological studies have repeatedly demonstrated that logical arguments are rarely effective against existing views. An experiment in Stanford, for example, demonstrated that when students were provided with fictitious information, they still based their opinions on this information even when it was revealed that the data was false (Ross & Mark Lepper, 1975). A related study at Stanford a few years later revealed that not just opinions, but people's beliefs and values, which had been formed based upon false information, were not changed even when the information that lead them to form these beliefs was shown to be false (Anderson, et al., 1980). According to another study 'corrections actually increase misperceptions among the group in question' (Nyhan & Reifler, 2010, p. 303). The authors call this the backfire effect and suggested that if people

counter-argue unwelcome information they may end up entrenching views that are more extreme than those originally held.

Fear and anxiety play a significant role in risk perception.. And for those in fear, encountering those who deny the existence of the threat can lead to greater anxiety since the burden of facing that threat is considered greater when others do not accept its existence. Common advice to help people reassure those with anxieties is that fears should not be invalidated, but should be accepted as real to those who hold them. When confirmation bias (which explains how people selectively interpret new information to support their existing beliefs) is also considered, it becomes clear that challenging attitudes to cyberspace threats is not as simple as presenting the case for the other side. Once an issue has become securitised, it is extremely difficult to convince the audience that their acceptance of the threat is wrong. This difficulty was demonstrated following the enactment of the IPA. Some at GCHQ thought that the act would 'defeat claims of mass surveillance' but this notion was dispelled after its passing when the ORG described it as 'one of the most extreme surveillance laws ever passed in a democracy' (David, 2016) (Killock, 2016).

5.5 CONCLUSION

The consequentialist approach appears to be the most applicable to the securitisation of cyberspace but it is still extremely problematic. Determining whether state surveillance has an overall negative or positive impact on the world cannot be achieved objectively and individuals and academics will continue to hold different views based upon their own ethics, values and subjective experience of the world. But whilst it is extremely difficult to reliably determine the ethics of particular acts of securitisation, it might be possible to apply the consequentialist approach collectively to the two competing securitisations that lie at the heart of the CSD. When considering the case of Apple versus the FBI, it is not necessary to make a judgement about the validity of each side's securitising claims in order to judge whether the dispute as a whole was undesirable. Viewed as a whole, it is clear that competing securitisations caused both Apple and the FBI to take hardline positions, which lead to conflict, enmity and an outcome that was in neither side's interests.

Instead of attempting to address acts of securitisation, it might be more effective to address the root cause of these acts - the genuine fear of cyberspace threats,

which exists on each side of the debate, the fear that the actions of the other side are making things worse, and the animosity and distrust that this creates. These issues are at the heart of the CSD and thus, to desecuritise cyberspace, the CSD must be overcome. The following chapter uses examples from the dispute between the state and the DRC to help understand the failure of past approaches and then proposes some general principles that can be used to overcome the CSD.

6 OVERCOMING THE CYBER SECURITY DILEMMA

Chapter 5 concluded that, rather than addressing and contesting particular acts of cyberspace securitisation, it would be more useful to address the root causes of the security dilemma, which include the genuine fear of cyberspace threats that exist on each side of the debate, the fear that the actions of the other side are making things worse, and the animosity and distrust that this creates. This chapter considers current and historic attempts to overcome the CSD and discusses why these have not been successful. From these conclusions, it then establishes several guiding principles that could be used to help overcome the CSD in the future.

6.1 HISTORY REPEATING ITSELF

Despite the passage of time and the rapid development of technology, the arguments on both sides of the Crypto Wars and the CSD have not changed very much in the past few decades. This is demonstrated by considering the similarities in the FBI's statements on encryption made by Louis Freeh in 1997 and James Comey in 2014 (Electronic Frontier Foundation, 2014).

> We believe that unless a balanced approach to encryption is adopted… the ability of law enforcement to investigate and sometimes prevent the most serious crimes and terrorism will be severely impaired. Our national security will also be jeopardized (Freeh, 1997).

> Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority…. And if the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place (Comey, 2014).

The arguments from members of the DRC have also remained very similar. In 1997 eleven prominent cryptography experts, including Whitfield Diffie, Bruce Schneier, Ron Rivest and Ross Anderson, collaborated on a paper on the unworkability of key escrow, which was designed to provide support to the arguments of the DRC (Abelson, et al., 1997). In 2015 the same authors, along with a few additions, wrote a very similar paper on the danger of government-imposed mandates on access to encrypted data (Abelson, et al., 2015). Once again, the paper was designed to

support the DRC in the face of renewed government calls for access to encrypted data.

The Open Technology Institute (OTI) asks whether we are 'doomed to repeat history' and fail to learn from the mistakes of the first Crypto Wars, arguing that much of the debate is a repeat of what has gone on before *(Kehl, et al., 2015, p. 21).*

> They [the government] have revived many of the arguments they made about encryption in the 1990s, seeming to have forgotten the lessons of the past. In response, encryption proponents have countered with many of the same arguments that they made in the 1990s (Kehl, et al., 2015, p. 21).

The OTI conclude that the arguments have been settled, the case for digital rights has emerged victorious, and governments should just accept that they have lost. But this is a simplistic argument, which fails to appreciate the reason why the Crypto Wars have re-emerged[26]. For the state, the issue was never resolved because their security concerns were never addressed. The fear that encryption is harming law enforcement and making areas of cyberspace ungovernable still exists and, due to the exponential growth in online communication, this fear is only becoming more pronounced (Comey, 2014). Whilst the DRC frequently point to the success of encryption as evidence that they were right all along, the state can point to evidence that unbreakable encryption has led to an outbreak of illicit behaviour in cyberspace (Hogan-Howe, 2014). Ungovernable marketplaces on the Dark Web that deal in drugs, weapons and child pornography, encrypted communications between terrorists that are inaccessible to law enforcement, and the use of online anonymity to spread extreme ideology are evidence for the state that unrestricted use of encryption is damaging their ability to maintain law and order (Rudd, 2017; Moore & Rid, 2016; Intelligence and Security Committee of Parliament, 2014). The issue is far from resolved.

6.2 Attempts to Overcome the Security Dilemma

Over the last forty years, there have been many attempts to resolve the CSD and end the Crypto Wars. Each side has attempted to 'win' the Crypto Wars but, on each occasion, the dispute has re-emerged after the 'losing' side has refused to

[26] Or never went away

accept the new reality (Foundation for Information Policy Research, 2005). There have also been attempts to solve the CSD in a more collaborative manner by finding solutions acceptable to both sides. Technical solutions like David Chaum's Privategrity have sought to provide strong encryption for the 'good guys' but prevent this from being used for 'evil'. 'Peace talks' between the state and the DRC have also been attempted with varying degrees of success. But a resolution of the Crypto Wars is proving elusive and a spiralling cycle of action, counter-action and fear has resulted in greater insecurity for all. This section considers both unilateral and collaborative approaches to the CSD, and how successful they have been.

6.3 Unilateral Attempts to 'Win' the Crypto Wars

Both state actors and members of the DRC have attempted to use a range of techniques to overcome the CSD by either winning or gaining the advantage in the Crypto Wars. The state has developed hacking techniques, targeted encryption directly and attempted to use legislation to ensure that it has access to the intelligence it needs to provide security, whilst the DRC has sought to develop and promote a wide range of security and encryption techniques to ensure that individual privacy and security is protected. In each of these examples, each side has attempted to address their own security issues, with little or no consideration of the impact that this would have on the other side.

6.3.1 State Attempts to win the Crypto Wars

Whilst the British and American establishments have always acknowledged and promoted the virtues of encryption, they have also always maintained that ubiquitous unbreakable encryption poses a significant threat to national security (Comey, 2014). For the state, the perfect solution to the problem of encryption is for the public to use encryption that is unbreakable to anyone but themselves. This has been the focus of much of the intelligence agencies efforts on encryption and has taken several forms, including undermining encryption, hacking, and using legislation to force companies to facilitate state attempts to access user data.

This approach is reflected in an NSA document leaked by Edward Snowden which provides details of a project to influence the design of commercial products to make them accessible to interrogation by the NSA and GCHQ.

> 'These design changes make the systems in question exploitable through SIGINT collection with foreknowledge of the modification.

> To the consumer and other adversaries, however, the system's security remains intact' (*New York Times*, 2013).

On paper, this approach would appear to be effective for GCHQ and the NSA but, as the examples demonstrate, it often creates a backlash that makes the job of the intelligence agencies even more difficult.

Undermining encryption

Due to the strength of modern encryption algorithms, GCHQ and the NSA have had to seek different means to access data when they have been unable to crack the encryption that is used. The Snowden disclosures revealed that the BULLRUN and EDGEHILL programmes at the NSA and GCHQ respectively, deployed several tactics to bypass encryption, including stealing encryption keys, hacking into systems or persuading vendors to install backdoors (The Guardian, 2013). However, of all the techniques that GCHQ and the NSA have utilised, it is the undermining of encryption itself that has most angered the DRC and has created a significant backlash and breakdown of trust. Evidence for the deliberate undermining of encryption was provided in an NSA budget request leaked by Edward Snowden that detailed how the NSA 'actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products designs' in order to enable 'expanded network operation and intelligence exploitation', whilst leaving systems security intact (*New York Times*, 2013). Methods of achieving this include attempts to 'insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets' and attempts to 'influence policies, standards and specification for commercial public key technologies' (*New York Times*, 2013).

Whilst British and American intelligence agencies feel that their ability to access encrypted communications helps to protect national security, the DRC feel strongly that this approach has done more harm than good. This was expressed by several academics, who jointly published an Open Letter reflecting their concerns following the Snowden disclosures (Paterson, et al., 2013).

> The first set of publications based on Edward Snowden's files were concerned with surveillance of internet communication happening more indiscriminately and on a much larger scale than previously thought. The more recent publications, presenting the systematic

> undermining of cryptographic solutions and standards, are the cause of much more substantial worry (Paterson, et al., 2013).

Other commentators, such as security researcher Bruce Schneier, were concerned that the actions of GCHQ and the NSA undermined trust and threatened the fabric of the Internet itself.

> Cryptography forms the basis for trust online. By deliberately undermining online security in a short-sighted effort to eavesdrop, the NSA is undermining the very fabric of the internet (Schneier, 2013).

Technology firms also expressed concern at the revelations. Microsoft said it had 'significant concerns' about the activities of GCHQ and the NSA, and Yahoo said it feared 'substantial potential for abuse' (The Guardian, 2013). As a result, technology companies accelerated and enhanced their own use of encryption and began to view the intelligence agencies as more of an adversary. Eric Groose, Vice President for security engineering at Google, described the situation as an 'arms race' between Google and the intelligence agencies (*Washington Post*, 2013). Google significantly accelerated their program to encrypt traffic between data centres, and Apple introduced end-to-end encryption by default on the iPhone (*Washington Post*, 2013).

The then US Director of National Intelligence, James Clapper, acknowledged the problem, claiming that 'as a result of the Snowden revelations, the onset of commercial encryption has accelerated by seven years' (Clapper, 2016). Whilst many would claim that an acceleration of cybersecurity is a good thing, Clapper explained that 'from our standpoint, it's not … it's not a good thing' (Clapper, 2016). The disclosures have had 'a profound effect on our ability to collect, particularly against terrorists' (Clapper, 2016). Whilst Clapper blamed Snowden for the accelerated provision of commercial encryption, the NSA themselves could also be blamed for their overzealous approach to breaking encryption. GCHQ and the NSA's efforts to protect national security by undermining encryption also undermined trust, triggering a counter-response within the DRC, which has subsequently made intelligence collection efforts more difficult.

Hacking

One of the ways by which GCHQ and the NSA seek to mitigate the 'Going Dark' problem is to use their technological capabilities and expertise to gain access to information through Computer Network Exploitation (CNE), or 'hacking' in standard parlance. The capability was first disclosed within the Snowden disclosures, but was confirmed for the first time by GCHQ during a case brought against them at the Investigatory Powers Tribunal (Bowcott, 2015). In 2013, 20% of GCHQ's intelligence reports contained information derived from hacking. In 2016, Foreign Secretary Philip Hammond said that 'the ability to exploit computer networks plays a crucial part in our ability to protect the British public' (Hammond, 2016).

Hacking is a three-stage process that involves identifying a vulnerability in a piece of software or hardware, writing an exploit to be used against that vulnerability, and deploying that exploit against the target. Whilst targeted hacking might be deemed more acceptable to the DRC than mass surveillance, many argue that state hacking undermines security because of the requirement of states to hoard vulnerabilities. Digital Rights activists such as Bruce Schneier argue that, rather than protecting national security, 'hoarding zero-day vulnerabilities is a bad idea. It means that we're all less secure' (Schneier, 2016). Evidence to support this case comes from the WannaCry attacks of 2017, which exploited a vulnerability discovered by the NSA and utilised elements of NSA software that were leaked onto the Internet.

The EternalBlue exploit was believed to have been developed by the NSA and used for around five years to gain access to computers using the Microsoft Windows operating system. The exploit was extremely powerful, and according to NSA employees, it was like 'fishing with dynamite' and produced an intelligence haul that was 'unreal' (*Washington Post*, 2017). The NSA considered the option of reporting the vulnerability used in the exploit to Microsoft so they could fix the problem, but decided that the intelligence it produced was too valuable. However, in early 2017, EternalBlue was stolen by the Shadow Brokers hacking group and, in April 2017, they released the code to the public. In May 2017, the WannaCry malware, which utilised the EternalBlue code, infected hundreds of thousands of computers around the world, encrypting files and demanding a ransom. The malware had a significant impact on the UK's National Health Service, resulting in hospitals and doctors' surgeries shutting down services and turning away patients (BBC News, 2017). Microsoft themselves placed the blame for the attack on the

NSA and echoed the sentiments of many within the DRC, who had long argued that stockpiling vulnerabilities was bad for security.

> This attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world (Microsoft, 2017).

Microsoft also pledged to work towards forcing governments to 'report vulnerabilities to vendors, rather than stockpile, sell or exploit them', an effort that, if successful, would remove the NSA's capability to use undeclared (i.e. Zero-Day) exploits to hack computers (Microsoft, 2017).

Hacking may sometimes be required by the state, but when revealed (as inevitably it sometimes will be), it causes considerable discomfort to the companies on whose products the vulnerabilities were found. The case of EternalBlue shows how this can lead to a backlash by technology companies who may then choose to reduce co-operation with the state to save face and to prevent future attacks.

Legislation

Another way in which the state has attempted to reduce the threat of the 'Going Dark' problem is to introduce legislation that forces companies to facilitate the state's attempts to gain access to communications data. The IPA includes several clauses that mandate companies to assist the state, including the requirement for ISPs to retain web browsing history for 12 months, provide facilities and services to law enforcement, and to remove electronic protection from communication data (HM Government, 2016, pp. 206-208).

According to the British government, the IPA 'will ensure that law enforcement and the security and intelligence agencies have the powers they need in a digital age to disrupt terrorist attacks', but these powers are considered by members of the DRC to be intrusive (HM Government, 2016). Others, such as Rid and Moore, suggest that legislation against encryption will ultimately backfire:

> Any attempt to systematically undermine end-to-end encryption – through legislation requiring service providers to retain the option of removing encryption for any given user – will likely strengthen

> more secure implementations by creating more demand for them, and thus help criminals and militants (Moore & Rid, 2016, p. 31).

The argument that companies will resist demands by the state to provide access to user data is evidenced by the actions of Apple, who have designed their iOS operating system so that they cannot provide user data even if issued with a government warrant (Apple, n.d.). As Jane Harman writes in 'Foreign Affairs', since the Snowden disclosures there has also been a significant change in attitudes in Silicon Valley, with companies less willing to co-operate with law enforcement as they do not want to appear complicit in mass surveillance (Harman, 2015).

> U.S. technology firms are taking increasingly dramatic steps to protect their customers' data. One can doubt the sincerity of the technology community's outrage over the NSA'S surveillance practices - doubt, for example, that the Facebook co-founder Mark Zuckerberg, whose company reportedly stores petabytes' worth of data about its billion-plus active monthly users, was shocked at the thought of mass data collection. But Silicon Valley's reaction has bite, and the outcome has been an encryption drag race that has top government officials panicking… Rather than fight surveillance policies in court, where the government has an overwhelming edge, companies such as Apple, Facebook, and Google have responded in cyberspace. To satisfy a global customer base with strict privacy expectations, they've developed technical capabilities to put customer data under lock and key (Harman, 2015).

Attempts to gain access to data by forcing technology companies to provide it have proven counterproductive, as they have caused the technology companies to develop technologies to make sure they cannot comply with these requests.

6.3.2 DRC Attempts to win the Crypto Wars

Members of the DRC tend to view encryption and other security measures as inherently positive in nature, whilst state surveillance is considered to be intrusive and unaccountable and is thought to cause more harm than good (Dixon-Thayer, 2016; Cult of Mac, 2016). Much of the focus of the DRC has therefore been on denying the state the capability to access encrypted communications through technologies such as end-to-end encryption, full disk encryption and onion routing networks such as Tor. This approach reflects the view expressed by Security

Researcher Bruce Schneier that 'either we build encryption systems that keep everyone secure, or we build them to leave everybody vulnerable' (Schneier, 2016). In other words, there is no middle ground and encryption must be applied to its fullest to protect everyone's security.

On paper, this approach by the DRC appears to be well grounded because the more that encryption is improved and applied, the more secure the Internet becomes. But this does not take into consideration the security concerns of the state, which considers some applications of encryption to be detrimental to national security.

Full Disk Encryption

Full Disk Encryption (FDE) can be applied to PCs, Laptops, smartphones or other devices and is used to makes the data stored on these devices inaccessible without the decryption key. FDE was introduced as an option in the Honeycomb edition of the Android operating system but is turned on by default in later versions. For Apple smartphones, FDE was introduced in version 8.0 of iOS and is now turned on by default (Apple, 2017). FDE can involve a variety of different key management protocols, with the key either stored externally, internally or in a specially protected area on the device that protects it from brute-force attacks[27]. FDE is widely promoted by the DRC as a method to combat state surveillance, including the EFF who describe it as 'Surveillance Self-Defense' (Electronic Frontier Foundation, n.d.). However, certain implementations of FDE are considered threatening to law enforcement agencies as they deny them access to information to investigate crime and terrorism.

The dispute between Apple and the FBI resulted from the fact that Syed Farook's phone had been protected with FDE and the FBI was unable to brute force the decryption key. Apple's implementation of FDE and refusal to co-operate with the FBI, led the FBI to purchase knowledge of a vulnerability in the iPhone from an unnamed black-market vendor (Aspen Institute, 2016). As Section 4.4.2 demonstrates, this provided the FBI with unrestricted access to all iPhone 5C's, notified the public of a major flaw in the iPhone software and left an exploit for the flaw in the hands of an unknown black-market vendor. Apple blame the FBI for these negative consequences. However, an argument could be made for holding

[27] Brute force attacks are attacks that test every single possible key until the correct one is found

Apple responsible, since if they had cooperated with the FBI then these negative outcomes would not have occurred.

President Obama has also argued that a focus on strong encryption will backfire because, in the wake of a terrorist attack, public opinion will shift and poorly written legislation will be rushed through (Obama, 2016).

> If your argument is strong encryption no matter what, and we can and should in fact create black boxes, that I think does not strike the kind of balance we have lived with for 200, 300 years. And it's fetishizing our phones above every other value. That can't be the right answer. What will happen is, if everybody goes to their respective corners, and the tech community says 'either we have strong perfect encryption or else it's Big Brother and an Orwellian world', what you'll find is that after something really bad happens, the politics of this will swing and it will become sloppy and rushed and it will go through Congress in ways that are dangerous and not thought through (Obama, 2016).

Whether it is through rushed legislation, hacking or backdoors, if there is no ordered way for the state to access specific information in the light of terror attacks then it is likely to attempt to access this information in ways that are more dangerous for both privacy and security.

End-to-End Encryption

End-to-end encryption (E2EE) is a method of encryption which restricts access to messages to just the sender and the receiver, unlike in other protocols where a third party such as a service provider may also hold the key. Keys can either be established beforehand using secure means or they can be negotiated dynamically using techniques such as Diffie-Hellman Key Exchange. The DRC advocate the widespread uptake of E2EE and argue that it is more secure because it 'reduces the number of parties who might be able to interfere or break encryption' (EFF, n.d.). But, as David Cameron argues, the common use of a system of communication that cannot be accessed by the state, even in extremis, can be considered a threat to national security.

> [do]we want to allow a means of communication between two people which even in extemis with a signed warrant from the home secretary personally that we cannot read? ...My answer to that

> question is no, we must not. The first duty of any government is to keep our country and our people safe (Cameron, 2015).

After the Westminster terror attacks in March 2017, Home Secretary Amber Rudd made similar comments, claiming that WhatsApp was giving terrorists a 'place to hide' and that it was 'completely unacceptable' that terrorists were able to communicate in secret without law enforcement being able to read their communications (Rudd, 2017).

In response to the dispute over end-to-end encryption, the government has acted to defend their security interests. Section 255 of the IPA details the function of Technical Capability Notices (TCN) that provide the government with the power to oblige an operator to remove 'electronic protection applied by or on behalf of that operator to any communications or data' (HM Government, 2016, p. 208). How the clause will be used is unclear. It could be used to mandate companies to remove encryption when they hold the key, it could be used to oblige companies to secretly remove E2EE encryption from future messages sent by individuals, or, it could be used to force companies to hack their own customers. The implementation of encryption on widely used platforms, which are inaccessible by the state, will inevitably lead the state to seek technical or legal methods for undoing this protection. This could ultimately leave some systems less secure than if they implemented encryption in a way that allowed the state access.

Tor and the Dark Net

The Onion Router (Tor) uses encryption to provide online anonymity for Internet users. When using the Tor Browser, an individual's web traffic is encrypted and bounced around several Tor relays throughout the world so that it is difficult to link a Tor user with the websites they visit. Tor also allows websites to operate anonymously so that the owners and operators of these sites cannot be traced. The Tor Project and the DRC argue that Tor provides individuals and organisations with greater security and privacy, whilst avoiding censorship and protecting civil liberties, and the more users that use the service the more secure it is because individuals are hidden within the mass of the userbase (The TOR Project, n.d.).

But the state has frequently expressed the view that technologies such as Tor are turning the Internet into a 'dark and ungoverned' space that is frustrating police operations and threatening to turn the Internet 'anarchic' (Hogan-Howe, 2014). Academic studies reveal the huge amount of illegal activity that is conducted on Tor

(Moore & Rid, 2016). Thus, from the state's perspective, the more people that use Tor the more effort they must make to bypass its security features. In recent years US and UK law enforcement agencies have run several high-profile operations to shut down dark web marketplaces, de-anonymise drug dealers and child exploiters and prevent the sale of arms. In 2015, GCHQ and the National Crime Agency (NCA) created a joint unit to focus on tackling child abuse on 'the dark web[28]' (NCA, 2015). 'GCHQ is using its world-leading capabilities to help the NCA reach into the dark web and bring to justice those who misuse it to harm children' (NCA, 2015).

Rid and Moore argue that 'Tor hidden services[29] present a formidable political risk to cryptography itself' (Moore & Rid, 2016, pp. 28-29). They argue that 'the widespread and highly visible abuse of unidentified Tor hidden services provides an easy target for any critic of encryption' (Moore & Rid, 2016, p. 29). Tor is becoming a victim of its own success because its high level of security attracts criminals and undermines the arguments for encryption. This is exacerbated by the refusal of the DRC to countenance any restrictions in Tor's functionality, such as the removal of hidden services, which provide the basis for most of the criminality on the network and have limited legitimate uses.

6.3.3 The Problem with Unilateral Approaches

Unilateral attempts to 'win' the Crypto Wars or gain a permanent advantage over the other side have always failed because of their failure to address the fears and uncertainty of the other. If the state does not achieve an acceptable level of access to online communications then it will continue its efforts to defeat, remove, undermine, circumvent or outlaw certain types of encryption until it achieves this. This was evident after the so-called end of the 'Crypto Wars' when GCHQ did not accept defeat and secretly continued to utilise all means available to it to access online communications.

Likewise, if members of the DRC do not believe they have achieved acceptable limits on state surveillance and acceptable levels of protection for communications, then they too will continue their efforts to thwart state attempts to access online communications. This is demonstrated by the DRC's redoubling of its efforts to

[28] The Dark Web or Dark Web is often used synonymously with Tor although they are not the same thing

[29] Hidden services on Tor are website's or other services that have their physical location and ownership details hidden so that no-one can identify running the service. Darknet markets use hidden services to enable them to sell drugs, weapons or other illicit goods without detection.

secure cyberspace and prevent state surveillance following the Snowden disclosures.

There may be periods of apparent calm within the Crypto Wars, but allegations that a terrorist attack was planned using encrypted communications or a cyber attack exploited a vulnerability hoarded by GCHQ, will reawaken all the same arguments. Perfect security is impossible and the government is unlikely to ever obtain unrestricted access to data. It is highly unlikely that either side can 'win' the Crypto Wars unilaterally as it would appear that the other would never stop fighting. Only a collaborative approach would seem likely to be able to ease an ongoing conflict that is damaging both national security and digital rights.

6.4 A Collaborative Approach

Whilst the Crypto Wars have been categorised by competing securitisations, extreme rhetoric and uncompromising attitudes towards surveillance, there have been some attempts at a more collaborative approach. These have included technical solutions that attempt to help differentiate between good and bad uses of encryption, peace talks designed to build trust and develop common security goals, and attempts to re-articulate and reframe the issue away from zero-sum scenarios and towards common security interests.

6.4.1 Technical Solutions

Several technical solutions to the CSD have been attempted, including the Clipper Chip and key escrow, which theoretically provide the state with access to data whilst ensuring it remains secure from attackers. But these attempts failed because they were opposed by members of the DRC, who were suspicious of government-imposed solutions and feared that the techniques would weaken encryption and lead to a reduction in security (Blaze, 1994). If the CSD is to be resolved then a technical element will be required, but this must satisfy both sides that it meets their security needs.

One potential approach was proposed by David Chaum, who has been described as the father of online anonymity following his 1981 paper on untraceable email, which put in place much of the theory for anonymous communications (Chaum, 1981). At the Real World Crypto conference at Stanford in 2015, Chaum announced that he and his colleagues had designed a solution that he claimed 'breaks the Crypto Wars' (Chaum, 2016). Speaking on the issue of online anonymity, Chaum

took an unusual step for a privacy advocate and acknowledged that systems that focussed solely on privacy would not ultimately be effective in the real world.

> You have to perfect the traceability of the evil people and the untraceability of the honest people. That's how you break the apparent trade-off, this standoff called the encryption wars (Chaum, 2016).

Chaum argued that his system would provide law enforcement with the access they required without affecting anyone else's privacy.

> If you want a way to solve this apparent logjam, here it is. We don't have to give up on privacy. We don't have to allow terrorists and drug dealers to use it. We can have a civil society electronically without the possibility of covert mass surveillance (Chaum, 2016).

Chaum's 'PrivaTegrity' system involves an encryption technology, which he calls cMix, that passes messages around numerous servers (nine in his example), which each perform a different cryptographic function on the message (Chaum, et al., 2016). The interesting feature of Chaum's solution comes from the fact that, whilst none of the servers can access the original message, if all nine act together then the message can be decrypted. Chaum argues that the system provides greater security than competing services such as Tor, but also contains the unique feature that messages can be decrypted and deanonymized if all nine servers work together to do so. Chaum suggests that the servers could be spread around nine countries and, only when the administrators of all nine servers agree, could a message be decrypted and de-anonymised. This would be reserved for 'serious abuse, something that leads to death and real harm to people, or major economic malfeasance' (Chaum, 2016). Chaum also notes that the number of servers could be more or less than nine and a limit could be placed on the number of decryptions possible within a timeframe.

Whilst Chaum's particular system may or may not prove workable, his concept is an interesting solution to the CSD. It is a technical solution proposed by a privacy activist that could provide the state with access to data, without otherwise compromising security. Chaum's suggestion of nine servers in nine countries could be adapted in a variety of different ways; for example, four servers could be used with one being controlled by a state agency such as GCHQ, another by a technology company such as Facebook, another by an independent privacy commissioner, and

a final one by the judiciary. Only when all four agree that there is a proportionate, reasonable and legal case to decrypt a message could this task be performed. Such a solution could solve the state's fear of 'Going Dark', and could provide the DRC with the reassurance that surveillance was only possible in a targeted and legal manner.

Despite the apparent potential of such a system, Chaum's ideas were heavily criticised immediately after their announcement. Chaum had made the fatal mistake of describing the system as 'like a backdoor with nine different padlocks on it' (Chaum, 2016). As previously discussed, the term backdoor has been institutionalised within the DRC as inherently bad, and the reference immediately invokes negative reactions and hostility from the DRC. Backdoors are considered unacceptable security vulnerabilities and are associated with underhand actions by intelligence agencies and hackers. As Wired put it in an article on Chaum's new method;

> The mere mention of a "backdoor"—no matter how many padlocks, checks, and balances restrict it—is enough to send shivers down the spines of most of the crypto community (Wired, 2016).

Following Chaum's announcement, the DRC heavily criticised the idea, with much of that criticism focussed on the 'backdoor' aspect of the software. A senior technologist at Amnesty International, Claudio Guarnieri, said that backdoors should never be discussed. Others such as 'activist technology researcher' Christopher Soghoian, argued that doing so was just playing into the hands of the FBI.

> Even discussing of a crypto backdoor "solution", despite of how "secure" it might be, is a dangerous step back to a critical debate (Guarnieri, 2016).

> Security experts: Backdoors weaken security. They're a bad idea. Chaum: I've built a new system with a backdoor. FBI: See? It is possible (Soghoian, 2016).

> …this is little more than a huge political gift to the FBI, who can go back to their stupid claims that if technologists just work

> harder they can come up with a "solution" to the false problem of "going dark" (Anon., 2016).

The word ‘backdoor’ did not feature in Chaum’s paper on PrivaTegrity but he did use the term in a widely quoted interview with Wired magazine. This was something that Chaum later admitted was a major mistake.

> I agreed to allow the term 'backdoor' to be used in the article to refer to access in general, not as a deliberate weakening of a system. This probably was my big mistake … It's B.S. There unconditionally is no hidden weakening within PrivaTegrity. My whole career has been about reducing the likelihood of these backdoors and all about creating structures that aren't subject to clandestine manipulation (Chaum, 2016).

Chaum has a very strong digital rights background and created PrivaTegrity, after learning from the Snowden disclosures about a dangerous relationship between the NSA and technology companies. He considers his system to have much stronger privacy and security qualities than the current ‘front door’ security concerns of well-established technology companies.

> Current social media systems all have a front door through which those who operate them, possibly under the influence of government, can do whatever they want, including inserting a man in the middle—even if clients think they're doing end-to-end encryption (Chaum, 2016).

But his use of the ‘backdoor’ metaphor discredited his work and turned him overnight from a hero to an enemy of the DRC.

> Holy crap, has Chaum turned evil in his old age? (Andrea, 2016).

> I'm heartbroken to see that Chaum is proposing key escrow for everyone on the planet: What happened to David Chaum? (Appelbaum, 2016).

> Don't you think the intelligence agencies tried to $$$ convince $$$ the least ethical of the guys working with cryptography till they found one that was up for sale? (Ninja, 2016).

> Bought or extorted, David Chaum is now with the enemy (Dawson, 2016).

Chaum claimed that protecting digital rights could be better achieved by a system that satisfied the requirements of the state, since this would stop them from pursuing the type of tactics revealed by Edward Snowden. This appreciation of the other side and its impact, shows that Chaum was sensitive to the nature of the CSD and understood that unilateral approaches to solving it could not be successful. But despite his privacy credentials, Chaum's efforts to engage with the logic of the state's arguments on encryption were enough to see him discredited and lambasted by the DRC.

The reactions to Chaum's proposals echo those towards historical figures who have attempted to reconcile with an adversary but have been ostracised by their own side. Anwar Sadat, the president of Egypt attempted to solve the conflict between Israel and Arab nations by engaging with Israel's security fears. In 1977, he publicly recognised the right of Israel to exist. in 1978, he agreed to the Camp David Accords. In 1979, he signed the Egypt-Israel Peace Treaty with Israeli Prime Minister Menachem Begin (Booth & Wheeler, 2008). These reconciliation efforts seemed to have broken a historical deadlock but Sadat's actions were viewed as treacherous by many on his own side. Ultimately, in 1981, he was assassinated by ideological fundamentalists within the Egyptian Army.

Sadat was assassinated for seeking to improve Egypt's security by engaging with and responding to Israeli fears, and a similar (figurative) fate awaited Chaum after he attempted to engage with the fears of the state. Chaum reached out to the other side but, by using the term backdoor, he lost the support of his own. Chaum's approach was unsuccessful because it focussed on a purely technical solution to the CSD and overlooked the trust building that is necessary for security co-operation. The failure of Chaum's approach mirrors failures of security co-operation in the international arena, such as the Northern Ireland peace talks in the 1970s and 1980s, which failed due to a lack of trust building (Ruane & Todd, 1996).

Many of the key actors in the CSD are technically minded, including academic cryptographers, coders, crypto-libertarians and GCHQ employees, so the focus on technical solutions is understandable. For many digital rights advocates, the solution to state surveillance is to develop better encryption technologies, 'encrypt as much communications as you can' and spread the message of encryption as

widely as possible (Electronic Frontier Foundation, 2013). For cyberlibertarians technology is the ultimate solution to oppressive government, and the technologies of cyberspace render government control impossible (Barlow, 1996). However, after many years of trying and failing to solve their issues with technology, some within the DRC have begun to realise that technology alone might not be the solution. The prominent security researcher, cryptographer and privacy campaigner Bruce Schneier wrote a book on this topic, in which he dismantled the arguments in his previous book that cryptography was the solution to everything (Schneier, 2004; Schneier, 1995). On his website, he explained how his thinking had changed (Schneier, 2000).

> Seven years ago I wrote another book: Applied Cryptography. In it I described a mathematical utopia: algorithms that would keep your deepest secrets safe for millennia, protocols that could perform the most fantastical electronic interactions-unregulated gambling, undetectable authentication, anonymous cash-safely and securely. In my vision cryptography was the great technological equalizer; anyone with a cheap (and getting cheaper every year) computer could have the same security as the largest government. In the second edition of the same book, written two years later, I went so far as to write: "It is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics."
>
> It's just not true. Cryptography can't do any of that. It's not that cryptography has gotten weaker since 1994, or that the things I described in that book are no longer true; it's that cryptography doesn't exist in a vacuum. Mathematics is perfect; reality is subjective. Mathematics is defined; computers are ornery. Mathematics is logical; people are erratic, capricious, and barely comprehensible.
>
> The error of Applied Cryptography is that I didn't talk at all about the context. I talked about cryptography as if it were The Answer™. I was pretty naïve (Schneier, 2000).

Schneier was not responding specifically to the CSD, but his recognition that cryptography does not exist in a vacuum is directly relevant. Technological solutions

to the CSD cannot prove effective if they are not coupled with efforts to build trust and common identity between the conflicting parties. As Schneier went on to conclude, '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).

6.4.2 Peace Talks

The Crypto Wars have created distrust, enmity, suspicion, a tendency towards extreme positions and an unwillingness to compromise. Although technical solutions are essential, they cannot solve the CSD alone. Peace talks are the first steps towards establishing peace between nations as they help to build trust, dispel myths and establish common interests and ideologies. There have been several attempts to hold peace talks between key actors within the CSD, which have had varying degrees of success.

James Comey's Adult Conversation

The difficulty in establishing an initial dialogue is demonstrated by the response to FBI director James Comey's attempts to engage in discussion with technology companies over the CSD. Speaking at the 2016 Symantec Government Symposium, Comey acknowledged the difficult issue of encryption but said that the problem was 'less technological and more ideological' (Comey, 2016). He announced that the FBI planned to 'collect information this year so that next year [after the Presidential elections] we can have an adult conversation in this country' (Comey, 2016). His comments were greeted with hostility from members of the DRC who were angry at the condescending tone. The Register wrote an article attacking the comments, which was tag-lined 'how about f**k off – is that adult enough?' (The Register, 2016). Techdirt was similarly scathing of Comey's attempts at negotiation and their response shows how difficult it is to establish a dialogue when there is so much distrust and hostility between the two parties (Tech Dirt, 2016).

> This is not just insulting, but counterproductive. Plenty of experts have been trying their damnedest to have an "adult conversation" with Comey, explaining to him why he's wrong about the risks of "going dark," while others have -- in fairly great detail -- explained the serious dangers behind Comey's approach. Comey's response to these efforts so far has been the equivalent of sticking his fingers in his ears and screaming "nah, nah, nah -- can't hear

you!" while repeating his "nerd harder" mantra (Tech Dirt, 2016).

> An "adult conversation" has to be one where someone in Comey's position is able to admit that maybe, just maybe, he's wrong. It's not one where he gets to keep demanding a new conversation until people tell him that night is day. Because that's just silly. This new claim about an "adult conversation" is also stupidly counterproductive. All it's going to do is make the actual experts here -- like the authors of that MIT paper on the dangers of backdoor -- dig in and have absolutely no interest in dealing with Comey. How could you when he so flippantly brushes off all the work they've done already? (Tech Dirt, 2016).

The response to Comey's words demonstrates the difficulty in even establishing a dialogue when enmity is strong and historical grievances are still raw. Comey's 'adult conversation' never happened because he was sacked by Donald Trump for unrelated reasons, but it is difficult to see how he could have achieved any degree of success given his reputation within the DRC.

Hilary Clinton's Manhattan Project

In the run-up to the 2016 US Presidential elections, Hillary Clinton laid out her digital policy saying that she rejected the false choice between privacy and security and wanted to work with technology companies to protect them both (Clinton, 2016). During a debate, she announced that she wanted to launch a Manhattan-like project to bring the government and tech community together and solve the CSD (Clinton, 2015).

> I would hope that, given the extraordinary capacities that the tech community has and the legitimate needs and questions from law enforcement, that there could be a Manhattan-like project, something that would bring the government and the tech communities together to see they're not adversaries, they've got to be partners… I just think there's got to be a way, and I would hope that our tech companies would work with government to figure that out (Clinton, 2015).

The similarities between Clinton's policies and Apple's position were noted by several news outlets. Kif Leswing, for Business Insider, claimed that Clinton and

Apple were in lockstep and noted how 'remarkable' it is that 'Clinton's position mirror's Apple's public statements (Leswing, 2016). Daniel Dilger, writing for Apple Insider, claimed that her policies 'read as if they were ghost written by [Tim] Cook for Apple's ideal America' (Dilger, 2016). Apple themselves appreciated Clinton's policies and, in leaked emails between Apple's Vice President, Lisa Jackson, and the chairman of Clinton's presidential campaign, John Podesta, Jackson thanked Clinton 'for the principled and nuanced stance the Secretary took last night on encryption and the tech sector' (Jackson, 2015). Further emails revealed the close relationship between Clinton and Apple after Podesta said that he was 'looking forward to working [with Apple] to elect the first woman President of the United States' and Jackson replied that she would do whatever she could to help before later promising to play a more public role in Clinton's campaign (Jackson, 2015; Podesta, 2016). In August 2016 Jackson and Tim Cook jointly held a fundraiser to support Clinton's presidential bid.

Despite Clinton's conciliatory tone and close alignment with Apple, her comments were still rejected by many within the DRC, who suggested that she was attempting to create a backdoor into encryption or even to break it (Laguna, 2015). Edward Snowden claimed that Clinton had 'just terrified everyone with an internet connection' and Marc Andreessen of Netscape mocked her comments as unrealistic facetiously claiming that 'also we can create magical ponies who burp ice cream while we're at it' (Snowden, 2015; Andreessen, 2015).

The reaction to Clinton's statements shows how difficult it is to even begin to debate the issue of encryption and surveillance because trust between the government and DRC is so low. The mere suggestion that government could work with technology companies to assist law enforcement is viewed by some of the DRC as an attempt to install a backdoor.

Wilton Park and Ditchley Park Events

Peace talks are often held in secret because it allows actors to express views that might not be publicly unacceptable, and meet the other side without accusations that they are dealing with the 'enemy'. In the UK there have been several attempts to establish peace talks between the state and members of the DRC, including an event at Wilton Park on 6-7 October 2014, titled 'Privacy and security in the digital

age: UK perspective[30]. The event was sponsored and run by GCHQ but run on neutral ground, and brought together MPs, industry, academics, think tanks and civil liberties organisations.

The event was held in secret, so the outcomes were unclear, but it did lead to a follow-up event at Ditchley Park between 14-16 May 2015. This was more openly publicised; a list of attendees was released and a report on the findings was made available on the Ditchley Foundation website[31]. The conference operated under Chatham House rules, meaning that participants could use the information they received but could not attribute comments to attendees. These rules were established at Chatham House in 1927 to facilitate free discussion, but are now used worldwide to help individuals speak freely and express views that do not necessarily reflect those of the institution they serve.

The Ditchley Park event brought together high-level leadership from the intelligence and security agencies, the government, technology companies, and the digital rights movement, including current and former directors of GCHQ, a member of the intelligence and security committee, an investigative journalist, security and privacy representatives from Google and Apple, and the former head of the Secret Intelligence Service (aka MI6), Sir John McLeod Scarlett. The stated aim of the conference was to consider 'how the twin needs of security and privacy can be met in modern democracies, and the principles which should underpin the bargain between the State and the citizen in this area' (Ditchley Park, 2015).

The official report on the event indicates that participants made substantial progress. It was agreed that intelligence agencies should be more transparent and should push the boundaries of what could be revealed to show convincing evidence of what surveillance is for. It was also agreed that terms such as 'national security' should be defined more precisely.

Investigative journalist and digital rights campaigner Duncan Campbell was the first to reveal the existence of GCHQ in 1976, and he has since spoken and written extensively about surveillance issues. After attending the Ditchley event, he wrote a blog about the experience in which he expressed his surprise at the fact that at the event 'no-one argued against calls for greater openness' arguing that this was

[30] https://www.wiltonpark.org.uk/event/privacy-and-security-in-the-digital-age-uk-perspective-wp1352/

[31] http://www.ditchley.co.uk/conferences/past-programme/2010-2019/2015/intelligence

‘a first; coming 40 years after a time when it was a crime in Britain even to mention the existence of GCHQ’ (Campbell, 2015; Campbell, 2015). Campbell also expressed surprise at ‘some unexpected and surprising comments from senior intelligence voices, including that "cold winds of transparency" had arrived and were here to stay‘ (Campbell, 2015). He highlighted other comments from security sources that surprised him, including opinions that ‘Snowden's actions were an inevitable and perhaps necessary counterbalance to admitted excesses of intelligence collection after 9/11’ and that ‘we [intelligence agencies] should have seen it coming in the first place, and so put more information in the public domain first’ (Campbell, 2015).

Campbell claimed that ‘away from the foetid heat of political posturing and populist headlines’, the participants could speak more openly, suggesting that ‘you don't get nuanced thoughts like that on Fox News or in Britain's Daily Mail’ (Campbell, 2015). He also commented on the lack of ‘rhetoric’ and polarised debate over the villainous or heroic nature of Edward Snowden, adding that the conference conclusions would focus on developing future principles rather than focussing on allegations of harm (Campbell, 2015).

Campbell’s surprise at some of the comments by intelligence officials demonstrates the ‘other minds’ problem of the CSD, and the Butterfieldian difficulty in putting yourself in the other person’s counter fear. It is interesting that, despite years of campaigning on surveillance issues, Campbell only heard the real views of surveillance practitioners once a safe environment had been created that promoted honest and open discussion. The Ditchley event demonstrates how carefully managed peace talks can potentially help to break down misunderstandings and mistrust. Campbell finished his blog with the phrase ‘we are not in Kansas anymore’, suggesting that he believed the conference to have moved the debate into unchartered waters (Campbell, 2015).

The official report into the conference also took an upbeat tone, claiming that there was optimism that ‘satisfactory arrangements could be found between the agencies and the companies, despite recent arguments following the Snowden revelations’ (Holmes, 2015). But some reporting on the event demonstrated why it could be so difficult for the government to engage in such discussions. In a highly misleading article, titled ‘Snowden leak: governments' hostile reaction fuelled public's distrust of spies’, the Guardian newspaper, who did not attend, claimed that the conference had concluded that ‘the hostile reaction of the British and US

governments to the Snowden disclosures of mass surveillance only served to heighten public suspicion of the work of the intelligence agencies' (Travis, 2015). In fact, the official summary of the event concluded that it was the government's policy to release as little information as possible, but the allegation that this policy had increased suspicion, and hostility was never mentioned by anyone in attendance (Holmes, 2015).

Such reporting highlights why frank and open discussion is so difficult and, whilst there is an irony in the notion that discussions about greater transparency are best held in secret, the Ditchley event appears to show the benefits of such an initiative. Whilst the secretive nature of the event precludes a thorough analysis, the positivity of representatives from the state and DRC indicates that the event was a success and appears to have helped to build bridges between the government, technology companies and privacy advocates. Whilst it did not lead to tangible new policies, it did demonstrate that, in the right environment, with the right people, old enmities can be overcome and progress on the CSD can be made.

Global Internet Forum to Counter Terrorism

Another initiative to encourage dialogue is the Global Internet Forum to Counter Terrorism (GIFCT) which was established in June 2017 to help technology companies coordinate their efforts to make 'consumer services hostile to terrorists and violent extremists' (Facebook, 2017). It includes representatives from Facebook, Microsoft, Twitter and YouTube, and has a 'mission is to substantially disrupt terrorists' ability to use the internet in furthering their causes, while also respecting human rights' by collaborating with civil society and government (Global Internet Forum to Counter Terrorism, 2017).

> We believe that the best approach to tackling online terrorism is to collaborate with each other and with others outside the private sector, including civil society and government (Global Internet Forum to Counter Terrorism, 2017).

The forum held its first workshop on 1st Aug 2017 and included representatives from more than two dozen technology companies and NGOs, as well as a range of state representatives, including the British Home Secretary, Amber Rudd. Statements from the forum demonstrated an acute awareness of the government's concerns over the use of technology by terrorists and stated a clear determination to deal with the problem.

Comments made by Amber Rudd before the first forum, where she appeared to threaten technology companies and imply that 'real people' did not need encryption (see Section 6.3.3), meant that the forum did not get off to a good start. These remarks struck at the heart of sensitivities over encryption and set a tone of confrontation rather than collaboration. They also make it more difficult for technology companies to collaborate with the government without being accused of succumbing to government demands to undermine encryption. However, the GIFCT still has the potential to help create a much better relationship between the government and technology companies by focussing on common interests, such as the removal of terrorist content from social networks.

Reframing the debate

One of the major difficulties associated with the CSD is the way it is framed by different actors. It is framed as good versus evil, security versus privacy, security versus insecurity or the people versus the government, but these framings are simplistic representations of an issue that is extremely complex.

Frames are useful as cognitive shortcuts that help make sense of complex information but, when using frames, we discount potentially important information and filter our perceptions through a lens. According to Shmueli, Elliott and Kaufman, the divergence of frames between two different parties plays a significant role in conflict (Shmueli, et al., 2006).

> Disputants differ not only in interests, beliefs, and values but also in how they perceive the situation at the conscious and preconscious levels. These differences engender divergent interpretations of events, paint parties into negative characters, yield mutually incompatible issues, and focus attention on specific outcomes that impede exploration of alternatives (Shmueli, et al., 2006, p. 209).

This framing applies to public reaction to the CSD, as Jim Killock of ORG explains.

> A lot of the public reaction is based upon the way they see the framing of these things so with surveillance either you can see it as a vital security measure and you're operating in the frame of terrorist threats and the threat to national security …if you are operating on the level of intrusion into people's personal privacy

> and the legitimacy of doing that without genuine suspicion then you get a different reaction from people (Killock, 2016).

As this framing becomes embedded within the thinking of the state and the DRC, it can make it far more difficult to achieve compromise as each side thinks that they are right and should not compromise (Shmueli, et al., 2006).

> As conflicts become intractable, frame differences often exacerbate communication difficulties, polarize parties, and escalate strife. In turn, polarization is reflected in the parties' frames, feeding stakeholders' sense that they are in the right and should not compromise. Divergent frames are self-reinforcing because they filter parties' subsequent information intake and color interpretation (Shmueli, et al., 2006, p. 209).

In the CSD, encryption is framed as a universal good so, for the DRC, any policy that might compromise any implementation of it to any degree should be defeated, whereas, for the state, access to information is deemed essential to national security so any technologies that prevent this must be opposed or circumvented.

However, according to Shmueli et al, interventions to reframe an issue can help to improve its tractability. De-escalatory processes that seek to reduce escalatory cycles, perspective-taking processes that seek to help disputants understand the views of the other, and identification of commonalities that seek to find common ground, can all help to reframe seemingly intractable conflicts.

Whilst reframing is difficult, there have been some attempts to reframe the CSD and help break the current cycle of insecurity.

Encryption Substitutes

The issue of encryption sits at the heart of the CSD because it is framed very differently by the state and DRC. Members of the DRC tends to believe that any tampering with any implementation of encryption represents a backdoor that makes everyone insecure, whilst the government frequently highlights how particular implementations of encryption can threaten national security (Hogan-Howe, 2014; Cook, 2016). The problem seems intractable, but Andrew Kean Woods of the Hoover Institute has sought to reframe the debate away from encryption and focus instead on what each side really wants.

> Law enforcement officials are, in general, agnostic about the method through which they obtain evidence—what matters is obtaining it. Privacy-seekers are similarly agnostic about how they secure their privacy—what matters is having it. This means that policymakers have a wide set of options—not only about whether to allow law enforcement to access personal data, but also how to do so. This wide set of options is not reflected in the debate over encryption, which is typically framed in all-or nothing terms. Widening the scope of the policy discussion to include related issues—what I will call "encryption substitutes"—may increase the chances of compromise and may generate better policy (Woods, 2016, p. 1).

To reframe the issue away from encryption, Woods suggests a range of 'Encryption Substitutes' that could provide security to both law enforcement and the DRC. For law enforcement, he argues that equipment interference, metadata and unencrypted market-driven data can all provide the information that law enforcement needs without breaking encryption. For the DRC, Woods suggests that judicial substitutes such as blocking statutes, and technological substitutes such as anonymization tools, can be used to provide privacy without the use of encryption. Wood's proposals are not so much useful for their practical insights but more for their attempt to reframe the debate away from the tricky issue of encryption.

Cryptopolitik

Daniel Moore and Thomas Rid also attempt to address the contentious issue of encryption, calling for a less idealistic approach to the issue, which they call Cryptopolitik (Moore & Rid, 2016).

> Encryption is too important to be left to true believers. The future design of crypto systems should be informed by hard-nosed political and technical considerations. A principled, yet realistic, assessment of encryption and technology more broadly is needed, informed by empirical facts, by actual user behaviour and by shrewd statecraft – not by cypherpunk cults, an ideology of technical purity and dreams of artificial utopias. Pragmatism in political decision-making has long been known as realpolitik. Too

> often, technology policy has been the exception. It is high time for cryptopolitik (Moore & Rid, 2016, p. 30).

Whilst acknowledging the complexity of the problem, Moore and Rid suggest examples of compromises that could be made by each side. Attempts to 'systematically undermine end-to-end encryption' should be a 'political no-go area' as they would backfire but, equally, crypto-utopias such as Tor should restrict their offerings to rid the services of their most illicit uses and protect the reputation of encryption (Moore & Rid, 2016, p. 31). Rid and Moore suggest that instead of focussing on technical issues or utopian dreams, we should first focus on deciding what we want as a society before then designing software to achieve it. They suggest that attention should be focussed away from banning or promoting better encryption, and challenge software engineers to consider whether they can design platforms that improve anonymity, authentication and availability, but do not incentivise illiberal and illegal behaviour.

Rid and Moore attempt to reframe encryption as a tool of policy-making rather than a master of it and, in doing so, they hope to remove the heat from the encryption debate and move towards a more pragmatic approach to the CSD. The challenge is to convince two sides who are deeply wedded to their views on encryption that they can improve their own security if they change their focus.

Other Attempts to Reframe

Other authors have also suggested that this debate around privacy and security needs reframing. Paul Ohm suggests that both 'parties have spent most of the debate fighting their battles in the trenches, butting heads over picayune specific details in statutory text that rarely, by themselves, impact safety or privacy' (Ohm, 2004, p. 1599). He suggests reframing the debate one level up. 'Can we develop sound procedures or prophylactic measures to ensure privacy and security, even if we cannot agree today on the specific substantive form that our Internet surveillance laws should take?' (Ohm, 2004, p. 1599). Sergei Boeke also notes that whilst 'the debate on government surveillance programs is frequently characterised by the apparently absolute dichotomy of security versus privacy … basic concepts such as privacy and surveillance elude precise definition' (Boeke, 2017, p. 307). By breaking down issues into domestic/foreign, upstream/downstream, targeted/bulk, metadata/content, Boeke claims that a better understanding about the nuanced nature of surveillance can be reached,

which would inform a better debate. Quin DuPont criticises the domination of the debate by 'cyberlibertarians on one side and law and order proponents on the other' and suggests that the solution is to reject the extremes on either side (DuPont, 2015).

> there's a desperate need to reframe the debate around encryption – and that starts with rejecting advocacy for pervasive and ubiquitous cryptography as well as the overreaching state demands for wholesale surveillance. Instead, solutions should leverage strong democratic controls and collective decision-making (DuPont, 2015).

6.3 Can Security Dilemmas be Overcome?

The examples highlight the difficulties faced by those attempting to resolve the CSD. Unilateral attempts to improve security for one side often fail because they exacerbate the security concerns of the other, provoking a reaction that leads to grater insecurity for both. And more collaborative approaches have also proven difficult as a lack of trust, historic enmity and an inability to appreciate the concerns of the other act as impediments to co-operation.

Authors such as John Mearsheimer would take this as evidence for the fatalistic view that security dilemmas can never be overcome. Mearsheimer argues that because national security matters are a question of state survival, uncertainty over the intentions of another state must lead to the assumption that they are a threat and should be deterred militarily. Within his theory of offensive realism, Mearsheimer suggests that the nature of the anarchic international system is responsible for aggressive state behaviour in international politics (Mearsheimer, 2001; Toft, 2005). His concept of offensive realism is based on the assumptions that states can never be certain of the intentions of other states, they value their survival as their primary goal, and they behave as rational actors. Whilst the fatalistic approach simply extends the security dilemma to its logical conclusion, it is based upon the assumption that states will always feel insecure if they do not possess complete knowledge of the intentions of the other, and that this insecurity will always lead to conflict.

Others suggest that the security dilemma is not absolute and can be mitigated in a variety of ways. One method is to address the offence-defence balance problem by

implementing pacts such as arms control agreements that make it easier to defend than attack. Another is to address the offence/defence differentiation problem by using methods such as mutual weapons inspections to ease doubts over the other's military power (Jervis, 1978). These strategies address what Charles Glaser describes as the general condition of uncertainty that exists at the heart of the security dilemma. States that are better informed of each other's intentions are more likely to realise the defensive nature of the other's activities (Glaser, 1997).

As ORG Director, Jim Killock explains, public debate might be one way in which the CSD can be mitigated.

> You can never know what the sinister motivations [of the state] might be because those motivations exist in the heads of people, not necessarily in policy documents. But public debates clear the air of those suspicions to a greater or lesser extent and flushes out those concerns that are not legitimate and allows them to be properly contested, whereas if you don't do that you either produce a suspicion of those nefarious motivations or you indeed allow them to flourish because they are not being properly challenged (Killock, 2016).

Whilst this mitigation approach may help to avert the most tragic consequences of the security dilemma, the structural problems of uncertainty and fear are only lessened rather than resolved. Transcendence is an alternative, constructivist approach, more aligned with securitisation theory itself and closely aligned to the de-securitising concept of re-articulation. It attempts to solve the issue of fear and uncertainty by completely reframing the problem.

Emanuel Adler and Michael Barnett apply Karl Deutsch's concept of security communities to the security dilemma to change the game from one of competing security concerns to one of mutual security interests. Deutsch describes the existence of pluralistic security communities, where states become integrated to the point that they gain a sense of community, which in turn creates the assurance that they will settle their differences short of war (Deutsch, 1957). Adler and Barnett argue that whilst individual states cannot escape the security dilemma alone, together they can transcend it by eliminating the fear on which it is based. Security communities do not need to be designed from the top down but emerge once states recognise that seeking co-operation on security or economic issues can

have mutual benefit (Adler & Barnett, 2009). This interaction can open space for the establishment of norms and states can start to look at issues collectively rather than in isolation. States then begin to view each other as security partners as fear and uncertainty subside. Alliances such as NATO, concepts such as the West, and political unions such as the UK and the EU can be considered security communities, which have transcended fear and uncertainty[32]. These communities are particularly effective in the face of a common enemy, such as the Warsaw Pact to NATO, but this is not essential to their success. The spectre of war and mutual annihilation, and the development of a mutual sense of identity, can help to facilitate the creation of security communities without the need for an external threat.

6.4 How to solve the Cyber Security Dilemma

If transcendence can be achieved then security competition will be turned into security co-operation, but this first requires the creation of an environment of mutual understanding, trust and co-operation. Whilst this may be difficult to achieve after years of enmity, the following guiding principles can help to shape an environment within which the CSD can be overcome;

- Shared values and Identities;
- Future Certainty;
- Positive Signalling and Symbolism;
- Ideological Flexibility;
- Security Dilemma Sensibility;
- Good Interpersonal Relationships;
- Trust;
- Transparency.

These guiding principles will be discussed in the following section;

6.4.1 Shared Values and Identities

Rational Egoism is the believe that actors will always take actions that seek to maximise their own self-interest. It often forms the basis for negotiations, but as Booth and Wheeler explain, 'co-operation cannot survive, and indeed flourish, if it is based on no more than rational egoism' (Booth & Wheeler, 2008, p. 131). Jervis

[32] Whilst many consider the UK's vote to leave the European Union in 2016 to be borne from fear and uncertainty, EU countries are still largely considered to be security allies with each other and the UK.

expands on this idea explaining that for co-operation to last, shared values and identification with the other must also be a priority.

> In part because of the tendency for people to be self-righteous and to see their own acts as cooperative and those of others as hostile, temptations and fears may produce mutually undesired outcomes as long as narrow self-interest is dominant. At a minimum, the feeling that one is morally obligated to reciprocate cooperation—and that others live under the same code—permits a wider range and scope for mutually beneficial exchanges. In fact, the actors may gain most when they do not regard the interaction as one of self-interested exchange at all. Even if this extreme is not approached (and it is not likely to be in international politics), without the power of at least some shared values, without some identification with the other, without norms that carry moral force, cooperation may be difficult to sustain (Jervis, 1988, p. 348).

The Investigatory Powers Act (IPA) can be viewed as having been based upon a rational egoist approach, rather than one of shared values and identifies. The Investigatory Powers Commission considered 830 pages (once transcribed) of oral evidence and 1532 pages of written evidence, which were submitted by lawyers, academics, intelligence officials, digital rights organisations, technical experts and industry bodies (HM Government, 2016; HM Government, 2016). It was also supported by three reviews into investigatory powers provided by the Royal United Services Institute, David Anderson QC and the Intelligence and Security Committee (ISC) (Anderson, 2015; Intelligence and Security Committee, 2013; Royal United Services Institute, 2015). A draft bill was published in November 2015 and, after scrutiny by the House of Commons Science and Technology Committee, the Intelligence and Security Committee, the Joint Committee of both Houses of Parliament and the aforementioned organisations, the final bill was submitted to parliament a year later in November 2016.

The government claims that the final act took into consideration the concerns and requests of all contributors and in response delivered a ‘much clearer’ bill with ‘clearer and stronger privacy safeguards’ and ‘additional protection for journalists’ (HM Government, 2017). Technically the bill appears to have satisfied the requirements of all sides; it provides the intelligence agencies with more powers than they previously had, it makes these powers clearer, and it creates far greater

privacy controls and oversight and accountability mechanisms. Yet as a solution to the CSD, it cannot be considered a success because fear and uncertainty on each side are undiminished. As previously highlighted, ORG director Jim Killock called the act 'one of the most extreme surveillance laws ever passed in a democracy' and a petition to repeal the Act received 212,000 signatures (Killock, 2016; Killock, 2017). Only a few months after the IPA was enacted, the Home Secretary Amber Rudd and the DRC were once again in conflict in the wake of reports that the Westminster terrorist Khalid Masood had used the encrypted messaging platform WhatsApp to communicate just before the attack.

This consultative and rational egoist approach to the IPA succeeded in incorporating the requirements of a large range of actors, but did nothing to identify and develop shared values and identities. As a result, the state and the DRC do not identify with each other or consider their security interests to be mutually compatible, and this has resulted in a continuing state of conflict.

6.4.2 Future Certainty

Even if fear and uncertainty can be overcome in the present, this may not be enough to resolve the security dilemma. Whilst a state may be considered a current ally, fears over the stability of the alliance, the potential for a change of government or a future break-down in trust means that the status quo cannot be relied upon to last forever. Whilst defenders of state surveillance argue that the people and agencies who practice it are benign and ethical, others fear that the very existence of surveillance technology is a threat because at a future date a less benign force may use it to subjugate the population. In 2015, the ORG raised concerns about data sharing between US and UK intelligence agencies, fearing that this could pose a significant risk if this relationship broke down.

> We are increasingly dependent on the US for the NSA's technology and data. This could mean it is difficult to separate our own strategic interests from those of the US… If there were a crisis in the relationship between the UK and the US, what risks would our shared intelligence arrangements pose? (Open Rights Group, 2015).

In his first interview after exiling himself to Hong Kong, Edward Snowden made a similar point, warning of a potential future where a new leader exploits the NSA's surveillance machinery to support a tyrannical regime.

> Eventually, there will be a time when policies will change, because the only thing that restricts the activities of the surveillance state is policy… a new leader will be elected, they'll flip the switch, say that because of the crisis, because of the dangers that we face in the world--some new and unpredicted threat-- we need more authority, we need more power. And there will be nothing the people can do at that point to oppose it and it will be turnkey tyranny (Snowden, 2013).

Three years later, Snowden's warnings were revisited after it emerged that Donald Trump could be elected President of the US. This fear was exacerbated when Trump responded to allegations of Russian hacking by saying 'I wish I had that power, man that would be power' (Trump, 2016). When Trump was elected on 8th November 2016, Nick Merrill, the executive of the Calyx Institute and an advocate for encryption, suggested that trust in Obama had led to complacency over surveillance powers.

> There have been some people who were complacent about things like drone killing of US civilians and mass surveillance under Obama, because they trusted him. That wilful neglect on their part is about to come back and possibly bite all of us in the ass (Merrill, 2016).

Ben Wizner of the American Civil Liberties Union and lawyer for Edward Snowden, also suggested that trust in the executive had been misplaced.

> The danger of the aggregation of executive power we have seen over the last decade is that we might have an executive who is not worthy of that trust. This has been a trend in the US but there has been a weakening of constitutional oversight during the growth of the national security state (Wizner, 2016).

Former NSA whistle-blower Thomas Drake also warned that Trump would abuse the surveillance powers he had available to him.

> The electronic infrastructure is fully in place – and ex post facto legalised by Congress and executive orders – and ripe for further abuse under an autocratic, power-obsessed president. History is just not kind here. Trump leans quite autocratic. The temptations

> to use secret NSA surveillance powers, some still not fully revealed, will present themselves to him as sirens (Drake, 2016).

In the UK, Trump's election was also used as evidence by the DRC that their fears were well-founded. ORG director, Jim Killock, tweeted shortly after his election that 'Donald Trump has effective control of GCHQ's technology and full access to their data collection' (Killock, 2016).

> Given that the agencies' operations are nearly indistinguishable, it makes it incredibly hard for the UK to resist using our resources for risky endeavours or even human rights abuses … Trump's election ought to remove the complacency MPs have been suffering from (Killock, 2016).

For members of the DRC to trust state intelligence agencies, they are likely to require legislation and bureaucratic structures that guarantee future administrations will not exploit them for malicious purposes.

State actors are also concerned about the future and in particular the prospect of a 'dark' future where the intelligence agencies can no longer access information online (Hogan-Howe, 2014). The rapid growth of cyberspace has also posed challenges for legislation, which the state fears can become obsolete shortly after being passed. The state has attempted to combat this problem in the IPB by future-proofing its language and using generic terminology such as 'Internet Connection Records', 'Technical Capability Notices' and 'Electronic Protection', which Theresa May admitted were intentionally vague (May, 2016). The former head of MI5, Lord Evans, explained that 'In the rapidly changing world of communications, the new Act gives as much 'future proofing' against technological change as we are likely to achieve', but this future proofing is inevitably threatening to the DRC (Evans, 2016). Whilst the government has consistently denied that they wish to ban encryption, references in the IPA to 'removing electronic protection' have led many in the DRC to fear that that is exactly what they wish to achieve.

To overcome the security dilemma, some resolution to both the current and future fears and uncertainties of both the state and the DRC must be achieved.

6.4.3 Positive Signalling

Weapons such as guns and knives carry ambiguous symbolism since they can be used to hunt and prepare food, as well as to attack others. Similarly, nuclear non-

proliferation treaties are difficult to enforce because it is difficult to determine whether nuclear facilities are designed for civilian or military applications. But this ambiguity can be countered through better use of signalling to convey an actor's intentions. Signing up to arms control agreements, demonstrating adherence to a defensive doctrine or withdrawing offensive weapons, may help to signal to another party that an actor's intent is defensive in nature. Defensive signalling can cause an increase in overall security if it encourages the other side to do the same. An example occurred during nuclear tensions between India and Pakistan, when each side agreed to a state of non-deployed non-weaponization, where nuclear warheads were stored away from their delivery vehicles. This signalled to the other that the weapons existed for defensive and not offensive purposes (Ganguly & Hagerty, 2006).

Within the CSD, the state's intentions towards encryption provide a good example of ambiguous symbolism that serves to exacerbate the conflict. The DRC's sensitivity towards any suggestion that encryption might be 'banned' or 'weakened' has previously been discussed, but the government's actions often inflame these concerns, as demonstrated by Home Secretary Amber Rudd's attempt to explain the government's position on encryption (Rudd, 2017).

> To be very clear – Government supports strong encryption and has no intention of banning end-to-end encryption. But the inability to gain access to encrypted data in specific and targeted instances – even with a warrant signed by a Secretary of State and a senior judge – is right now severely limiting our agencies' ability to stop terrorist attacks and bring criminals to justice. I know some will argue that it's impossible to have both – that if a system is end-to-end encrypted then it's impossible ever to access the communication. That might be true in theory. But the reality is different...
>
> … Real people often prefer ease of use and a multitude of features to perfect, unbreakable security. So this is not about asking the companies to break encryption or create so called "back doors". Who uses WhatsApp because it is end-to-end encrypted, rather than because it is an incredibly user-friendly and cheap way of staying in touch with friends and family? Companies are constantly

> making trade-offs between security and "usability", and it is here where our experts believe opportunities may lie (Rudd, 2017).

Rudd claimed that she was being very clear, but her statement was extremely ambiguous. She suggested that the reality of end-to-end encryption was different to the theory, but she was not clear how that was the case. She hinted that an opportunity lay in the trade-off between security and usability, but did not say what that opportunity was. Rudd's comments were interpreted in many ways, including that she wanted to 'ban encryption', that she thought that 'ordinary people don't care about security', that she wanted technology companies to assist the police with hacking, and that she wanted companies to push out compromised apps with end-to-end encryption disabled (Open Rights Group, 2017). Jim Killock of the ORG said she had caused 'immense confusion' and Renate Samson of Big Brother watch claimed her comments were 'at best naïve, at worst dangerous' (Samson, 2017; Killock, 2017).

Ambiguous signalling such as this leads to the worst-case scenario assumption that the government wants to ban encryption. Clearer signalling will be an essential part of any moves to solve the CSD.

6.4.4 Ideological Flexibility

Ideological fundamentalism occurs when policymakers bring biases to an encounter and assign an enemy status to others based on their political identity and what they are, rather than how they behave. Ralph White describes this as the 'diabolical enemy image' and suggests that it is the major cause of war (White, 1984).

> An exaggerated, literally diabolical image of another country—a country that is actually composed of human beings not so very different from the citizens of one's own country—is in my judgment the very taproot of war in the present-day world (White, 1984, p. 121).

Examples of ideological fundamentalism include the US' hostility towards Iranian and North Korean nuclear capabilities whilst it remains ambivalent towards Israeli and Indian capabilities, and the designation of the US as the 'Great Satan' by Iran. In these examples, the designation of the other as evil creates a lens through which their actions are viewed. For co-operation to improve, ideological fundamentalism such as this must be resisted.

> security dilemma sensitivity can be significantly enhanced, and hence the prospects for co-operation improve, if leaders avoid ideological fundamentalism, characterised as it is in practice by stereotyping, crusading and black boxing (Booth & Wheeler, 2008, p. 165).

A clear example of Ideological fundamentalism within the CSD is the 'diabolical image' of state surveillance practitioners that is constructed by many within the DRC. Chapter 2 discusses how the DRC uses dark and shadowy Orwellian language to construct the state as a threat, and common phrases such as 'Snoopers' Charter' serve to denigrate legislation such as the IPA. The ORG describe how they use this language to resonate more with the public and gain support.

> …it's an attempt to reclaim the language … which I think is often important when you have things like this a lot of the public reaction is based upon the way they see the framing of these things. Communications campaigning is about your language prevailing over theirs essentially; the question is, is your language and your explanation for certain phenomena, do they resonate more or less with the public? Do they believe your story more or less? And the language you use to explain those stories is a vital part of that (Killock, 2016).

Constructing the state as a diabolical enemy may be a useful way to gain support for the cause of digital rights, but once the state has been constructed in this manner it becomes far more difficult to understand their real fears and uncertainty and move towards cooperation.

As well as people, technology itself can be viewed in an ideologically fundamentalist manner. The DRCs consideration of all state attempts to gain access to data as backdoors, the institutionalisation of backdoors as inherently threatening, and opposition to anything that might be viewed as 'weakening encryption' are all examples that have been previously discussed (Cook, 2016; Schneier, 2016). The state's view that there cannot be any 'safe spaces' for terrorists online, or any form of communication 'that we cannot read' can also be viewed in a similar manner (Cameron, 2015; May, 2017).

The more each side entrenches into these seemingly incompatible ideologies, the more difficult it becomes to establish common ground and work towards mutually

acceptable solutions. To overcome the security dilemma, ideological fundamentalism must be replaced by ideological flexibility, which allows issues to be considered on their own merits, rather than through the lens of an established ideology.

There is also something to say about the notion, often expressed by each side, that technology can be the solution. This is something that Egbert Schuurman calls technicism, 'a fundamental attitude which seeks to control reality, to resolve all problems with the use of scientific-technological methods and tools' (Schuurman, 1997, p. 1). But, as Schuurman explains, 'science and technology must not play a messianic role' (Schuurman, 1997, p. 2). Whilst technical innovations may play their part in overcoming the CSD, they cannot be relied upon alone, and each side must realise the limitations on technology to solve all their problems.

6.4.5 Security Dilemma Sensibility

Booth and Wheeler use the term 'security dilemma sensibility' to describe the ability of an individual to understand the point of view of the other (Booth & Wheeler, 2008, p. 7).

> Security dilemma sensibility is an actor's intention and capacity to perceive the motives behind, and to show responsiveness towards, the potential complexity of the military intentions of others. In particular, it refers to the ability to understand the role that fear might play in their attitudes and behaviour, including, crucially, the role that one's own actions may play in provoking that fear (Booth & Wheeler, 2008, p. 7).

The ability to appreciate the other's point of view is essential to overcoming the security dilemma and has been the foundation of several historic peace initiatives. In 1977, Egyptian leader Anwar Sadat surprised many when he explained to an Egyptian magazine why Israeli's lived in fear for their existence.

> They lived in ghettos fearing majority populations everywhere. They were exposed to many massacres and persecutions … Life itself is their problem. They are not threatened by a lack of food or housing. But they are threatened in merely maintaining an existence. That is why they have been truly terrified of the slogan "we will bury you in the sea" (Mangold, 1990, p. 63).

Following Sadat's words, Egypt and Israel signed the Camp David Accords and later the Egypt-Israel Peace Treaty. Sadat's ability to appreciate the fears of the other contrasts with others who are unable to understand how others might perceive them. When writing about Pakistan's nuclear standoff with India, President Musharraf wrote in his memoirs that 'India's intentions were offensive and aggressive, ours were defensive' (Musharraf, 2006). He failed to see the fear that drove India's actions and this proved an impediment to lasting peace.

Lack of security dilemma sensibility leaves each side frustrated with their inability to explain to the other why they feel threatened. For many within the DRC, this is best encapsulated by the phrase 'if you have nothing to hide you have nothing to fear', which has been used by defenders of surveillance to reassure those concerned with the practice that if they are innocent then they have nothing to worry about. It was initially successfully used by John Major in defence of a programme to vastly increase the installation of CCTV cameras around the country, and resulted in CCTV being widely viewed as a friendly eye in the sky rather than an Orwellian intrusion (Rosen, 2005). The phrase was also used by the Foreign Secretary William Hague in the immediate aftermath of the Snowden disclosures, and then repeated by Conservative MP Richard Graham when addressing the House of Commons on the draft Investigatory Powers Bill (The Independent, 2015). As Daniel Solove points out in his book, 'Nothing to Hide', the phrase resonates well with many members of the public who argue that as they have nothing to hide they are quite happy for the government to conduct surveillance, but for the DRC it is often associated with authoritarianism and is frequently linked to both Nazi Propagandist Joseph Goebbels and George Orwell's 1984 (Solove, 2011). Negative reactions to the phrase are powerful and there are dozens of academic papers and online articles claiming to debunk it (Solove, 2011; American Civil Liberties Union, 2013; Crossman, 2008; Freiwald, 2014). The ORG provides a thorough summary of arguments against the notion, including quotes from digital rights campaigners such as Edward Snowden, Bruce Schneier and Glenn Greenwald.

> The premise [is] that privacy is about hiding a wrong. It's not. Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect (Coustick-Deal, 2015).

For the state, the phrase may seem intuitive for they 'know' that they mean the public no harm, but the use of the phrase demonstrates a lack of sensitivity to the fears of the DRC and exacerbates the CSD.

The difficulty the state faces in understanding the fears of the DRC is encapsulated by GCHQ analysts, who respond to allegations that they are conducting mass surveillance with the question 'how can people actually think we live like this?' (Fiona, 2016). From their perspective, intelligence professionals 'know' that they are acting in the public good, have no interest in reducing individual rights and 'know' that they make considerable efforts to protect these rights.

A similar issue from the state's perspective relates to the so-called 'Going Dark' problem of surveillance. For state intelligence agencies, a major concern is that encryption and other security technologies are impeding investigations and, if not countered, the trend will lead to the breakdown of law and order. But many within the DRC describe this as a myth and reports such as 'Don't Panic', which was written by several security and digital rights experts, claim to show how the future will provide more surveillance opportunities rather than less (Berkman Center, 2016). But, such claims show lack of sensitivity to the fears of the state, which is concerned over the inaccessibility of *any* particular form of communication rather than the overall volume of data available. This fear is repeated frequently by the state but ignored by the DRC. The following quotes are examined in Chapter 2 but it is worth revisiting them here to examine the language carefully. Cameron, Hogan-Howe and Rudd do not claim that the overall volume of information available to law enforcement is reducing but instead focus on their fear that particular areas of cyberspace are becoming inaccessible to the state.

> Do we want to allow a means of communication between two people, which even in extemis, with a signed warrant from the home secretary … that we cannot read? ...My answer to that question is no, we must not (Cameron, 2015).

> We cannot allow parts of the internet - or any communications platform - to become [a] dark and ungoverned space (Hogan-Howe, 2014).

> We need to make sure that organisations like WhatsApp … don't provide a secret place for terrorists to communicate with each other (Rudd, 2017).

The lack of security dilemma sensibility on both sides of the conflict serves to exacerbate the CSD and impede efforts towards a resolution.

6.4.6 Good Interpersonal Relationships

The success of co-operation is dependent on the personalities of those involved and the relationships between them, and this depends on the willingness and ability of leaders to rise above their preconceptions and engage with the other's counter fear. The relationship between Ronald Reagan and Mikhail Gorbachev is a good example of a personal relationship between leaders that helped to overcome the security dilemma by establishing friendship and trust but, as King Hussein of Jordan explains, for peace to fully take hold it is the people who must learn to understand and trust each other.

> It is the tearing down of barriers between people. It is the coming together, coming to know one another. It is the children of martyrs on both sides embracing … it is people getting together and doing business. Real peace is not between governments but between individuals who discover that they have the same worries, the same concerns, that they have suffered in the same way, and that there is something they can both put into creating a relationship that would benefit all of them (Shlaim, 2007, p. 544).

Interviews with GCHQ staff revealed a common lament that if only people could get to know them they would realise that they're well-intentioned, but the secrecy that surrounds surveillance practitioners makes this difficult to achieve. When the opportunity has arisen, it has been difficult to get GCHQ staff to engage with the DRC because they do not want to be 'in the firing line' (Fiona, 2016). To overcome the CSD both sides must be willing to reach out, engage with the other and establish good interpersonal relationships. Chapter 7 explores this idea further in the context of Hunted and the exposure that former state intelligence actors experience whilst participating in the show.

6.4.7 Trust

Booth and Wheeler consider trust to exist on a spectrum between functional co-operation and interpersonal bonding (Booth & Wheeler, 2008, p. 229). Functional cooperation describes our trust in a chef not to poison our food, despite us not having met them, because we judge that this is not in their interests. At the other end of the spectrum, interpersonal bonding is the trust an individual has in the

people they know. Trust is a strategy for dealing with uncertainty, which can lead to what social psychologists term the 'trust dilemma', where wrongful mistrust can lead to missed opportunities, but misplaced trust can lead to the risk of being taken advantage of (Kramer, 2001). The 'trust dilemma' lies at the heart of the security dilemma's dilemma of interpretation, as it is only through trust that a positive interpretation of the other's activities can be made.

6.4.7.1 Trust Attributes

To escape this dilemma, we must begin to trust others whilst convincing them to trust us. Booth and Wheeler propose four linked pairs of attributes of trust that they argue are central to its existence.

Leap in the dark/uncertainty

All relationships begin in a condition of uncertainty and to develop trust, one party must take a 'leap in the dark', trusting the actions of another when the consequences are uncertain. This is a high-risk high-reward strategy that could lead to devastating consequences if the trust is misplaced, but could equally help to break the insecurity spiral if reciprocated by the other.

Empathy / Bonding

Empathy, according to Lauren Wispe, is the 'self conscious effort to share and accurately comprehend the presumed consciousness of another person, including his thoughts, feelings and perceptions as well as their causes' (Wispe, 1968, p. 441). Empathy allows an actor to understand the fears of their adversary, which helps to establish trust and facilitates cooperation. Karin Fierke argues that processes that build mutual empathy can create environments in which each side can 'acknowledge how the acts of the other have been conditioned by their own experience of suffering', and 'analytic empathy' can help each side acknowledge how they have contributed to this suffering (Fierke, 2005, p. 148). As former UN Secretary-General Dag Hammarskjold put it:

> You can only hope to find a lasting solution to a conflict if you have learned to see the other objectively, but, at the same time, to experience his difficulties subjectively (Booth & Wheeler, 2008, p. 237).

To achieve this, individuals must 'hold in suspension two interpretations of the same facts, the other fellow's and one's own' (Booth & Wheeler, 2008, p. 237).

Bonding can follow from empathy and can lead to longstanding and robust relationships once a personal or political relationship has developed and a new collective identity has been formed.

To reach such a state between members of the DRC and the British state will require a slow establishment of relationships, a mutual expression of fears and concerns, an acknowledgement by the state of how the concept of surveillance threatens the DRC and an acknowledge by the DRC of how their actions affect the state's ability to investigate and prevent threats. This also requires the establishment of personal relationships, which can be achieved by shared events such as those held at Wilton Park and Ditchley Park.

Dependence/ Vulnerability

As Hoffman explains 'trust refers to an actor's willingness to place something valued under another actor's control' so to trust is to risk betrayal. (Hoffman, 2002, p. 394). To trust, actors must accept their vulnerability to betrayal if the trust placed in the other is misplaced. To move towards resolving the security dilemma each actor must accept that they are vulnerable to harm from another, but trust that this power will not be abused.

Currently, Edward Snowden and many within the DRC do not take the view that they should place their data and their privacy under the control (or even reach) of governments and intelligence agencies. As Snowden puts it, we should 'speak no more of faith in man, but bind him down from mischief by the chains of cryptography' (2014, p. 24). In other words, we should place out trust in cryptography and not the state. But after around half a century of the Crypto Wars and half a decade since Snowden's disclosures, the DRC have been proven incapable of using cryptography to completely prevent state surveillance. As members of the DRC readily admit, regulation, hacking, subversion, court orders, backdoors and other means have allowed the state to continue surveillance practices regardless of advancements in technology. The state may be restricted but it is by no means shackled. Despite what some would like to believe there is no technological silver bullet to help win the Crypto Wars for either the state or the DRC. Applying the work of Booth, Wheeler and Hoffman to the problem indicates that for the DRC to really feel safe, they must accept that they are vulnerable to harm from the state, but trust that this power will not be abused. The plea to 'trust us' is frequently rejected out of hand by the DRC but if the state can start to

demonstrate its trustworthiness by being more accountable, transparent and accessible then perhaps, over time, the DRC will become more willing to accept a certain level of vulnerability.

Integrity/reliability

If actors behave with integrity and act in a reliable and predictable fashion, then feelings of mistrust and uncertainty can be overcome. If interactions between states are peaceful then 'states can internalise positive images of one another, and come to expect friendly behaviour in the future. They can learn to trust one another' (Shore, 1998, p. 334).

Impediments to trust

Misperceptions about the other, which are often driven by bias and prejudice, can make it difficult to establish trust between two parties. Both psychological and bureaucratic biases can impede trust and fuel the security dilemma. Attribution theory states that humans are motivated to assign causes to the actions and behaviours of both themselves and others, which can be subject to psychological biases (Kassin, et al., 2015). One example is the Actor/Observer difference, which posits that people attribute their own behaviour to situational factors whilst attributing others behaviour to dispositional factors. For example, a leader might consider their own military forces to be necessary due to a variety of internal and external pressures, whilst simultaneously interpreting another's as evidence of hostile intent. Likewise, the DRC consider their own desire for privacy/secrecy to be necessary for their own security, due to hacking and an intrusive state, whilst simultaneously interpreting the state's desire for secrecy as evidence of malintent. Mirroring this, the state considers its own desire for secrecy to be necessary for national security, due to terrorism, organised crime and hostile states, whilst simultaneously believing that only those with something to hide, should require privacy from the state.

Whilst individuals are susceptible to psychological bias, bureaucratic bias from within states can also reduce trust and fuel the security dilemma. Militaries are inclined to exaggerate an adversary's capabilities for a variety of reasons, including a desire for conflict, hostility and a safety-first approach to risk assessments. Glaser also suggests that powerful interest groups who could benefit from military competition or expansion might exaggerate an adversary's capabilities or motives to advance their own interests. States are also inclined to create and re-enforce

myths about their own unthreatening nature, while in turn fantasising about the threat of others (Evera, 1998).

Attempts to overcome the CSD will only be successful if built upon a foundation of trust but, after years of mutual suspicion, developing such trust is a long and difficult process.

6.4.8 Transparency

Stephen Van Evera describes secrecy as a 'hydra-headed cause of war' as it can result in actors under or overestimating each other, allows for surprise attack, raises the risk of preventative war, narrows the circle of experts consulted on policy, and prevents arms control agreements by making them harder to verify (Evera, 1998, p. 11). Michael Colaresi argues that whilst transparency can resolve these issues, secrecy is essential for national security and this results in a 'Secrecy Dilemma' (Colaresi, 2014).

> How can the public be confident that foreign policy programs advocated by the executive will enhance security if that same leader has the power to selectively reveal and hide relevant information? The capacity to keep secrets is useful for security, but it can also be used for non-security ends. The same classification and counterintelligence powers that can hide security vulnerabilities and reduce threats to the public can also cover up executive incompetence and corruption or undercut legitimate domestic political opposition (Colaresi, 2014, p. 1).

Whilst the issue of secrecy appears intractable, Colaresi suggests that 'transparency cost deflation' and oversight bodies can be used to mitigate the problem. National secrets tend to lose their value over time as capabilities become obsolete, sources no longer need protecting and enemies become allies. The details of the allied capability to decipher German Enigma codes is an obvious example of a national secret that was of huge value at the time, but no longer has a transparency cost associated with it. Therefore, the delayed release of secret information can provide some degree of accountability and oversight without significant transparency costs.

Oversight institutions exist outside of the executive and have the powers to investigate abuses of state power whilst simultaneously protecting sensitive information. If they are considered to be more trustworthy than the institutions they are overseeing, then this can help to reassure the public by ensuring that

wrongdoing is exposed and wrongdoers are punished. Strong and trustworthy oversight institutions are essential to uncovering wrongdoing, but they can also benefit national security by bolstering public support in times of crisis.

> Retrospective oversight institutions should lead to greater public support during international crises. Because there is a greater probability of abuse being revealed, ex post, with stronger oversight institutions, citizens have less reason to distrust that crisis actions are not in the public interest (Colaresi, 2014, p. 11).

As discussed, trust plays a huge role in the CSD. Mistrust in the state leads the DRC to consider its capabilities to be threatening and, when the state discusses issues such as encryption, this distrust leads the DRC to assume that the state wants to ban it. For the state, there may be bureaucratic biases that cause it to have exaggerated fear of threats such as 'Going Dark'.

Much of this trust is fuelled by the secrecy that surrounds the intelligence agencies. Edward Snowden claimed that 'transparency' was the goal of his disclosures and that he handed over NSA and GCHQ files to journalists because he trusted them rather than the government to determine what should remain secret and what should remain concealed (Snowden, 2013). Whilst GCHQ maintains that the secrecy surrounding surveillance is designed to protect national security, a leaked internal memo from a court briefing appeared to suggest that GCHQ wished to also use secrecy to avoid public debate and legal challenges (Guardian, 2013).

> Our main concern is that references to agency practices (i.e. the scale of interception and deletion) could lead to a damaging public debate which might lead to legal challenges against the current regime (Guardian, 2013).

The state has attempted to address this issue within the IPA, which grants significant new authority to oversight organisations, including the new 'Investigatory Powers Commissioner', who is charged with ensuring that the intelligence agencies act within the law. Since its inception in September 2017, The Office of the Investigatory Powers Commissioner (IPCO) has taken steps to build trust with the public by demonstrating its independence from the intelligence agencies. One example is a pinned Tweet on its Twitter feed which reads: 'Watching the watchers … Since September 2017'. This applies phraseology normally associated with the DRC, such as in Spy Blog's tagline 'Watching Them, Watching

Us', and helps to portray the IPCO as independent of the intelligence agencies, not subservient to them like the old Intelligence and Security Committee were often accused of being (Blog, n.d.; Investigatory Powers Commissioner's Office, 2017).

Whilst the potential for the IPCO to help build trust is encouraging, less progress has been made on direct disclosure of information relating to GCHQ's activities. The government's policy on releasing state information has evolved over time from the 50-year rule set in 1958 to the 30-year rule set in 1967, and current efforts to reduce the period to 20 years, but exceptions can still be made for national security-related documents. Without better disclosure, the DRC will tend to assume the worst of the intelligence services, who are themselves impeded from defending their own activities. After the Snowden disclosures, GCHQ was left frustrated because, in their own words, 'someone else had told our story … but it was wrong' (Fiona, 2016). They also commented that they had 'one arm tied behind our back because we can't talk about specific cases' (Matt, 2016). Whilst transparency can harm national security, so too can secrecy if this results in reduced trust in the intelligence services and a consequent reduction in formal and moral support for their activities. Allowing GCHQ to discuss intelligence matters and release intelligence material to the public in a way that does not compromise national security could have a significant impact on the trust relationship between the state and the public.

The use of transparency to de-escalate tensions was demonstrated in the BRIXMIS and SOXMIS exchange programmes, which were enacted during the Cold War. An agreement between the UK and the Soviet Union permitted military units from each country to operate in the other's zone of influence in Germany, allowing them to gather intelligence on the other side. The missions reassured each side that the other was not planning an imminent invasion and helped to de-escalate tensions. The Limitation of Strategic Offensive Arms Treaty (SALT II) is another example from the Cold War. As part of the treaty, the US and the Soviet Union banned the use of encryption during certain types of weapons testing so that the other side could gather intelligence on the function and capability of the weapon (Bureau of Arms Control, Verification and Compliance, 1979). Banning encryption provided transparency and reassured each side about the other's capability, thus helping to de-escalate tensions.

6.5 CONCLUSION

The Cyber Security Dilemma has endured for over forty years, yet seems no closer to resolution than it did in the early days of encryption export bans and mandatory hardware backdoors. The exponential growth of cyberspace and its importance to society has raised the issue from a niche dispute, presided over by academic experts and government intelligence agencies, to one that impacts on the lives of billions of people across the globe. Whilst concern over surveillance appeared to ebb in the 2000's following terror attacks in New York and London, the issue returned to the public agenda with a vengeance in 2013, following the Snowden disclosures. The importance of the debate has grown dramatically but the issues have not changed significantly.

Competing securitisations, amplified by the media, have intensified the issue, which has become framed as binary, absolute and unresolvable. The key actors have become demonised, the language has become loaded with emotion, and each side has become firmly anchored to their own framing of the problem, making compromise and co-operation difficult. The difficulties in addressing issues of surveillance and encryption parallel those found in any global conflict and include long-standing enmity, lack of understanding, mistrust, insecurity, ambiguous symbolism, broken relationships, ideological fundamentalism and secrecy. As such, our experience of international relations might help point a way out of the CSD. By addressing trust, secrecy and the relationships between securitising actors, it might be possible to find creative ways to overcome the dilemma.

Each side has attempted to win the Crypto Wars or gain the upper hand but, paradoxically, unilateral efforts to boost security have often resulted in greater insecurity. Technical solutions have been proposed but enmity, mistrust and entrenched positions have hampered their progress.

Attempts to establish a dialogue have generally been unsuccessful due to the actors involved or the nature of the approach, but there has been some cause for optimism. The Ditchley Park event demonstrates that, away from the media and public spotlight, trust can be improved - a vital component of long-lasting peace. And there is a small but growing body of academics and other thinkers who are attempting to break the deadlock.

Solutions to the CSD need to operate on several levels. They need to resolve the enmity and distrust at the heart of the dilemma, they need to reframe the debate

away from entrenched issues of encryption and backdoors towards a more pragmatic and less ideological approach, and they need to provide technical solutions that resolve the fears of both the state and the DRC. There are still huge impediments to security co-operation, but by adapting the principles that have been used to improve security between nations there is the potential to establish an environment of collaboration and mutual security interest between the state and the DRC. This may ultimately reduce fear and deliver greater security for all.

7 HUNTED CASE STUDY

Chapters 1-5 describe how the DRC and the British state have securitised cyberspace, using technification, hypersecuritisation and everyday security practices. As each side has constructed the actions of the other as threatening, a CSD has emerged. Each side fears the actions of the other and takes their own action to counter this threat. This in turn appears threatening to the other, resulting in a spiral of insecurity and fear.

Chapter 6 explores current efforts to overcome the CSD and why they have so far been unsuccessful. It then draws on security dilemma theories to examine several principles that can be used to help overcome the problem. This chapter considers three of these principles in more detail, using the reality television show, Hunted. Using interviews, ethnographic research and episodes of the show, this chapter explores the issues of security dilemma sensibility, good interpersonal relationships and transparency, and how they can be utilised to help overcome the CSD. These principles have been selected because they form the foundations for overcoming security dilemmas and are particularly difficult to address within the context of the conflict between digital rights and national security.

7.1 HUNTED

The Channel 4 television show Hunted provides an opportunity to further observe state intelligence actors in an environment mirroring that of a British intelligence agency and to observe public reaction to their activities. Within this reality crime show, members of the public (fugitives) attempt to avoid a team of state intelligence actors (hunters) for 28 days. The hunters are split between an intelligence headquarters (Hunted HQ) and operations on the ground and they utilise surveillance techniques to try to discover and apprehend the fugitives. The show is broadcast over six, one-hour episodes, which focus equally on the fugitives' attempts to escape and the hunters' attempts to catch them. Hunted is unique in its portrayal of state intelligence actors at work and supplements the information gathered through discourse analysis and interviews used throughout this thesis. The show is comprised of fugitives, hunters, production and TV Command, each of which plays a specific role.

- **Fugitives**: Around 10 members of the public are selected by the production team to act as fugitives and spend up to 28 days on the run. They are

accompanied by a camera crew who are charged with recording the activities of the fugitives whilst remaining neutral to the hunt.

- **Hunters**: Around 30 members of the public are recruited by the production team to act as hunters. Most of these have had prior experience in policing, the military or the intelligence community, although some were recruited after completing an MA in Intelligence and Security[33]. Cyber expertise is provided by a team from NCC Group. The hunters are charged with finding and capturing fugitives within 28 days, using the same powers that the police and intelligence agencies would utilise in real life. They are split between around 12 ground hunters, who interrogate the fugitive's friends and family and follow up leads, and around 18 HQ hunters, who work in Hunted HQ and develop intelligence to find the fugitives. Hunted HQ is comprised of leadership, an analyst team, an information management team, a cyber team and an open source intelligence team. The hunters always wear microphones and camera crews record everything they do.
- **TV Command**: TV Command is led by former Detective Chief Superintendent, Kevin O'Leary. It coordinates the show, ensuring that the powers of the state are replicated accurately and that information which could compromise national security is not exposed.
- **Production**: The production team from Shine TV is responsible for recruiting the participants, producing and editing the show. They also liaise with the participants and attempt to address any concerns they have.

Due to my prior experience working for the police and the Royal Air Force, I was able to take part in Hunted as the lead intelligence analyst within Hunted HQ.

To a limited extent, Hunted acts as a proxy for observation of a real intelligence headquarters and provides some useful insight into the environment, practices and pressures experienced by state intelligence actors. This insight has been used throughout this thesis to help inform on the perspective and opinions of the state and the intelligence agencies. But despite significant efforts to replicate a real-world operation, Hunted cannot replace observation of a real-world intelligence HQ. However, Hunted does offers something more unique and insightful. The presence of television cameras and the broadcasting of the show on national television creates an additional layer of complexity which provides an opportunity

[33] These individuals took on more junior roles but were fully involved in the whole of the show.

to explore several issues that would usually be extremely difficult to study. These help inform our understanding of 3 of the guiding principles, set out in Chapter 6, which can be used to help overcome the cyber security dilemma; security dilemma sensibility, transparency and good interpersonal relationships.

The permanent presence of television cameras and microphones on the Hunters resulted in state intelligence actors experiencing surveillance for themselves. This resulted in them entering 'the other man's counter fear' and provided an insight into the difficult issue of security dilemma sensibility (Butterfield, 1951, p. 21). The presence of television cameras and microphones also allowed state intelligence actors to experience operating in a far more transparent environment than they were used to. This helped them to challenge their own perceptions around what this is like and how transparency should be approached within intelligence work. And finally, the broadcasting of the show to a large nationwide audience and the presence of non-state intelligence actors within Hunted HQ exposed the everyday actions and behaviours of state intelligence actors to members of the public. This provided an insight into how perceptions of state intelligence actors and their work may be influenced by their (lack of) exposure. This helps reaffirm the importance of interpersonal relationships to overcoming the cyber security dilemma.

There is substantial existing research into reality crime shows, such as Hunted, including John Sears' evaluation of the impact of reality crime show, 'Crimewatch' and Cavender and Fishman's consideration of the impact of US crime shows 'Cops' and 'America's Most Wanted'. Annette Hill also considers how reality crime television shows such as Hunted demonstrate the entertainment appeal of mixing facts and entertainment, which helps to connect crime entertainment with the real world (Fishman & Cavender, 1998; Sears, 1995; Hill, 2017). But the ethnographic study of Hunted within this work is focussed on the experiences of the show's participants and the audience's reaction to them, rather than the construction of the show itself. Such a study is unique in relation to the public understanding of the securitisation of cyberspace and the security dilemma.

7.2 An Exploration of Three Principles

The establishment of security dilemma sensibility, transparency and good interpersonal relationships are critical to overcoming the CSD, but the nature of the dispute between national security and digital rights makes addressing these issues particularly difficult. Transparency is difficult to achieve given the importance of

secrecy to national security and privacy to digital rights. Good interpersonal relationships are hard to establish, given the secrecy of state intelligence actors, and security dilemma sensibility is difficult when the two sides are distanced from each other and do not have access to the same information. Using examples from Hunted, the following sections will explore these issues further and draw lessons to help inform the wider question of how to overcome the CSD.

7.2.1 Security Dilemma Sensibility

Chapter 6 explains the importance of security dilemma sensibility to overcoming the CSD. Developing security dilemma sensibility requires a willingness to engage with and understand the motivations and actions of the other, but may only be fully achieved by living the experiences of the other, feeling their fears and seeing the situation from their entirely different perspective. As former UN Secretary-General Dag Hammarskjold put it:

> You can only hope to find a lasting solution to a conflict if you have learned to see the other objectively, but, at the same time, to experience his difficulties subjectively (Booth & Wheeler, 2008, p. 237).

To achieve this, individuals must 'hold in suspension two interpretations of the same facts, the other fellow's and one's own' (Booth & Wheeler, 2008, p. 237).

For state actors to achieve security dilemma sensibility, they must not only understand why the DRC fears surveillance but experience that fear for themselves and learn why surveillance is considered threatening. They must be able to move beyond the mantra of 'if you have nothing to hide you have nothing to fear' and begin to understand why good and law-abiding people still fear surveillance. David Lyon amongst others, explains this fear by arguing that surveillance leads to social sorting, which can lead to cumulative social disadvantage when the same people are subject to increased suspicion and scrutiny due to innocent activities such as attending a Mosque (Lyon, 2014). But as demonstrated in Section 4.4.2.4, state intelligence actors believe that their actions are defensive in nature and find it difficult to imagine why others would fear them.

Whilst state intelligence actors are subject to the same levels of surveillance as members of the public,[34] they do not fear this surveillance because they know the

[34] Actually, greater levels if security vetting is considered.

people, agencies and practices involved. It is difficult for them to see surveillance from the perspective of individual citizens. But during the filming of Hunted, a range of current and former state intelligence actors were placed in an environment where they were constantly watched and recorded by TV cameras and microphones. This simulated a level of surveillance and, whilst the hunters participated voluntarily and had no reason to distrust the show's producers, it still allowed them to experience what it is like to not know when you are being watched and not know how this information will be used. The show's hunters have experience in the police, military and intelligence agencies and are accustomed to using surveillance techniques to gather intelligence on criminals and terrorists. But, during Hunted, the ever-presence of television cameras and audio recording equipment served to emulate the experience of those within the DRC who feel that they are always being watched and monitored by the government. Everything the hunters did was recorded and monitored, and even visits to the bathroom could be accidently captured if they forgot to turn microphones off. They had little control over what was collected and how it was used.

This experience resulted in significant anxiety for the hunters. One of the major concerns was over their lack of control over data held about them. They were being filmed and recorded at all times, but the vast majority of this footage would never be seen by the public and the producers had the power to use this footage however they wished, potentially portraying the hunters in misleading and unflattering ways. There was no evidence to suggest that the producers would do this but the lack of control caused significant anxiety. The issue was raised by the hunters on several occasions, but the producers' appeals to 'trust us' and their promises not to use footage out of context did not appear to convince the hunters. The issue was a frequent topic of discussion on set, during lunch, and after filming, and was only quelled when the producers hosted a pre-screening of the first episode. Only once the trustworthiness of the producers had been proven were anxieties reduced, although some concerns persisted until the show was broadcast.

The experiences of the hunters parallel those who are told by the government and GCHQ to 'trust us', about how they use data collected on British citizens. Responding to the Investigatory Powers Tribunal, which ruled that state surveillance complied with the Human Rights Act, Rachel Logan, legal advisor for Amnesty International explained that 'trust us' was not enough.

> The government's entire defence has amounted to "trust us" and now the tribunal has said the same … "trust us" isn't enough (Logan, 2014).

Some of the hunters also experienced anxiety over the level of intrusion into their own individual privacy, which was demonstrated by an incident on set. During a quiet period, one of the producers appeared, accompanied by three other members of production. She took them around to each section and introduced them as some of the show's transcribers. Despite the show's procedures being explained in training, some of the hunters were surprised when the reality that individual members of production were listening to everything they said became clear. '[You listen to us] even when the cameras are not on us?' asked one of the analysts, 'yes, all the time', replied one of the transcribers. 'What about when we're off set making tea?' asked the analyst, 'yes', said the transcriber. 'So you heard us talking about…' said the analyst, referring to a conversation that occurred in HQ when, off camera, the hunters were talking about relationships. 'Yes' said the transcriber with a smile and a laugh. 'We try not to listen to conversations that aren't about the hunt but it's hard because we don't know what you're going to say next'. The analyst went quiet.

Despite being aware of the cameras, the filming and the microphones and despite having agreed to the conditions of the show, the reality of another human, unknown to them, monitoring everything they said, had only just dawned. After the incident, conversations were notably tamer and the hunters even took measures to defend their own privacy. As the head of the Cyber Team, Paul Vlissidis explains;

> You don't feel you have any real opportunity… any downtime when you can perhaps have a laugh and a joke about what's going on and so that increases tensions and frustrations. That said, there were a couple of occasions where we felt we needed to have a conversation and we turned our microphones off and went somewhere else to do it (Vlissidis, 2016).

A flick of the head to the set exit or a written note hidden from cameras was used to indicate a desire to talk in private and, after a quiet space outside the set was found, microphones were turned off.

The hunters were affectively under 'sousveillance', a term coined by Steve Mann to describe inverse surveillance, or the practice of surveilling the surveiller to

moderate their behaviour (Mann, et al., 2002; Mann, 1998). They reacted to this form of surveillance by engaging in resistance. Resistance to surveillance can take the form of counterveillance techniques, which include blocking all opportunities for surveillance by, for example, going off grid or through 'univeillance', which involves the continuation of normal communicative activities whilst blocking the surveiller, though, for example, the use of end-to-end encryption (Bakir, 2015). The hunters used counterveillance techniques by limiting their conversations, but then moved to univeillance by switching off microphones and shifting conversations to a different area. Whilst the hunters were not trying to hide illicit conversations and the show's producers were simply acting within the well explained requirements of the show, the experience did demonstrate to the hunters the potential negative impact of being on the other side of surveillance.

The scenario reflects the experiences of the those who fear state surveillance and act to evade it. A variety of polls reveal that internet users in major democracies self-censor their online conversations out of fear of state surveillance (Pew Research Centre, 2014; PEN America, 2015). Whilst the sheer volume of information, the technological and financial challenges, issue of proportionality, the limited resources, the ethics of state intelligence actors and the law, all preclude the pervasive monitoring of the entire population, there are many who believe that they are personally being monitored by the state, in the same way that the hunters were personally monitored by the show's transcribers. Through film, television and literature, the public have always had some general awareness of the capability of the intelligence agencies, but the Snowden disclosures turned that abstract notion into something more personal to many people. When Snowden revealed GCHQ's capability to hack into webcams, this capability was presented by the media as something personal to individuals, through headlines such as 'GCHQ has been checking **you** out through your webcam' (TechDirt, 2014). Even articles defending surveillance tended to personalise this practice, including the argument made by the Telegraph that 'Yes, Big Brother is watching **you**. But for good reason' (Telegraph, 2013). The sense that the Internet was being turned into a giant panopticon designed to control individual behaviour intensified after Snowden with both GCHQ and the NSA being accused of working towards this goal (Sullivan, 2013; Mitrou, et al., 2014).

Many feel that state surveillance is personally targeting them, and this leads individuals to take measures to protect themselves in a similar manner to the

hunters. The anti-surveillance campaign 'Don't spy on us', for example, is backed by around a dozen UK rights organisations and specifically highlights how surveillance impacts on the individual. Other examples include Facebook's policy to notify users if they think their account has been targeted by a nation state, and the large range of web pages that have been set up to help individuals determine if they have personally been targeted by GCHQ.

Addressing the lack of security dilemma sensibility on each side of the dispute is, perhaps, the most significant challenge of the CSD. This is exacerbated by the secrecy of state surveillance and the distance between state intelligence actors and the DRC. But the experiences of the hunters demonstrate that whilst It is difficult to develop a better understanding of the fears of the other, it is not impossible. Although the experiences of the hunters are hard to replicate on a large scale, other measures to broaden the perspective of state intelligence actors and encourage them to appreciate different viewpoints, are possible.

7.2.2 Good Interpersonal Relationships

Chapter 6 demonstrates the importance of good interpersonal relationships in overcoming security dilemmas. If actors on each side can develop good relationships then this can form the basis for developing security dilemma sensibility, trust, and shared values and identities. But state intelligence actors are, by their nature, hidden from the public and this means that their image is still very much shaped by the news and entertainment media. Fictional characters, such as James Bond, characterise the state intelligence actor as 'an action hero of extraordinary abilities', whilst John Le Carre invokes a world of skulduggery and deceit (Funnell & Dodds, 2017, p. 220; Winder, 2006).

In Beyond Bond, Wesley Britton charts the development of espionage fiction, highlighting how various modern 'spy traits' have become established over time (Britton, 2005). These traits include patriotism ('39 Steps' – John Buchan), fearlessness and bravery ('The Spy – James Cooper), mystery and intrigue (French/Spanish dramas) and a maverick and shadowy nature ('Sherlock Holmes' – Sir Arthur Conan-Doyle). Espionage itself has been characterised as a 'Great Game' (Rudyard Kipling), futuristic, (Tom Clancy) glamorous (Ian Fleming) and adventurous (Sauerberg). These characterisations of state intelligence actors are also utilised and re-enforced by politics. State intelligence actors are often lauded for their heroism and patriotism by the ruling classes (May, 2017; Hammond, 2015).

Whereas their detractors, such as civil rights groups, often portray them as shadowy and untrustworthy (Snowden, 2013; Open Rights Group, 2013; Open Rights Group, 2009)

But despite these public constructions, most state intelligence actors are hidden from the public, so public imaginations of state intelligence actors can be extremely misleading. Peter Taylor of the BBC was given access to officers from MI5 and MI6 for a documentary called 'Modern Spies' (Taylor, 2012). He concluded that 'those who actually carry out these covert and potentially dangerous operations could not be further removed from their imaginary counterparts' (Taylor, 2012). MI6 Officer, Anna also highlights the discrepancies between the media portrayal and the actual reality of being an intelligence professional.

> If James Bond actually worked in MI6 today, he'd spend a large amount of time behind a desk doing paperwork and making sure everything was properly cleared and authorised. He certainly wouldn't be the lone wolf of the films (Taylor, 2012).

Some state intelligence actors also explain how working for the intelligence agencies has changed their own preconceptions of these organisations. MI5 Officer Shami explained how she was almost put off applying because she thought that 'you had to be upper class, academically bright and white male' to work at MI5 (Taylor, 2012). Similarly, MI5 Officer, Emma said she 'thought it would be largely male, and women would usually be a PA or Miss Moneypenny from James Bond' (Taylor, 2012).

Whilst the intelligence agencies have long survived under the cover of the Official Secrets Act, in recent years they have recognised the need to open up and improve their public image. As part of this process they have been particularly keen to highlight the existing diversity within the intelligence community in order to attract an even more diverse array of talent. GCHQ, for example, engaged in a very public act of support for 'National Coming Out Day' by lighting their headquarters in the colours of the PRIDE flag. They also attempted to draw a parallel between coming out as gay and GCHQ coming out as an organisation.

> In many ways GCHQ has come out as an organisation, and more than once. Not only from under a veil of secrecy back in 1983 when our function and existence was avowed in Parliament, but also more recently (Stewart, 2016).

Other initiatives include the CyberFirst Girls competition, which is designed to promote cyber careers to women, and participation in the Asian Network documentary 'Minority Report', which is designed to attract more Black, Asian and Minority Ethnic recruits and was discussed in Chapter 3 (GCHQ, 2016; GCHQ, 2017).

The relationship between state intelligence actors and the public can be affected by several factors, including the perceived entitativity of state intelligence agencies, mechanistic dehumanisation of state intelligence actors and a lack of familiarity with state intelligence actors. Entitativity is the degree to which an organisation or institution is viewed as a real entity rather than a collection of individuals. Castano et al demonstrate that the perception of the other is significantly affected by the degree of entitativity; the greater the entitativity the more threatening an institution can appear (Castano, et al., 2003). If an organisation such as an intelligence agency is imagined as a single body, then it can appear more threatening than if it is regarded as a collection of individual intelligence actors, who may act to moderate each other's behaviour. Dehumanisation can take the form of animalistic dehumanisation, where the individual is considered to be sub-human and mechanistic de-humanisation, where the individual is portrayed as cold, unfeeling and lacking in human nature (Haslam, 2006). Mechanistic dehumanisation is the most applicable to state intelligence actors, who are often portrayed as faceless figures or are represented using mechanistic imagery, such as CCTV cameras. Whilst familiarity is said to breed contempt, sociologist Niklas Luhmann argues that 'trust has to be achieved within a familiar world' (Luhmann, 2000, p. 94). Whilst familiarity is a precursor to trust it is difficult to achieve in the intelligence world where state intelligence actors are distant and separated from the public.

Intelligence agency entitativity, mechanistic dehumanisation of intelligence actors and lack of familiarity with state intelligence actors all serve to make it difficult to establish relationships between the state and the public. But by exposing state intelligence actors to both the public and others working on the show, Hunted provides a good insight into the importance of interpersonal relationships within the CSD. Given the lack of public visibility of state intelligence actors, Hunted represents a unique opportunity for state intelligence actors to be observed by the public, whilst carrying out their professional duties. Whilst Hunted takes place in the simulated environment of a television show, it is presented as an actual security

operation and allows the Hunters to be observed conducting analysis, making decisions and taking actions.

The first series of Hunted was pitched as an attempt to 'dramatically explore the scale of Britain's surveillance state's all-seeing gaze' (Channel 4, 2015). It was advertised through a series of interesting and innovative methods, which largely focussed on the scale of state surveillance and the difficulties faced by those attempting to avoid it. Adverts at train stations highlighted the volume of CCTV cameras monitoring passengers, adverts on cash machines instructed customers to cut up their credit cards, and oyster card holders informed recipients that these could be used by the state to track them (OMD Blog, 2016).

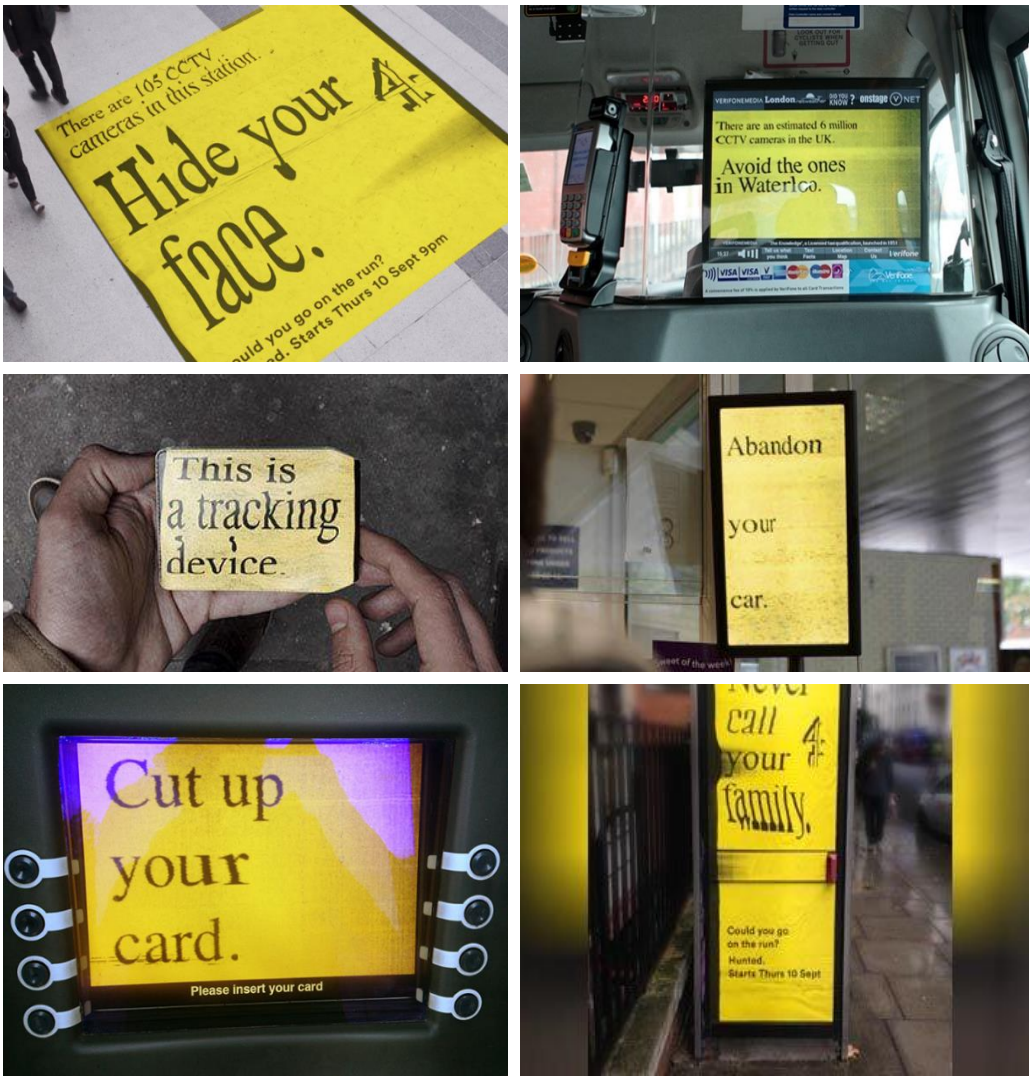

Figure 7.1: Hunted advertising

This advertising was supported by a social media campaign based on the Twitter handle @Hunted_HQ, which was designed to represent a sinister and shadowy

fictional character who worked for the hunters and was run by Aaron Eccles, the show's social media manager.

> [we constructed] a fictional Hunter that worked in Hunter HQ, that was slightly sinister, and we'd have this twitter account and we'd see people who talked about the show on Twitter and we'd kind of almost goad them a little bit, that kind of thing … oh you think you can hide … at the beginning of the series Hunted HQ came across as … it was sort of the state in a slightly shady way (Eccles, 2016).

The nature of the advertising campaign and the use of the @Hunted_HQ character helped to establish the fugitives as underdogs, set against the all-powerful state. The Twitter account portrayed the state as a faceless, sinister figure, indulging in its access to the private lives of its citizens; a portrayal that was also reflected in the advertising. The audience's initial reaction was to support the fugitives, but the Hunted social media team believed that this attitude began to shift as the show progressed.

> I think the view of the hunters and fugitives really changed as the show went on. It started with a huge amount of support for the fugitives, everyone was just thinking it's a regular person up against the state, up against this kind of powerful state and as an underdog can you actually get away from them so there was a lot of support for the fugitives … I think people began to shift, they started to see the hunters become characters in their own right … they stopped being a faceless force and started being real people … and so when there were a few episodes when the fugitives were caught and the hunters were quite pleased, the public would be happy with that (Eccles, 2016).

Eccles' observations demonstrate the impact of entitativity on the perception of state intelligence actors who became more popular when viewed as 'characters in their own right' rather than just part of the 'powerful state'. Feeling the hunter's emotions also helped to develop familiarity and to rehumanise the hunters as real people.

Whilst it is difficult to accurately quantify support for the fugitives and the hunters, there is some evidence that support for the hunters increased as the show progressed. The hashtags #TeamHunter and #TeamFugitive became established on Twitter to demonstrate support for each team and, although the hashtags were

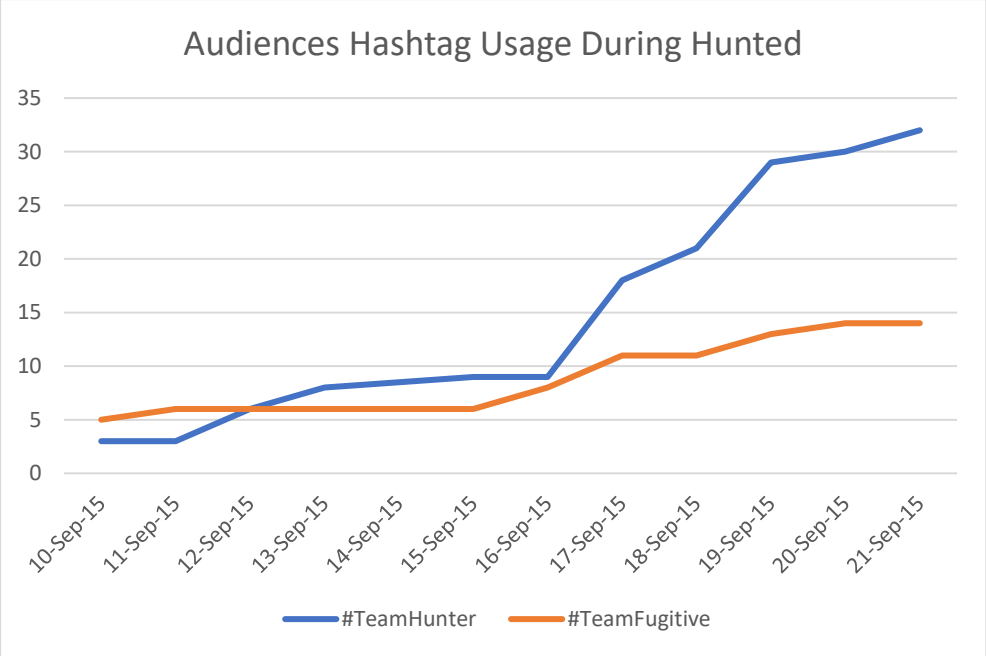

Figure 7.2: Hashtag usage during Hunted series 1

used by relatively few commentators, there was a noticeable increase in the use of #TeamHunter as the series progressed (See Figure 6.2).

This shift was a surprise to the show's producers, who had been expecting the fugitives to continue to enjoy most of the public's support.

> I don't think we expected to see this shift in support towards the hunters … the marketing campaign and the social campaign were all linked to this faceless force but you got to know them [the hunters] a bit better, I didn't expect that to happen in the way that it did, I think you saw their real emotions and having a laugh at times as well. They became a bit less scary (Eccles, 2016).

It also appeared to be the case that support for the hunters varied across social media channels. Peter Bleksley, the Chief hunter and the most active hunter on social media, attributed this difference to how much the hunters interacted with the audience on each channel.

> On twitter I found that support for the hunters was the prevalent view, people seemed to want to connect with the hunters on twitter, converse with them, they wanted fugitives caught … I

> found that the Facebook people were overwhelmingly in support of the fugitives. And they all wanted them to evade capture and thwart us. By using Twitter, we weren't remote people who were just on the telly, we were real people communicating, offering views, entering into conversations, really personalising that relationship (Bleksley, 2016).

Whilst the show changed the minds of some of the audience, the affect was even more intense for some of the show's participants. Whilst most of the hunters were former security and state intelligence actors, some had not previously worked for the state and this provided the opportunity to study their reactions working with state intelligence actors. One of the most striking reactions from the inexperienced hunters was their surprise at how 'normal' the experienced hunters were. Aisha Ishaq was studying for a Masters in Intelligence Studies when she took part in Hunted as an Intelligence Officer, but had no previous practical experience within the intelligence community. The show significantly altered her impressions of intelligence work and those who carry it out. Aisha explained that her impressions of intelligence and security practitioners before the show were negative; she did not think that they paid enough attention to ethics and they did not understand wider issues beyond their role.

> [before Hunted] I had a very strong perception of people in the military and in the police, who thought single-mindedly, very strategically … By strategic I mean achieving the goals, in the long run protecting citizens but being focussed on getting the work done and forward with the investigation… So the ethical side really gets chucked out the window (Ishaq, 2016).

But working with the hunters on Hunted gave Aisha a different perspective.

> [Hunted] gave me a different insight. In meeting Ben and Louisa who are from the military, they're just like normal people. You forget that these people are just like normal. But because I was in that academic environment, not knowing them outside of the classroom I was also getting only one side. Knowing Ben and Peter and Louisa and everyone else who had these backgrounds, they're just normal people. I was surprised that, yes, they are aware of

> different perspectives, they're just normal people you'd meet on a day to day basis (Ishaq, 2016).

Aisha's surprise at the normality of the state intelligence actors she worked with on Hunted demonstrates the disconnect between the public's perceptions of state intelligence actors and the day-to-day reality. Her reaction differed to Paul, who had also never worked for the state but had been previously been exposed to the intelligence profession through his work.

> I do actually have a high degree of trust in them [intelligence agencies] partly because I've been personally exposed to some of the individuals who work for those organisations because they're colleagues of mine and I've had direct dealings with some of those organisations throughout my career. I know that they do take a lot of care and trouble and concern around these things. My personal knowledge humanises them and makes you naturally much more trusting of them. I might feel a bit differently about it, if I had no personal knowledge of them, they would be this big brother like faceless identity and it would be very difficult to trust something like that because you don't know what their motives are, you've never been exposed to them in any human sense so your natural response is to be suspicious and to be wary. It's very much about your personal experience (Vlissidis, 2016).

Paul and Aisha's experiences reiterate the importance of people and personalities within the CSD. When seen as faceless, the intelligence community appear sinister, but when they become visible, this attitude can change.

Hunted revealed the human side of state intelligence actors, including their motivations, emotions and everyday human behaviour and this re-humanisation changed attitudes towards them. It is likely that that the secretive nature of the intelligence agencies is contributing to their de-humanisation, which in turns reduces the public's trust in their work. Whilst this secretive nature has previously added glamour and intrigue to the profession, in an era of distrust in state institutions this secrecy is now more damaging. Reversing this may be difficult for the intelligence agencies, who justifiably need to protect the identities of staff but if they are to improve trust then they must find a way to present the human side of intelligence work.

7.2.3 Transparency

Chapter 6 demonstrates the importance of transparency in overcoming the CSD. Whilst secrecy creates mistrust and suspicion, transparency can build trust and help provide future certainty. But the necessity of secrecy for national security creates a Secrecy Dilemma. Secrecy is required for national security but transparency is required for public trust.

Often, the British state's resistance to oversight of the intelligence agencies is considered evidence that they are behaving in a malicious manner. In calls for greater oversight of the intelligence agencies, the DRC sometimes reverse a trope used to defend surveillance, claiming that 'if the government has nothing to hide, then there's nothing to fear' (Casey, 2017). But fear of oversight can also be considered a natural upshot of the culture of secrecy, which is instilled within state intelligence actors from the moment they apply for a job and is re-enforced throughout their careers. Applicants to the intelligence services are informed that they can only discuss their application with close family and, if they are successful, they must maintain discretion for life. Every document they produce, computer system they use, building they enter, room they work in, and communications system they use, is assigned a classification which restricts its access. Employees are trained in the principle of need-to-know, so they can only discuss operations or capabilities with colleagues who have been specifically cleared to access that information.

As Charney and Irvin explain, this culture of secrecy makes it difficult to study the intelligence community, due to legal and national security restrictions and the limited availability of state intelligence actors for research (Charney & Irvin, 2014). But there are some sources of information that can help to illuminate how this culture of secrecy impacts on state intelligence actors. Laurence Miller's psychological guide to undercover policing, for example, describes the inability to discuss operations as a major stress factor for under-cover police officers (Miller, 2008).

> The most commonly reported symptoms included anxiety, heightened suspiciousness, loneliness, feelings of isolation, and relationship problems. Many officers were distressed at not being able to talk to anyone about the assignment (Miller, 2008, p. 11).

The impact of this culture of secrecy can also be studied using direct evidence from state intelligence actors themselves, which demonstrate the difficulty of operating in this type of environment.

> The hardest part is maintaining the web of lies you have weaved. It is a massive undertaking if you decide to live a robust social life like I did. I suppose if you take the hermitic path it would be a lot easier (Laux, 2016)

> Fewer than 10 people in the world know what I do, and they include close girlfriends and my ex-boyfriend. My parents couldn't tell their friends when I got the job, they couldn't tell anyone "look at what my daughter has achieved" since. That is hard on them (Anonymous, n.d.).

> The job of a spy can be very lonely**.** You can never discuss details of operations or what's happening with particular agents ... When you start off as a young recruit, you think, "Fine, that suits me." But it is emotionally crushing for officers in the secret services and you can never really share that guilt with anybody. You always carry that around with you. That does grind people down over time (Ferguson, 2014).

Long-term existence in a culture of secrecy can also generate paranoia within state intelligence actors, instil a fear of the spotlight, and lead to difficulties forming trusting relationships.

> When people ask what you do, you're trained to think what is it that this person is actually looking to learn? Do you want to know that I read top secret documents in the morning? (Anonymous, n.d.).

The unease with which state intelligence actors view intrusions into their world was demonstrated when the BBC was granted exclusive access to GCHQ in 2010. Reflecting on his experience, Mark Savage from the BBC explains how the presence of the BBC affected GCHQ staff (Savage, 2010).

> Their job is to listen in on others, record their conversations and pick up their e-mails. It is said, by the government, to provide "essential intelligence in the battle against terrorism and

> [contribute] to the prevention of serious crime". But for the first time in its history we were turning the microphones on them (Savage, 2010).

Prior to the BBC's visit, signs were placed throughout the building to warn staff of their presence and an announcement over the public-address system called for internal blinds to be closed when the BBC passed by. BBC staff were made to wear red badges, denoting their lack of security clearance, and were escorted around the building by minders. Whilst some staff were willing to talk to the BBC, Savage recounts that others 'weren't entirely happy with our presence … People gave us a wide berth. It felt like I had a communicable disease.'

Greater oversight of intelligence agencies is often the subject of lobbying by the DRC and there have been many technical discussions about how to produce greater scrutiny whilst limiting the impact on national security and the safety of state intelligence actors. The Investigatory Powers Act (IPA), for example, attempted to address the issue by creating a new Investigatory Powers Commission (IPC), which is designed to independently scrutinise the work of the intelligence agencies without compromising national security. However, whilst technical arguments for greater oversight might be convincing, for new policies to be effective, state intelligence actors themselves need to understand and accept the need for these policies. They also need to be reassured that they will not undermine the protection of national security and their own safety. The first step to achieving this is to understand how such efforts might be received by state intelligence actors, who are accustomed to a culture of secrecy and who might be naturally opposed to actions that reduce the protections traditionally provided by secrecy.

In Hunted, the culture of secrecy and fear of oversight was evident, although some of the hunters became more supportive of the idea of greater scrutiny because of the experience. Despite the appeal of taking part in an exciting show like Hunted, several of the hunters expressed significant reservations about participating and several prospects turned down the chance to take part due to concerns over the exposure they would receive. Several of those who did take part were also apprehensive about making the switch from the secretive world of intelligence to the very public world of television. Hunted transformed the watchmen into the watched through the permanent presence of television crews, which recorded every statement, action and decision that was taken by the hunters. For many who

took part, including Ben and Paul, stepping out from the shadows was extremely unnerving.

> When I was in [a government intelligence job] I saw this as a massive no-no. I was part of an operations centre over the Olympic period and I was very fully aware that in the future it would be all linked up with CCTV and we would wear microphones and everything would be recorded, the thought process, the decisions made, the logs, it's written down, it's on the computers, it's recorded visually and verbally and I really did not want to go down that route (Owen, 2016).

> When I first started it I felt very, very uncomfortable as for my whole life I've been trying to avoid cameras, I'd normally run a mile so it took me a while to get used to it, to realise I'm not in that world anymore, its fine (Owen, 2016).

> Particularly in the early days of filming, we all felt quite self-conscious that we were being scrutinised essentially by being on the show. What we were saying was being scrutinised, the level of your professionalism is being scrutinised (Vlissidis, 2016).

One of the major reservations expressed by the hunters was the fear that the show would expose surveillance capabilities to criminals and terrorists. One of TV Command's responsibilities was to protect these capabilities by ensuring that only those within the public domain could be used throughout the show. Despite TV Command holding final responsibility for protecting these capabilities, many of the hunters were still wary about compromising national security, despite most having left active service.

Prior to the start of filming, three days were set aside to enable the hunters to familiarise themselves with equipment, establish working practices and learn about how the show would operate. There were also discussions between the hunters and TV Command about what intelligence techniques might be used to track down the fugitives, how these could be facilitated and how they might be presented to the audience. Despite the show only utilising techniques within the public domain, there was substantial unease within the hunters that they could inadvertently reveal information that might damage national security. Whilst the show's producers took significant measures to protect against this, observation of the

hunters revealed this tension to be evident throughout the show and after it was broadcast.

The hunters also felt personal responsibility for the intelligence they collected on the fugitives. Whilst they were motivated to acquire as much information as they could about the fugitives and their associates, it became apparent that they also became personally responsible for the protection of this information. As head of the Cyber Team, Paul had direct access to the most intrusive data from the fugitive's phones and computers, and despite the fugitives giving permission for this intrusion into their lives, he began to feel personally protective of the information his Section discovered.

> I was concerned that although people had given all this permission … there might be things that came out as a result of the programme that when they saw it in the edit they'd be absolutely horrified because … suddenly their lives would be a matter of public record and that did concern us, and we did agonise over that…. you feel responsible for the information you've just acquired I felt like I was a bit of a custodian (Vlissidis, 2016).

> Emma Channel's i2 charts showed 5 calls to one telephone number. That was the most number of calls she made in that time period and that telephone number turned out to be a medical centre. I deliberately did not ask for us to monitor that telephone number because I felt that the potential collateral damage to that was too intrusive to too many people and we're talking about people's medical histories. Even though that might have been the key to unlock the mystery of where she was I deliberately said we're not applying for that one (Bleksley, 2016).

The examples demonstrate some of the human factors that promote a reluctance to accept oversight and scrutiny within the intelligence agencies. However, the experiences of the hunters also demonstrate that this reluctance can be overcome. Despite initial wariness of the TV cameras, Hunted was a transformative experience which led some of the hunters, such as Chief Peter, and Deputy Chief Ben, to change their existing attitudes towards oversight and scrutiny.

> Having done the Hunted experience, having sat there in an Ops room with these massive great big cameras and obvious

> microphones and that not having an effect greatly on my work then … it was fine, it's a good thing and it's accountability isn't it and I think that better decisions will be made in the long run. if people have been trained properly and they're applying the correct processes to their work then they're going to make the right decisions whether its recorded or not and I think that would give the public more assurance and hopefully give them less paranoia, I think they should publicise that more, I think they should say look these are all recorded, we're not sitting here smoking cigars, drinking whiskey saying ah we should shoot the guy anyway, it's all recorded and I think they should let the public know that, I really do (Owen, 2016).

Both Peter and Ben suggested that after the experience they would both me more accepting of scrutiny and even advocate for a change in practices.

> I think that if I talked to them now I would say it's [greater scrutiny] a really good idea and they [his former colleagues] would say it's a really bad idea. I've changed my view (Owen, 2016).

> What it did do [the presence of TV cameras] is it kind of just cranked up the tension a little bit because your every word and deed and action was on camera but, you know, it's quite a good thing because it's almost a check and balance being in place there and I found it, looking back, a good thing because at the end of the day we were all subject to scrutiny on the show by the program makers, by our colleagues and ultimately by the television audience … and there were massive levels of scrutiny throughout the entire process and I think that law enforcement could, if they wanted to listen to us, learn something from that because scrutiny is a good thing. This was something that grew out of my experience on the show. That level of scrutiny. It was good (Bleksley, 2016).

State intelligence actors are trained to keep secrets, hide their identities and only share information with those who need to know, and this culture of secrecy can lead to a natural suspicion of scrutiny and transparency. This resistance to 'opening up' can be interpreted by outsiders as evidence that the agencies have something to hide, but may largely be driven by an instilled distrust of scrutiny. Whilst it is easy

to criticise the lack of transparency associated with the work of intelligence agencies, achieving change will require more than new legislation, such as the increased powers of scrutiny that were included in the new Investigatory Powers Act. Those working in this industry are naturally resistant to oversight because they are trained to work in secret and this resistance can impede efforts to deliver greater scrutiny of their work. But the examples from Hunted demonstrate that when state intelligence actors become accustomed to oversight, they may begin to change their attitudes towards it, acknowledge its benefits and even embrace it.

7.3 CONCLUSION

Chapter 6 considers a variety of efforts to overcome the CSD and why they have failed. It then introduces several key principles that can be used to help overcome this difficult issue. This chapter has explored three of these principles in more detail, through the lens of the television show Hunted. This has revealed both the depth of the challenges faced in overcoming the CSD and the potential areas where improvement can be achieved. Achieving security dilemma sensibility is difficult because of the distance between the state and the DRC and differing access to information, but by acknowledging this gap and taking steps to bridge it, both the state and the DRC can improve their own prospects by beginning to learn about, experience and feel the genuine fears of the other. Good interpersonal relationships are difficult to achieve between the DRC and the state because state intelligence actors will always be somewhat distanced from the public, but there are clear indications that opening up can help to rehumanise the intelligence agencies and the practices of surveillance. This can help lay the groundwork for the establishment of greater understanding and trust.

The secrecy of the intelligence agencies and the resultant lack of transparency is perhaps the most difficult element of the CSD to overcome because there appears to be an intractable conflict between the need for secrecy and need for transparency. But the two do not exist in a zero-sum game. As Chapter 6 discusses, moves towards transparency do not necessarily come at the cost of national security. And as this chapter demonstrates moves towards transparency may also need to begin by combatting the fear of transparency that some state intelligence actors may hold.

Simply demanding more transparency or legislating to guarantee transparency is not enough to solve the problem. Instead it is necessary to understand the culture

of secrecy at the heart of the intelligence community, how this creates resistance to transparency and how this can be overcome. Assigning malicious intent to this resistance may be understandable, but it is unhelpful and fails to appreciate the perspective of state intelligence actors who dedicate their lives to the protection of their countries.

8 CONCLUSIONS

Chapter 2 of this thesis introduced the actors involved in the securitisation of cyberspace and the establishment of the CSD and Chapter 3 examined how cyberspace has been securitised using language and metaphor. The consequences of this securitisation were explored in Chapter 4, which considered how competing securitisations have created a CSD between the state and the DRC. Chapter 5 discussed how to address the securitisation of cyberspace and Chapter 6 considered how to resolve the CSD. Chapter 7 then used the television show, Hunted, to focus on particular aspects of the CSD.

This chapter summarises the thesis and introduces a range of principles that can be applied in future attempts to solve the CSD. It then discusses potential work to complement and develop the work within this thesis.

8.1 SUMMARY

The following is a summary of the chapters within this thesis, their conclusions, and how they meet the research questions.

Q1: How do the British state and the DRC construct cyberspace threats?

Chapter 2 identifies several key actors involved in the securitisation of cyberspace, including the government, intelligence agencies, whistle-blowers, technical experts, academia, rights organisations and the technology industry. The chapter demonstrates how the securitisation of cyberspace is not achieved by a single actor but is achieved through the collective securitising acts of a range of different actors. Whistle-blowers such as Snowden achieve incredible reach and gain massive exposure, whilst academic experts bring credibility, and rights organisations provide the foundation for the digital rights campaign. On the state side, the government has huge reach but is widely untrusted, whilst the security and intelligence agencies provide credibility and expertise to the cause. The different actors also have different relationships with different audiences, which influences their ability to convince them of the existence of cyberspace threats. The DRC and technology companies, for example, are often united in opposition to state surveillance but have a more fractious relationship with regards to potential privacy abuses by the technology industry. The state has the best ability to influence the legislature and create new surveillance legislation, but if the DRC convince the

technology industry to oppose this legislation then they can design their technology to resist state attempts to access data.

Chapter 3 considers how this range of actors use language and metaphors to securitise cyberspace. It demonstrates how both the state and the DRC use hypersecuritisation and everyday security practices to construct cyberspace threats as extreme and directly applicable to the audience. It also shows how they both also use technification to construct the issues as technical, positioning themselves as the expert authority to speak and act on the issues. Each side also use military, home security, biological and darkness metaphors to help enhance the threats and generate emotional responses in the audience. This process is taken further by connecting cyberspace securitisations with other securitised issues, such as terrorism and totalitarianism.

Q2: How have competing threat constructions led to conflict between the DRC and the British state?

Chapter 4 builds on Chapters 2 and 3 and considers how competing securitisations by the state and the DRC have created a CSD. The CSD describes how both the state and the DRC fear the consequences of each other's actions but are unable to see that they are driven by fear. In response, each side takes countermeasures which provoke additional fear in the other and create a spiral of escalating rhetoric and decreasing security for all. Chapter 4 considers some of the characteristics of the CSD, including the pre-eminence of security-seeking behaviour and the likelihood that the state's desire for national security and the DRC's desire for digital rights are not incompatible. The chapter discusses means through which the CSD is intensified, including the difficulty in differentiating between defensive and offensive behaviour by the state and the DRC. For example, whilst GCHQ may have developed the ability to hack webcams to target terrorists, the same technology can also be used to target the public. The chapter also considers how the CSD is intensified by the perception that the defence/offence balance is weighted towards offence.

Q3: What strategies can be applied to help resolve this conflict?

Chapter 5 addresses the normative dilemma of how the security researcher should respond to the securitisation of cyberspace and the resultant CSD. It first considers different approaches to desecuritisation, including the Copenhagen Approach, the Discursive Ethical Approach and the Consequentialist Approach, but highlights

difficulties with each. The Copenhagen Approach suggests that desecuritisation is generally desirable, but not always, and provides no tools to help decide which is the case. The Discursive Ethical Approach addresses this problem by suggesting that acts of securitisation should be judged based upon whether their claims are true or not. Whilst appealing, this approach is also difficult, given the range of different opinions highlighted in Chapters 3 and 4 and the difficulty of deciding whether securitising claims are true. The Consequentialist Approach resolves this issue by focussing on the consequences of securitisation, rather than its processes, but this approach is difficult to apply to the CSD. For example, judging whether surveillance is proportional to the threat is extremely difficult. The chapter also considers methods of desecuritisation, including replacement, counter-securitisation, silencing, de-escalation and re-articulation, highlighting problems with each. The chapter concludes that desecuritisation alone is not the best approach to the CSD because of the way it is created through competing securitisations. Instead, a different approach is required.

Chapter 6 reviews the history of the 'Crypto Wars' and the CSD and assesses why attempts to resolve these have not been successful. It considers unilateral attempts to 'win' the 'Crypto Wars' through the DRC's use of encryption and the state's use of surveillance, but concludes that such attempts cannot be successful as they only address the fears of one side. The chapter also considers attempts at more collaborative approaches. Technical solutions, such as David Chaum's Privategrity had promise, but failed because they did not combine the technical aspect with a parallel effort to build trust and reduce enmity. Some attempts at peace talks have been more successful, although, due to historic enmity and mistrust, they have also proven of limited utility. Some attempts at reframing the debate are also promising but have not achieved widespread support. The chapter then discusses how to solve the CSD by utilising the experiences and literature related to resolutions of traditional security dilemmas.

Chapter 7 considers several factors that affect the ability of the Security Dilemma to be solved and applies these to the CSD, illustrating several of these with examples from the television show, Hunted. It considers issues such as trust, secrecy, and ideological fundamentalism and concludes that the CSD can be overcome if these issues are all addressed.

8.2 KEY RESEARCH CONTRIBUTIONS

Within the literature review several research gaps were identified, which this thesis sought to address. These include the lack of work on the securitisation of British cyberspace, the failure to address securitisation conducted by non-state actors such as the DRC, the lack of substantial work into the emergence of a security dilemma between the British state and the DRC, and a lack of detailed analysis of the actions and motivations of British state intelligence actors. This work had contributed towards a greater understanding of each of these areas.

8.2.1 Securitisation of cyberspace in the UK

Whilst there have been several studies into the securitisation of cyberspace, none have focused specifically on the UK, despite its prominent intelligence agencies and surveillance capabilities, its relation to the Snowden disclosures, and its world-leading investigatory powers legislation. This thesis contributes towards this research area by focussing specifically on the securitisation of British cyberspace. International events, such as the dispute between Apple and the FBI are addressed, due to their relevance to the UK, but primarily this thesis focuses on statements and official reports produced by the British government, interviews with staff at GCHQ and the ORG and observation of the British reality crime drama, Hunted. In doing so, this work exposes the mechanisms of cyberspace securitisation in the UK and sheds new light onto the dispute between the DRC and the British state.

8.2.2 Securitisation by non-state actors

There is a range of literature that considers the securitisation of cyberspace by states, but only Mariya Georgieva's work considers the influence of non-state, actors such as Edward Snowden. But to fully appreciate the dispute between the DRC and the state it is necessary to study the actions and intentions of not just the state but the DRC as well. This thesis considers the way in which the DRC securitises cyberspace in direct comparison to how the state securitises cyberspace. In doing so it helps to address this significant research gap and potentially opens an innovative new approach to studying conflict between state and non-state actors.

8.2.3 The Cyber Security Dilemma

The security dilemma is a useful tool to help understand the emergence of conflict and how to prevent it, but research into this framework has only infrequently been applied to cyberspace and only once, to the dispute between the British state and the DRC, in a short paper by Myriam Dunne Cavelty (Cavelty, 2014). But

understanding the interplay between the motivations and actions of the two sides is critical to understanding the conflict and how it can be overcome. This thesis addresses the parallels between the actions of the DRC and the British state, and how these can lead to a spiral of insecurity. This substantial application of the security dilemma to the dispute between the British state and the DRC contributes to a better understanding of the conflict and potentially opens new policy approaches which move beyond simple critiques of government policy towards ideas of community, mutual interest and common purpose.

8.2.4 Study of state intelligence actors

Whilst there is a substantial volume of research into government policy on surveillance and cyberspace, there is far less on the culture of intelligence agencies and the perspective of intelligence actors. This is likely driven by the secrecy of intelligence agencies and the necessity of 'insider status' to gain access to intelligence actors. But to understand what drives government policy decisions in this area it is necessary to understand the culture of those involved in decision making and the factors that influence them. By interviewing GCHQ staff and observing and interviewing former state intelligence actors on Channel 4's Hunted this thesis goes some way towards addressing this limitation. This study exposed both the opinions of intelligence actors and their reactions to new and novel situations. Whilst an ethnographic study of GCHQ could have added even more value, this work still helps to expose this under researched area and helps to show how the experiences of state intelligence actors influences the dispute between the British state and the DRC.

8.3 Some Key Principles

There is no single solution to the CSD and, as with any conflict, it will take time to overcome the enmity and distrust that has built up between a range of different actors. However, there are several principles that can help each side move away from conflict.

8.3.1 Accept that no-one can win the Crypto Wars

One of the most damaging elements of the surveillance and digital rights discourse is the framing of the issue as one of security vs privacy, national security vs digital rights or liberty vs totalitarianism. These framings and the use of the term, 'Crypto Wars', helps to construct a zero-sum game, which can only be won by one side. Some of the actions of both the state and the DRC play into this narrative, as each

has previously attempted to 'win' the Crypto Wars through technological, legal and discursive means. But as one side takes the advantage the other becomes more fearful and determined to counter the threat. There can be no lasting victory for national security or digital rights if the deliverance of one comes at the expense of the other. For progress to be made, each side must realise that co-operation is the only way to achieve their goals.

8.3.2 Understand and acknowledge the fears of the other

As Section 4.4 explains, the primary driver of the CSD is the inability of each side to understand the fears of the other. Intelligence agencies such as GCHQ find it difficult to understand why they are feared, whilst the DRC find it difficult to understand why enhanced digital rights might be problematic for GCHQ.

When the state articulates its fears that cyberspace will become anarchic because of encryption or the DRC articulates its fear that surveillance is leading to totalitarianism, the other side often tries to debunk and discredit these claims. Instead they should try to understand, acknowledge and address these fears in order to prevent a more harmful response.

8.3.3 Build trust

As Section 6.3 demonstrates, the establishment of trust and the development of interpersonal relationships will provide the foundation for any solutions to the CSD. Trust can be achieved on a range of different levels. Oversight agencies might provide functional trust in the intelligence agencies' ethics and lawfulness; meetings and conferences between the technology industry, state and DRC might help to establish interpersonal bonding; and the 'coming out' of intelligence agencies might help to rehumanise intelligence practitioners, enabling them to form a more trusting relationship with the public. Once trust is established, it will become easier to transcend the CSD and to establish common interests and goals. Threat constructions can then be rearticulated towards common enemies, such as criminals, terrorists and hostile states.

As well as learning to trust the other, each side must also learn to trust those on their own side who seek to reach out and engage with a different perspective. The example of David Chaum and Privategrity, discussed in Section 7.4, shows that this can be a difficult issue to address, but as Section 6.3.7 demonstrates, sometimes it takes a 'leap in the dark' to overcome issues of mistrust and enmity.

8.3.4 Reject absolutes

Section 3.2 introduces one of the most damaging elements of the securitisation of cyberspace; the construction of cyber issues as extreme, absolute and indivisible. Framing backdoors as inherently dangerous and encryption as inherently threatening, results in an environment where compromise becomes impossible. To facilitate a return to rational debate, it is in the interests of both sides to reject the most extreme securitising rhetoric from their own side and to focus on engaging with the other. In that way, issues can be discussed on a case by case basis, allowing for a more nuanced approach and a greater array of potential solutions.

8.3.5 Focus on the important issues

As Woods' report on encryption substitutes demonstrates (see Section 7.4), the British state and the DRC may be missing an opportunity to achieve their objectives by obsessing over the wrong issues (Woods, 2016). Woods demonstrates that whilst the DRC focus on encryption to deliver digital rights and the state focusses on accessing encrypted information to protect national security, both goals might be achievable through alternative means. The conflict over digital rights and national security is often distilled into a debate about encryption, but this renders the issue unsolvable as encryption is considered to be either secure or not. A more fruitful approach would be to start with the aims of the state and the DRC and work collectively to see how well they can be delivered.

8.3.6 Raise the quality of the debate

The quality of the debate around issues of encryption and surveillance is often poor and fails to generate increased understanding of the complex issues involved. Section 3.2 demonstrates how the debate is hyper-securitised, preventing issues from being discussed on anything more than a superficial level. Issues are also technified, with technology experts claiming the unique authority to interpret the ethics of new technology and the state claiming the unique authority to speak on issues of national security and intelligence.

The relationship between national security and digital rights is directly relevant to everyone but the issues are often inaccessible to the public. The IPA was keenly followed by the intelligence, security and human rights communities, but it was enacted with what the Guardian described as 'barely a whimper' and a distinct lack of interest from the public (The Guardian, 2016). It is in the interests of each side to raise the quality of the debate and attract a greater range of opinions and

expertise. Bringing outside perspectives, less tainted by enmity and less entrenched in ideology, will help to introduce new ideas and side-line the ideologically driven extremists on each side. As Moore and Rid exalt, when discussing encryption, the issue is 'too important to be left to true believers' (Moore & Rid, 2016, p. 30).

8.4 Contributions to Research Design and Practice

To obtain a deep understanding of the causes of the conflict between digital rights and national security, the result of that conflict, and the influence and perspectives of the key actors, it was necessary to utilise a combination of deep analysis of publicly accessible discourse, interviews with key actors, and ethnographic research. These different methodologies were combined to produce an understanding of not just the outcomes of the conflict, but the causes and the reasons why it is so difficult to resolve. Whilst ethnographic studies are an established research technique the approach used within this thesis was extremely novel. Instead of observing state intelligence actors in their usual environment, they were observed in an environment that was both familiar and unusual. By participating in Hunted they performed the role of surveillance officers whilst simultaneously being monitored and observed. As the security dilemma revolves around the difficulty of seeing the perspective of the other side, this environment provided a unique opportunity to study the same set of people experiencing surveillance from both ends of the CCTV camera. This human experiment provided unique insight into how fears of surveillance emerge and how they are mitigated.

To answer the research questions, it was also necessary to draw on research and utilise frameworks from a wide range of disciplines. These include intelligence studies, security studies, psychology, geopolitics and international relations, in additional to information security which provides the project with technical rigour. By utilising a wide empirical and theoretical base this mixed methods and interdisciplinary approach opens a new perspective on the conflict between the British state and the DRC and exposes novel approaches to addressing it. This type of approach can potentially be used more widely to address similar complex issues.

8.5 Further Work

To take the ideas presented in this thesis further, the following issues could be addressed.

8.5.1 International Cyber Security Dilemmas

This thesis establishes the formulation of the CSD in the UK, but different countries have taken different approaches and been influenced by different factors. It would be useful to compare the CSD in the UK with other countries. Does the CSD exist everywhere, how is it different and what impact has this had on national security and digital rights? What can the UK learn from experiences elsewhere and to what extent can these be replicated?

8.5.2 The role of technology companies in the Cyber Security Dilemma

Chapter 2 addresses some of the influence of technology companies on the CSD but this work could be taken further to address the following questions. What is the impact of the profit motive for technology companies such as Facebook and Google? How do the different strategies of companies such as Google (selling information) and Apple (selling hardware) affect their approach to and influence on the CSD? What role do technology companies have in exacerbating the CSD and how might they help resolve it?

8.5.3 Practical approaches to the Cyber Security Dilemma

This thesis establishes several broad principles which can help towards addressing the securitisation of cyberspace and the CSD, but further work is required to establish the technologies that will eventually be required to address the issues involved. Can technologies be created to both deliver national security and digital rights, and ease the fears of those who fear that each of these is under threat?

9 GLOSSARY

CSD ..... Cyber Security Dilemma

DRC..... Digital Rights Community

GCHQ..... Government Communications Headquarters

IPA ..... Investigatory Powers Act

JIC ..... Joint Intelligence Committee

NCSC..... National Cyber Security Centre

NSA..... National Security Agency

NSD..... New Security Dilemma

NSS ..... National Security Strategy

ORG ..... Open Rights Group

SDSR ..... Strategic Defence and Security Review

TSD ..... Traditional Security Dilemma

UK CSS ..... United Kingdom Cyber Security Strategy

APPENDIX 1: LIST OF INTERVIEWEES

GCHQ

David - Cyber Policy Adviser

Adrian - Head of Cyber Crime

Matt - Head of Communications and Campaign Planning

Emily - Head of News

Fiona - Public Communications and Campaign Planning

Open Rights Group

Jim Killock - Director

Javier Ruiz - Policy Director

Hunted

Peter Bleksley - Chief Hunter

Ben Owen - Deputy Chief

Aisha Ishaq - Intelligence Officer

Paul Vlissidis - Head of Cyber

Aaron Eccles - Production

10 BIBLIOGRAPHY

Intelligence and Security Committee of Parliament, 2015. *Privacy and Security: A modern and transparent legal framework,* s.l.: House of Commons.

ABC News, 2016. *Apple CEO Tim Cook Sits Down With David Muir (Extended Interview).* [Online]
Available at: http://abcnews.go.com/WNT/video/exclusive-apple-ceo-tim-cook-sits-david-muir-37174976
[Accessed 15 February 2018].

ABC News, 2016. *Apple CEO Tim Cook Stands Firm Against the FBI.* [Online]
Available at: http://abcnews.go.com/WNT/video/apple-ceo-tim-cook-stands-firm-fbi-37123364
[Accessed 15 February 2018].

ABC News, 2016. *Apple CEO Tim Cook Stands Firm Against the FBI.* [Online]
Available at: http://abcnews.go.com/WNT/video/apple-ceo-tim-cook-stands-firm-fbi-37123364
[Accessed 15 February 2018].

Abelson, H. et al., 1997. The Risks of Key Recovery, Key Escrow, and Trusted Third Party-Encryption. *World Wide Web Journal,* 2(3), pp. 241-257.

Abelson, H. et al., 2015. *Keys Under Doormats: mandating insecurity by requiring government access to all data and communications,* s.l.: Computer Science and Artificial Intelligence Laboratory - MIT.

Access Now, 2016. *Third Annual Heroes & Villains of Human Rights and Communications Surveillance.* [Online]
Available at: https://www.accessnow.org/third-annual-heroes-villains-human-rights-communications-surveillance/
[Accessed 15 February 2018].

Adler, E. & Barnett, M., 2009. Security Communities in theoretical perspective. In: E. Adler, ed. *Security Communities.* s.l.:Cambridge University Press, pp. 3-28.

Adrian, 2016. *Adrian Interview* [Interview] (1 April 2016).

Albert, R., Jeong, H. & Barabasi, A.-L., 2000. Error and attack tolerance of complex networks. *Nature,* 40(6), pp. 378-382.

Altheide, D. L., 2016. Terrorism and the Politics of Fear. *Cultural Studies ↔ Critical Methodologies,* 6(4), pp. 415-439.

Alves, A. d. M., 2015. Between the "Battlefield" Metaphor and Promises of Generativity: Contrasting Discourses on Cyberconflict. *Canadian Journal of Communications,* 40(3), pp. 389-406.

American Civil Liberties Union, 2013. *You May Have 'Nothing to Hide' But You Still Have Something to Fear.* [Online]
Available at: https://www.aclu.org/blog/you-may-have-nothing-hide-you-still-have-something-fear
[Accessed 15 February 2018].

Amnesty International, 2013. *UN response to surveillance must strike balance between privacy and security.* [Online] Available at: https://www.amnesty.org/en/latest/news/2013/10/un-response-surveillance-must-strike-balance-between-privacy-and-security/ [Accessed 15 February 2018].

Anderson, C., Lepper, M. & Ross, L., 1980. Perseverance of social theories: The role of explanation in the persistence of discredited information.. *Journal of Personality and Social Psychology,* 39(6), pp. 1037-1049.

Anderson, D., 2015. *A Question of Trust - Report of the Investigatory Powers Review,* s.l.: Crown.

Anderson, T. & Kanuka, H., 2003. *E-research Methods, Strategies and Issues.* s.l.:Allyn and Bacon.

Andrea, 2016. *Twitter.* [Online] Available at: https://twitter.com/puellavulnerata/status/684719616568999936 [Accessed 15 February 2018].

Andreessen, M., 2015. *Edward Snowden: Clinton's Call for a 'Manhattan-Like Project' Is Terrifying.* [Online] Available at: http://www.rollingstone.com/politics/news/edward-snowden-clintons-call-for-a-manhattan-like-project-is-terrifying-20151220 [Accessed 15 February 2018].

Anon., 2016. *Pioneer In Internet Anonymity Hands FBI A Huge Gift In Building Dangerous Backdoored Encryption System.* [Online] Available at: https://www.*TechDirt*.com/articles/20160106/09090233253/pioneer-internet-anonymity-hands-fbi-huge-gift-building-dangerous-backdoored-encryption-system.shtml [Accessed 15 February 2018].

Anon., 2016. *Social media giants 'failing' on extremism - MPs.* [Online] Available at: http://www.bbc.co.uk/news/uk-37180159 [Accessed 15 February 2018].

Anon., n.d. *Surveillance Self-Defense - End-to-end encryption.* [Online] Available at: https://ssd.eff.org/en/glossary/end-end-encryption [Accessed 15 February 2018].

Anonymous, 2013. *Anonymous Operation Last Resort.* [Online] Available at: https://www.youtube.com/watch?v=WaPni5O2YyI [Accessed 15 February 2018].

Anonymous, n.d. *Someone to watch over you.* [Online] Available at: http://www.stylist.co.uk/people/someone-to-watch-over-you [Accessed 15 February 2018].

Antispirituality.net, n.d. *The Cult of Cryptography.* [Online] Available at: http://antispirituality.net/cryptography [Accessed 15 February 2018].

Appelbaum, J., 2016. *Twitter.* [Online] Available at: https://twitter.com/ioerror/status/684763375260270592 [Accessed 15 February 2018].

Apple Inc, 2016. *A Message to Our Customers.* [Online] Available at: http://www.apple.com/customer-letter/

Apple Inc, n.d. *Apple Privacy Policy.* [Online] Available at: http://www.apple.com/uk/privacy/government-information-requests/ [Accessed 17 2 2016].

Apple, 2015. *Written Evidence - Draft Investigatory Powers Committee.* [Online] Available at: http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf [Accessed 15 February 2018].

Apple, 2017. *iOS Security.* [Online] Available at: https://www.apple.com/business/docs/iOS_Security_Guide.pdf [Accessed 15 February 2018].

Apple & Facebook, G. M. T. Y., 2016. *Written evidence submitted by Apple Inc, Facebook Inc, Google Inc, Microsoft Corp, Twitter Inc and Yahoo Inc (IPB 21).* [Online] Available at: https://publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB21.htm [Accessed 15 February 2018].

Apple, n.d. *Apple Privacy Policy.* [Online] Available at: http://www.apple.com/uk/privacy/government-information-requests/ [Accessed 15 February 2018].

Apple, n.d. *Apple Privacy Policy.* [Online] Available at: http://www.apple.com/uk/privacy/government-information-requests/ [Accessed 17 2 2016].

Apple, n.d. *Government Data Requests.* [Online] Available at: http://www.apple.com/uk/privacy/government-information-requests/ [Accessed 15 February 2018].

Aradau, C., 2004. Security and the democratic scene: desecuritization and emancipation. *Journal of International Relations and Development,* 7(4), pp. 388-413.

ArsTechnica, 2017. *To keep Tor hack source code secret, DOJ dismisses child porn case.* [Online] Available at: https://arstechnica.com/tech-policy/2017/03/doj-drops-case-against-child-porn-suspect-rather-than-disclose-fbi-hack/ [Accessed 15 February 2018].

Aspen Institute, 2016. *From Apple to ISIL: FBI Director on How Technology is Changing Security.* [Online]
Available at: https://www.aspeninstitute.org/blog-posts/from-apple-to-isil-fbi-director-on-how-technology-is-changing-security/
[Accessed 15 February 2018].

Assange, J., 2013. *Cyhperpunks: Freedom and the future of the Internet.* s.l.:OR Books.

Assange, J., 2014. *Wikileaks meets Surveillance Valley: An interview with Julian Assange.* [Online]
Available at: https://pando.com/2014/10/12/wikileaks-meets-surveillance-valley-an-interview-with-julian-assange/
[Accessed 15 February 2018].

Associated Press, USA Today, Vice Media, 2016. *Case No.16-cv-1850,* s.l.: United States District Court for the Distrit of Columbia.

Aviva, 2016. *UK: Cancer most feared disease in Britain - but more than 8 million British adults take no action to reduce their risk.* [Online]
Available at: https://www.aviva.com/newsroom/news-releases/2016/01/uk-cancer-most-feared-disease-in-britain-but-more-than-8-million-british-adults-take-no-action-to-reduce-their-risk-17581/
[Accessed 15 February 2018].

Bakir, V., 2015. "Veillant Panoptic Assemblage": Mutual Watching and Resistance to Mass Surveillance after Snowden. *Media and Communication,* 3(3), pp. 12-25.

Baliga, S. & Sjostrom, T., 2004. Arms Races and Negotiations. *Review of Economic Studies,* Volume 71, pp. 351-369.

Balkan, A., 2015. *So Long, and Thanks for All the Fish.* [Online]
Available at: https://ar.al/notes/so-long-and-thanks-for-all-the-fish/
[Accessed 15 February 2018].

Balzacq, T., 2005. The Three Face of Securitization. *European Journal of International Relations,* 11(2), pp. 171-201.

Balzacq, T., 2005. The Three Faces of Securitisation: Political Agency, Audience and Context. *European Jounral of International Relations,* 11(2), pp. 171-201.

Balzacq, T., 2011. *Securitisaion Theory: How Security Problems Emerge and Dissolve.* s.l.:Routledge.

Balzacq, T., 2011. *Securitisation Theory: How Security Problems Emerge and Dissolve.* Oxon: Routledge.

Barlow, J. P., 1996. *A Declaration of the Independence of Cyberspace.* [Online]
Available at: https://www.eff.org/cyberspace-independence
[Accessed 15 February 2018].

Barnes, S., 2006. A privacy paradox: Social networking in the United States. *First Monday,* 11(9), pp. Volume 11, Number 9.

Barry Buzan, O. W. J. d. W., 1998. *Security: A New Framework for Analysis.* London: Lynne Rienner Publishers.

Bartlett, J., 2015. *The Dark Net.* London: Random House.

Bartlett, J., 2015. *The online surveillance debate is really about whether you trust governments or not.* [Online]
Available at: http://www.telegraph.co.uk/technology/internet-security/11979682/The-online-surveillance-debate-is-really-about-whether-you-trust-governments-or-not.html
[Accessed 15 February 2018].

Bartlett, J., 2015. *Twitter.* [Online]
Available at: https://twitter.com/JamieJBartlett/status/663984482735796224
[Accessed 15 February 2018].

BBC News, 2000. *Y2K: Overhyped and oversold?.* [Online]
Available at: http://news.bbc.co.uk/1/hi/talking_point/586938.stm
[Accessed 15 February 2018].

BBC News, 2003. *Ex-GCHQ officer 'preventing war'.* [Online]
Available at: http://news.bbc.co.uk/1/hi/uk/3243266.stm
[Accessed 15 February 2018].

BBC News, 2006. *UK general warns of Afghan threat.* [Online]
Available at: http://news.bbc.co.uk/1/hi/uk_politics/4779321.stm
[Accessed 15 February 2018].

BBC News, 2014. *Facebook emotion experiment sparks criticism.* [Online]
Available at: http://www.bbc.co.uk/news/technology-28051930
[Accessed 15 February 2018].

BBC News, 2014. *Facebook hosted Lee Rigby death chat ahead of soldier's murder.* [Online]
Available at: http://www.bbc.co.uk/news/technology-30199131
[Accessed 15 February 2018].

BBC News, 2015. *Edward Snowden interview: 'Smartphones can be taken over'.* [Online]
Available at: http://www.bbc.co.uk/news/uk-34444233
[Accessed 15 February 2018].

BBC News, 2017. *NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history.* [Online]
Available at: http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/
[Accessed 15 February 2018].

Belfast Telegraph, 2014. *Snooping tools GCHQ could use to hack your phone's microphone, camera and keypad.* [Online]
Available at: http://www.belfasttelegraph.co.uk/technology/snooping-tools-gchq-could-use-to-hack-your-phones-microphone-camera-and-keypad-nosey-smurf-gumfish-and-foggybottom-30272505.html
[Accessed 15 February 2018].

Benjamins, J., 2013. The Good is Light and Bad is Dark Metaphor in Feature Films. *Metaphor and the Social World,* 3(2), pp. 160-179.

Berkman Center, 2016. *Don't Panic. Making Progress on the 'Going Dark' Debate,* s.l.: February.

Bernal, P., 2014. *Open letter from UK legal academic experts re DRIP.* [Online] Available at: https://paulbernal.wordpress.com/2014/07/15/open-letter-from-uk-legal-academic-experts-re-drip/
[Accessed 15 February 2018].

Berners-Lee, T., 2012. *Tim Berners-Lee urges government to stop the snooping bill.* [Online]
Available at: https://www.theguardian.com/technology/2012/apr/17/tim-berners-lee-monitoring-internet
[Accessed 15 February 2018].

Berners-Lee, T., 2012. *Tim Berners-Lee urges government to stop the snooping bill.* [Online]
Available at: https://www.theguardian.com/technology/2012/apr/17/tim-berners-lee-monitoring-internet
[Accessed 15 February 2018].

Berners-Lee, T., 2012. *Tim Berners-Lee urges government to stop the snooping bill.* [Online]
Available at: https://www.theguardian.com/technology/2012/apr/17/tim-berners-lee-monitoring-internet
[Accessed 15 February 2018].

Betz, D. J. & Stevens, T., 2013. Analogical reasoning and cyber security. *Security Dialogue,* 44(2), pp. 147-164.

Bigo, D. et al., 2014. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology,* 8(2), pp. 121-144.

Binney, W., 2016. *William Binney: NSA Surveillance Takes a Page From Nazi Germany.* [Online]
Available at: https://sputniknews.com/us/201605311040567328-loud-clear-binney-nsa/
[Accessed 15 February 2018].

Birnhack, M. D. & Elkin-Koren, N., 2003. The Invisible Handshake: The Reemergence of the State in the Digital Environment. *Virginia Journal of Law and Technology,* Volume 6, pp. 1-57.

Blakeley, R. & Raphael, S., 2016. British torture in the 'war on terror'. *European journal of International Relations,* 23(2), pp. 243-266.

Blaze, M., 1994. *Protocol Failure in the Escrowed Encryption Standard.* Virginia, ACM Conference on Computer Communications Security.

Bleksley, P., 2016. *Peter Interview* [Interview] (4 April 2016).

Blog, S., n.d. *Home.* [Online]
Available at: http://spyblog.org.uk/
[Accessed 15 February 2018].

Boeke, S., 2017. Reframing 'Mass Surveillance'. In: M. Conway, et al. eds. *Terrorists Use of the Internet.* s.l.:IOS Press Books, pp. 307-318.

Booth, K. & Wheeler, N. J., 2008. *The Security Dilemma: Fear, Cooperation and Trust in International Politics.* s.l.:Palgrave Macmillan.

Bossong, R., 2008. *The EU's Mature Counterterrorism policy - A Critical History and Functional Assessment,* s.l.: LSE.

Boswell, C., 2007. *The Securitisation of Migration: A Risky Strategy for European States,* s.l.: Danish Institue For International Studies.

Botero, G., 2017. *The Reason of State.* s.l.:Cambridge University Press.

Boulding, K., 1959. National Images and International Systems. *The Journal of Conflict Resolution,* 3(2), pp. 120-131.

Bowcott, O., 2015. *GCHQ accused of 'persistent' illegal hacking at security tribunal.* [Online]
Available at: https://www.theguardian.com/uk-news/2015/dec/01/gchq-accused-of-persistent-illegal-hacking-at-security-tribunal
[Accessed 15 February 2018].

Bowcott, O., 2015. *GCHQ accused of 'persistent' illegal hacking at security tribunal.* [Online]
Available at: https://www.theguardian.com/uk-news/2015/dec/01/gchq-accused-of-persistent-illegal-hacking-at-security-tribunal
[Accessed 15 February 2018].

Braithwaite, A., 2013. The logic of public-fear in terrorism and counter-terrorism. *Journal o fpolice and criminal psychology,* 28(2), pp. 95-101.

Branum, J. & Charteris-Black, J., 2015. The Edward Snowden affair: A corpus study of the British press. *Discourse and Communication,* 9(2), pp. 1-22.

Britton, W. A., 2005. *Beyond Bond: Spies in Fiction and Film.* s.l.:Praeger Publishers.

Bruno, Z., 2014. *The PRISM Program Panopticon: Foucault's Insights in the Era of Snowden,* s.l.: s.n.

Bruno, Z., 2014. *The PRISM Program Panopticon: Foucault's Insights in the Era of Snowden,* s.l.: Occidental College.

Buchanan, B., 2016. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations.* London: C. Hurst and Co.

Bureau of Arms Control, Verification and Compliance, 1979. *Treaty Between The United States of America and The Union of Soviet Socialist Republics on the Limitation of Strategic Offensive Arms (SALT II),* s.l.: Bureau of Arms Control, Verification and Compliance.

Busan, B., 2004. *American Exceptionalism, Unipolarity and September 11: Understanding the Behaviour of the Sole Superpower,* Montreal: ISA Conference.

Busan, B., Waever, O. & Wilde, J. d., 1998. *Security: A New Framework for Analysis.* s.l.:Lynne Rienner Publishers Inc.

Bush, G., 2002. *Full text of Bush speech on Iraq.* [Online] Available at: http://news.bbc.co.uk/1/hi/world/americas/2309049.stm [Accessed 15 February 2018].

Butterfield, H., 1951. *History and Human Relations.* 3 ed. s.l.:Collins.

Butterfield, H., 1951. *History and Human Relations.* s.l.:Macmillan.

Buzan, B., Waever, O. & Wilde, J. d., 1998. *Security: A New Framework For Analysis.* s.l.:Lynne Rienner Publishers.

Cable, J., 2015. *An overview of public opinion polls since the Edward Snowden revelations in June 2013,* Cardiff: Cardiff University.

Cameron, D., 2010. *Olympic Park to offer high-tech business development..* [Online] Available at: https://www.gov.uk/government/news/prime-minister-announces-east-london-tech-city-to-rival-silicon-valley [Accessed 15 February 2018].

Cameron, D., 2013. *David Cameron: Guardian Snowden leaks 'damaged national security'.* [Online] Available at: http://www.telegraph.co.uk/news/uknews/defence/10383089/David-Cameron-Guardian-Snowden-leaks-damaged-national-security.html [Accessed 15 February 2018].

Cameron, D., 2014. *UK PM Cameron says Internet must not 'be an ungoverned space'.* [Online] Available at: http://www.theregister.co.uk/2014/11/14/uk_pm_cameron_says_internet_must_not_be_an_ungoverned_space/ [Accessed 15 February 2018].

Cameron, D., 2015. *David Cameron Wants To Ban Encryption.* [Online] Available at: http://uk.businessinsider.com/david-cameron-encryption-apple-pgp-2015-1?r=US [Accessed 15 February 2018].

Cameron, D., 2015. *Facebook and Twitter have 'social responsibility' to help fight terrorism, says David Cameron.* [Online] Available at: https://www.theguardian.com/world/2015/jan/16/cameron-interrupt-terrorists-cybersecurity-cyberattack-threat [Accessed 15 February 2018].

Campaign for Accountability, 2016. *Ethics Letter.* [Online] Available at: http://campaignforaccountability.org/wp-content/uploads/2016/10/WH-Ethics-Letter-10-4-16.pdf [Accessed 15 February 2018].

Campbell, D., 2015. *Spooks admit it in private: Snowden has made them rethink their methods.* [Online] Available at: https://www.theguardian.com/commentisfree/2015/jun/02/spooks-snowden-transparency-mi6-gchq-cia [Accessed 15 February 2018].

Campbell, D., 2015. *Talking to GCHQ (interception not required) ....* [Online] Available at: http://www.duncancampbell.org/content/talking-gchq-interception-not-required
[Accessed 15 February 2018].

Campbell, D. & Goodwin, B., 2016. *MPs' private emails are routinely accessed by GCHQ.* [Online] Available at: http://www.computerweekly.com/news/450297574/MPs-private-emails-are-routinely-accessed-by-GCHQ
[Accessed 15 February 2018].

Campbell, D. & Honigsbaum, M., 1999. *Britain and US spy on world.* [Online] Available at: https://www.theguardian.com/uk/1999/may/23/duncancampbell.markhonigsbaum
[Accessed 15 February 2018].

Cannataci, J., 2015. *Digital surveillance 'worse than Orwell', says new UN privacy chief.* [Online] Available at: https://www.theguardian.com/world/2015/aug/24/we-need-geneva-convention-for-the-internet-says-new-un-privacy-chief
[Accessed 15 February 2018].

Casey, T., 2017. *Public Interest Defence: If the government has nothing to hide then there's nothing to fear.* [Online] Available at: http://www.pcaw.org.uk/latest/blog/public-interest-defence-if-the-government-has-nothing-to-hide-then-theres-nothing-to-fear
[Accessed 15 February 2018].

Castano, E., Sacchi, S. & Gries, P. H., 2003. he Perception of the Other in International Relations: Evidence for the Polarizing Effect of Entitativity. *Political Psychology,* 24(3), pp. 449-468.

Caster, C. N., 2016. *Edward Snowden, Hero or Traitor? An Analysis of News Media Framing,* California: the Faculty of the Communication Studies Department, California Polytechnic State University.

Cavelty, M. D., 2007. Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics,* 4(1), pp. 19-36.

Cavelty, M. D., 2013. From Cyber Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review,* 15(1), pp. 105-122.

Cavelty, M. D., 2014. Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics,* 20(3), pp. 701-715.

Cavelty, M. D., 2014. Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics,* 20(3), pp. 701-715.

Cavelty, M. D., 2014. Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics,* 20(3), pp. 701-715.

Cerny, P., 2000. The New Security Dilemma: divisibility, defection and disorder in the global era. *Review of International Studies,* 26(4), pp. 623-646.

Cerny, P., 2005. Terrorism and the New Security Dilemma. *Naval War College Review,* 58(1), pp. 11-33.

Cesari, J., 2009. *The Securitisation of Islam in Europe,* s.l.: Centre for European Policy Studies.

Chakrabarti, S., 2015. *Let me be clear – Edward Snowden is a hero.* [Online] Available at: https://www.theguardian.com/commentisfree/2015/jun/14/edward-snowden-hero-government-scare-tactics
[Accessed 15 February 2018].

Channel 4, 2015. *Channel 4 alerts Londoners to surveillance power of the state.* [Online]
Available at: http://www.channel4.com/info/press/news/channel-4-alerts-londoners-to-surveillance-power-of-the-state
[Accessed 15 February 2018].

Charney, D. L. & Irvin, J. A., 2014. *A Guide to the Psychology of Espionage,* s.l.: Association of Former Intelligence Officers.

Charrett, C., 2009. *A Critical Application of Securitization Theory: Overcoming the Normative Dilemma of Writing Security,* s.l.: Institut Català Internacional per la Pau.

Chaum, D., 1981. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM,* 2(24), pp. 84-88.

Chaum, D., 2016. *The Father of Online Anonymity has a plan to end the Crypto Wars.* [Online]
Available at: https://www.wired.com/2016/01/david-chaum-father-of-online-anonymity-plan-to-end-the-crypto-wars/
[Accessed 15 February 2018].

Chaum, D., 2016. *What Everybody Misunderstands About Privacy Pioneer David Chaum's Controversial Crypto Plan.* [Online]
Available at: http://fortune.com/2016/01/14/encryption-wars-crypto-david-chaum/
[Accessed 15 February 2018].

Chaum, D. et al., 2016. cMix: Anonymization by High-Performance Scalable Mixing. *IACR Cryptology ePrint Archive.*

Chilcott, J., 2016. *The Report of the Iraq Inquiry,* s.l.: The Iraq Inquiry.

Ciobotea, O., 2016. *Why the Apple-FBI battle made people realize the importance of privacy faster than Snowden.* [Online]
Available at: https://venturebeat.com/2016/04/29/why-the-apple-fbi-battle-made-people-realize-the-importance-of-privacy-faster-than-snowden/
[Accessed 15 February 2018].

Citizen Lab, 2018. *About the Ciitzen Lab.* [Online]
Available at: https://citizenlab.ca/about/
[Accessed 15 February 2018].

Citizen Lab, n.d. *About the Citizen Lab.* [Online]
Available at: https://citizenlab.org/about/
[Accessed 15 February 2018].

City AM, 2016. *Britain wants to woo US tech entrepreneurs to expand their businesses in London and the UK with SXSW campaign launch by mayor's office and UKTI.* [Online]
Available at: http://www.cityam.com/236392/britain-wants-to-woo-us-tech-entrepreneurs-to-expand-their-businesses-in-london-and-the-uk-with-sxsw-campaign-launch-by-mayors-office-and-ukti
[Accessed 15 February 2018].

City AM, 2017. *UK woos foreign tech investors to boost post-Brexit digital economy.* [Online]
Available at: http://www.cityam.com/272167/uk-woos-foreign-tech-investors-boost-post-brexit-digital
[Accessed 15 February 2018].

Clapper, J., 2016. *SPY CHIEF COMPLAINS THAT EDWARD SNOWDEN SPED UP SPREAD OF ENCRYPTION BY 7 YEARS.* [Online]
Available at: https://theintercept.com/2016/04/25/spy-chief-complains-that-edward-snowden-sped-up-spread-of-encryption-by-7-years/
[Accessed 15 February 2018].

Clarke, R. A., 2010. *Cyber War: The next threat to National Security and what to do about it.* s.l.:Harper Collins.

Clarke, R. A., 2012. *Cyber War: The next threat to National Security and what to do about it.* s.l.:Harper Collins.

Clegg, N., 2012. *Draft Communications Data Bill cannot proceed - Nick Clegg.* [Online]
Available at: http://www.bbc.co.uk/news/uk-politics-20668953
[Accessed 15 February 2018].

Clegg, N., 2013. *Edward Snowden leaks damaging, says Nick Clegg.* [Online]
Available at: http://www.bbc.co.uk/news/uk-24476047
[Accessed 15 February 2018].

Clegg, N., 2014. *Security and privacy in the internet age.* [Online]
Available at: https://www.gov.uk/government/speeches/security-and-privacy-in-the-internet-age
[Accessed 15 February 2018].

Clement, M., n.d. *Television, Ethnographic Research and Reality.* [Online]
Available at: https://mc560.wordpress.com/2015/08/24/ethnographic-research-and-reality-television/
[Accessed 11 February 2018].

Clinton, H., 2015. *Democratic debate transcript: Clinton, Sanders, O'Malley in New Hampshire.* [Online]
Available at: http://www.cbsnews.com/news/democratic-debate-transcript-clinton-sanders-omalley-in-new-hampshire/
[Accessed 15 February 2018].

Clinton, H., 2016. *Hillary Clinton's Initiative on Technology & Innovation.* [Online] Available at: https://web.archive.org/web/20161205091208/https://www.hillaryclinton.com/briefing/factsheets/2016/06/27/hillary-clintons-initiative-on-technology-innovation/
[Accessed 15 February 2018].

Colaresi, M. P., 2014. *Democracy Declassified: The Secrecy Dilemma in National Security.* s.l.:Oxford University Press.

Collins, L. et al., 2001. A National Survey of Stress Reactions after the September 11, 2001, Terrorist Attacks. *The New England Journal of Medicine,* 345(20), pp. 1507-1512.

Comey, J., 2014. *Going Dark Are technology, privacy andpublic safety on a collision course?.* [Online]
Available at: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course
[Accessed 17 February 2016].

Comey, J., 2014. *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?.* [Online]
Available at: Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?
[Accessed 15 February 2018].

Comey, J., 2014. *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?.* [Online]
Available at: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course
[Accessed 15 February 2018].

Comey, J., 2016. *FBI Director Comments on San Bernardino Matter.* [Online]
Available at: https://www.fbi.gov/news/pressrel/press-releases/fbi-director-comments-on-san-bernardino-matter
[Accessed 15 February 2018].

Comey, J., 2016. *FBI director looks to 2017 for 'adult' encryption debate.* [Online]
Available at: http://thehill.com/policy/cybersecurity/293786-comey-targets-2017-for-less-emotional-adult-conversation-on-encryption
[Accessed 15 February 2018].

Cook, T., 2015. *Apple boss: We have a human right to privacy.* [Online]
Available at: http://www.telegraph.co.uk/technology/apple/11441265/Terrorists-should-be-eliminated-says-Apples-Tim-Cook.html
[Accessed 15 February 2018].

Cook, T., 2015. *Apple's Tim Cook declares the end of the PC.* [Online]
Available at: http://www.telegraph.co.uk/technology/2016/01/21/apples-tim-cook-declares-the-end-of-the-pc-and-hints-at-new-medi/
[Accessed 15 February 2018].

Cook, T., 2015. *Tim Cook talks Edward Snowden, Apple Car and more in new interview.* [Online]

Available at: http://bgr.com/2015/03/02/tim-cook-interview-snowden/ [Accessed 15 February 2018].

Cook, T., 2016. *Apple CEO Time Cook on his fight with the FBI and why he won't back down.* [Online] Available at: http://time.com/magazine/us/4262476/march-28th-2016-vol-187-no-11-u-s/ [Accessed 15 February 2018].

Cook, T., 2016. *Customer Letter.* [Online] Available at: http://www.apple.com/customer-letter/ [Accessed 15 February 2018].

Cook, T., 2016. *Here's the Full Transcript of TIME's Interview With Apple CEO Tim Cook.* [Online] Available at: http://time.com/4261796/tim-cook-transcript/ [Accessed 15 February 2018].

Cook, T., 2016. *Tim Cook talks encryption in Utah.* [Online] Available at: https://www.youtube.com/watch?v=1yKcS2C24sM [Accessed 15 February 2018].

Co, R., 2014. *The New World Order: The Evil Exposed!.* s.l.:Rafal Col Publishing.

Cotton, T., 2016. *Cotton Statement on Apple's Refusal to Obey a Judge's Order to Assist the FBI in a Terrorism Investigation.* [Online] Available at: https://www.cotton.senate.gov/?p=press_release&id=319 [Accessed 15 February 2018].

Cotton, T., 2016. *Cotton Statement on Apple's Refusal to Obey a Judge's Order to Assist the FBI in a Terrorism Investigation.* [Online] Available at: https://www.cotton.senate.gov/?p=press_release&id=319 [Accessed 15 February 2018].

Counsel for Amici Curiae Digital Rights Ireland Limited, Liberty, and the Open Rights Group, 2014. *Brief of Amici Curiae Digital Rights Ireland limited, Liberty and the Open Rights Group in support of appelant Microsoft Corporation.* [Online] Available at: https://www.scribd.com/document/250254939/Amicus-Brief-Digital-Rights-Ireland-Liberty-and-ORG-in-Microsoft-v-USA [Accessed 15 February 2018].

Coustick-Deal, R., 2015. *Responding to "Nothing to hide, Nothing to fear".* [Online] Available at: https://www.openrightsgroup.org/blog/2015/responding-to-nothing-to-hide-nothing-to-fear [Accessed 15 February 2018].

Crossman, G., 2008. Nothing to hide, nothing to fear?. *International Review of Law, Computers and Technology,* 22(1-2), pp. 115-118.

Cryptome, 2000. *Microsoft offer to resolve "questions about NSA_key", then put up a brick wall..* [Online] Available at: https://cryptome.org/nsakey-ms-dc.htm [Accessed 15 February 2018].

Cult of Mac, 2016. *AT&T CEO thinks Apple should give up on protecting encryption.* [Online]
Available at: https://www.cultofmac.com/408298/att-ceo-thinks-apple-should-give-up-on-protecting-encryption/
[Accessed 15 February 2018].

Cypherspace.org, n.d. *export-a-crypto-system sig.* [Online]
Available at: http://www.cypherspace.org/adam/rsa/
[Accessed 15 February 2018].

Dalek, J., Senft, A., Crete-Nishihata, M. & Deibert, R., 2013. *O Pakistan We Stand on Guard for Three: An Analysis of Canada-based Netsweeper's Role in Pakistan's Censorship Regime,* s.l.: Citizen Lab.

David, 2016. *David Interview* [Interview] (15 April 2016).

Davis, D., 2013. *David Davis expresses strong support for the role played by Edward Snowden.* [Online]
Available at: http://www.daviddavismp.com/davis-davis-expresses-strong-support-for-the-role-played-by-edward-snowden/
[Accessed 15 February 2018].

Davis, D., 2015. *Surveillance and civil liberties: Interview with David Davis MP.* [Online]
Available at: http://blogs.lse.ac.uk/mediapolicyproject/2015/11/05/surveillance-and-civil-liberties-interview-with-david-davis-mp/
[Accessed 15 February 2018].

Dawson, L. S., 2016. *Twitter.* [Online]
Available at: https://twitter.com/linton_s_dawson/status/684803496072314881
[Accessed 15 February 2018].

Deibert, R., 2008. *Global Civil Society and the Securitisation of the Internet,* s.l.: MIT Press.

Deibert, R., 2012. The Growing Dark Side of Cyberspace. *Penn State Journal of Law and International Affairs,* 1(2), p. 260.

Deibert, R., 2012. The Growing Dark Side of Cyberspace. *Penn State Journal of Law and International Affairs,* 1(2), p. 260.

Deibert, R., 2012. The Growing Dark Side of Cyberspace. *Penn State Journal of Law and International Affairs,* 1(2), p. 260.

Deibert, R. & Crete-Nishihata, M., 2012. Global Governance and the Spread of Cyberspace Controls. *Global Governance,* 18(3), pp. 339-361.

Deibert, R. & Rohozinski, R., 2008. Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet. In: *Access Denied: The Practice and Policy of Global Internet Filtering.* s.l.:MIT Press, pp. 123-149.

Deibert, R. & Rohozinski, R., 2010. Liberation vs. Control: The Future of Cyberspace. *Journal of Democracy,* 21(4), pp. 43-57.

Deligiaouri, A. & Popovic, M., 2010. Reality TV and Reality of TV: How much Reality is There in Reality TV shows?. In: S. V. Bauwel & N. Carpenter, eds. *Trans-Reality*

Television: The Transgression of Reality, Genre, Politics and Audience. s.l.:Lexington Books, pp. 65-86.

DeNardis, L., 2010. *The Emerging Field of Internet Governance.* s.l.:Yale Information Society Project; Yale Law School.

DeNardis, L. & Hackl, A., October 2015. Internet governance by social media platforms. *Telecommunications Policy,* 39(9), pp. 761-770.

Derakhshan, H., 2016. *Mark Zuckerberg is a hypocrite - Facebook has destroyed the open web.* [Online]
Available at: http://www.ibtimes.co.uk/mark-zuckerberg-hypocrite-facebook-has-destroyed-open-web-1559298
[Accessed 18 February 2018].

Deutsch, K. W., 1957. *Political Community and the North American Area.* s.l.:Princetno University Press.

Dhami, M., 2011. *Behavioural Science Support for JTRIG's (Joint Threat Research and Intelligence Group's) Effects and Online HUMINT Operations,* s.l.: GCHQ Report disclosed by Edward Snowden.

Diffie, W., 1993. *The Impact of a Secret Cryptographic Standard on Encryption, Privacy, Law Enforcement and Technology.* [Online]
Available at: https://epic.org/crypto/clipper/diffie_testimony.html
[Accessed 15 February 2018].

Diffie, W. & Hellman, M. E., 1976. New Directions in Cryptography. *IEEE Transactions On Information Theory,* 22(6), pp. 644-654.

Dilger, D., 2016. *Hillary Clinton's tech platform backs Apple positions on encryption, privacy, innovation, patents, education.* [Online]
Available at: http://appleinsider.com/articles/16/06/29/hillary-clintons-tech-platform-backs-apple-inc-positions-on-encryption-privacy-innovation
[Accessed 15 February 2018].

Ditchley Park, 2015. *Intelligence, security and privacy.* [Online]
Available at: http://www.ditchley.co.uk/conferences/past-programme/2010-2019/2015/intelligence
[Accessed 15 February 2018].

Dixon-Thayer, D., 2016. *Mozilla Exec: There's No Such Thing as a Safe Backdoor.* [Online]
Available at: http://time.com/4263121/apple-fbi-backdoor/
[Accessed 15 February 2018].

Dixon-Thayer, D., 2016. *Mozilla Exec: There's No Such Thing as a Safe Backdoor.* [Online]
Available at: http://time.com/4263121/apple-fbi-backdoor/
[Accessed 15 February 2018].

Doctorow, C., 2015. *Every issue is a digital issue.* [Online]
Available at: https://www.openrightsgroup.org/blog/2015/every-issue-is-a-digital-issue
[Accessed 15 February 2018].

Dodge, M. & Kitchen, R., 2001. *Mapping Cyberspace.* s.l.:Routledge.

Donovan, K. M. & IV, C. F. K., 2015. The Role Of Entertainment Media In Perceptions Of Police Use Of Force. *Criminal Justice and Behaviour,* 42(12), pp. 1261-1281.

Don't Spy On Us, 2016. *Parliament passes most extreme surveillance law in UK history.* [Online]
Available at: https://www.dontspyonus.org.uk/blog/2016/11/17/parliament-passes-most-extreme-surveillance-law-in-uk-history/
[Accessed 15 February 2018].

Drake, T., 2016. *Privacy experts fear Donald Trump running global surveillance network.* [Online]
Available at: https://www.theguardian.com/world/2016/nov/11/trump-surveillance-network-nsa-privacy
[Accessed 15 February 2018].

Dreifach, K., 2015. *Apple INC's Reponse to Court's October 9, 2015 Memorandum and Order.* [Online]
Available at: https://www.scribd.com/document/286689775/Apple-Brief-10192015
[Accessed 15 February 2018].

DuPont, Q., 2015. *Opinion: It's time to rethink polarizing encryption debate.* [Online]
Available at: https://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1202/Opinion-It-s-time-to-rethink-polarizing-encryption-debate
[Accessed 15 February 2018].

Eccles, A., 2016. *Hunted Interview* [Interview] 2016.

Edelman, 2017. *Edelman Trust Barometer,* s.l.: Edelman.

Edelman, 2017. *Edelman Trust Barometer,* s.l.: Edelman.

Electronic Frontier Foundation, 2013. *Ten Steps You Can Take Right Now Against Internet Surveillance.* [Online]
Available at: https://www.eff.org/deeplinks/2013/10/ten-steps-against-surveillance
[Accessed 15 February 2018].

Electronic Frontier Foundation, 2014. *Academics and Researchers Against Mass Surveillance.* [Online]
Available at: https://www.eff.org/deeplinks/2014/02/academics-and-researchers-against-mass-surveillance
[Accessed 15 February 2018].

Electronic Frontier Foundation, 2014. *Academics and Researchers Against Mass Surveillance.* [Online]
Available at: https://www.eff.org/deeplinks/2014/02/academics-and-researchers-against-mass-surveillance
[Accessed 15 February 2018].

Electronic Frontier Foundation, 2014. *The 90s and Now: FBI and its Inability to Cope with Encryption.* [Online]
Available at: https://www.eff.org/deeplinks/2014/10/90s-and-now-fbi-and-its-

inability-cope-encryption
[Accessed 15 February 2018].

Electronic Frontier Foundation, 2015. *Who Has Your Back - Protecting your data from Government Requests.* [Online] Available at: https://www.eff.org/who-has-your-back-government-data-requests-2015
[Accessed 15 February 2018].

Electronic Frontier Foundation, 2017. *Who Has Your Back,* s.l.: Electronic Frontier Foundation.

Electronic Frontier Foundation, n.d. *Counter-Surveillance Success Stories.* [Online] Available at: https://www.eff.org/csss
[Accessed 15 February 2018].

Electronic Frontier Foundation, n.d. *Full disk encrption.* [Online] Available at: https://ssd.eff.org/en/glossary/full-disk-encryption
[Accessed 15 February 2018].

Electronic Frontier Foundation, n.d. *Full disk encrption.* [Online] Available at: https://ssd.eff.org/en/glossary/full-disk-encryption
[Accessed 15 February 2018].

Electronic Privacy Information Centre, 1994. *Crypto Experts Letter.* [Online] Available at: https://epic.org/crypto/clipper/crypto_experts_letter_1_94.html
[Accessed 15 February 2018].

Electronic Privacy Information Centre, 2016. *Apple v. FBI.* [Online] Available at: https://epic.org/amicus/crypto/apple/#legal
[Accessed 15 February 2018].

Emily, 2016. *Emily Interview* [Interview] (1 April 2016).

Erikson, J., 1999. Observers or Advocates?: On the Political Role of Security Analysts. *Cooperation and Conflict,* 34(3), pp. 311-333.

EU Transparency Register, 2016. *Google.* [Online] Available at: https://lobbyfacts.eu/representative/1d40cdaf822941888d1e6121858bb617/google
[Accessed 15 February 2018].

Evans, J., 2016. *The 'Snooper's Charter' hysteria is absurd – The IPB sets a new standard for the world.* [Online] Available at: http://www.telegraph.co.uk/news/2016/12/09/snoopers-charter-hysteria-absurd-ipb-sets-new-standard-world/
[Accessed 15 February 2018].

Evera, S. V., 1998. Offense, Defense, and the Causes of War. *International Security,* 22(4), pp. 5-43.

Evera, S. V., 1998. *Why States Beleive Foolish Ideas: Non-Self Evaluation by Government and Society,* Washington DC: Paper presented at the annual meeting of the American Political Science Association.

Facebook, 2017. *Facebook, Microsoft, Twitter and YouTube Announce Formation of the Global Internet Forum to Counter Terrorism.* [Online] Available at: https://newsroom.fb.com/news/2017/06/global-internet-forum-to-counter-terrorism/
[Accessed 15 February 2018].

Facebook, 2017. *Hard Questions: How We Counter Terrorism.* [Online] Available at: https://newsroom.fb.com/news/2017/06/how-we-counter-terrorism/
[Accessed 15 February 2018].

Facebook, G. M. T. Y., 2015. *Written Evidence - Investigatory Powers Committee.* [Online]
Available at: http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf
[Accessed 15 February 2018].

Farwell, J. P. & Rohozinski, R., 2011. Stuxnet and the Future of Cyber War. *Survival,* 53(1), pp. 23-40.

Farwell, J. P. & Rohozinski, R., 2012. The New Reality of Cyber War. *Survival,* 54(4), pp. 107-120.

Fast Company, 2012. *NYPD, Microsoft Launch All-Seeing "Domain Awareness System" With Real-Time CCTV, License Plate Monitoring [Updated].* [Online] Available at: https://www.fastcompany.com/3000272/nypd-microsoft-launch-all-seeing-domain-awareness-system-real-time-cctv-license-plate-monito
[Accessed 15 February 2018].

Fast Company, 2013. *Silicon Valley And The Intelligence Agencies.* [Online] Available at: https://www.fastcompany.com/3012725/silicon-valley-and-the-intelligence-agencies
[Accessed 15 February 2018].

Fast, S., 2015. *Facebook | Panopticon: an analysis of Facebook and its parallels to the Foucaultian Panopticon,* s.l.: The University of Tennessee.

Fast, S. A., 2015. *Facebook | Panopticon: an analysis of Facebook and its parallels to the Foucaultian Panopticon,* s.l.: University of Tennessee at Chattanooga.

FBI, 2016. *Going Dark.* [Online] Available at: https://www.fbi.gov/services/operational-technology/going-dark
[Accessed 15 February 2018].

Ferguson, H., 2014. *Undercover in MI6: what's it like to work as a spy?.* [Online] Available at: https://www.theguardian.com/careers/careers-blog/spy-career-secret-service
[Accessed 15 February 2018].

Fierke, K. M., 2005. *Diplomatic Interventions: Conflict and change in a Globalising World.* s.l.:Palgrave Macmillan UK.

Financial Times, 2016. *Google and WhatsApp back Apple in FBI encryption fight.* [Online]

Available at: https://www.ft.com/content/74a91e24-d5dd-11e5-8887-98e7feb46f27
[Accessed 15 February 2018].

Fiona, 2016. *GCHQ Interview* [Interview] (15 April 2016).

Fishman, M. & Cavender, G., 1998. Television Reality Crime Programs: Context and History. In: M. Fishman & G. Cavender, eds. *Entertaining Crime.* s.l.:Walter de Gruyter, pp. 3-18.

Fitzgerald, M., Hough, M., Joseph, I. & Qureshi, T., 2002. *Policing for London.* 1 ed. s.l.:Willan.

Floyd, R., 2008. The Environmental Security Debate and its Significance for Climate Change. *Italian Journal of International Affairs,* 43(3), pp. 51-65.

Floyd, R., 2011. Can securitisation theory be used in normative analysis? Towards a just securitisaion theory. *Security Dialogue,* 42(4-5), pp. 427-439.

Foreign Policy, 2013. *Is Edward Snowden the New Che Guevara?.* [Online] Available at: http://foreignpolicy.com/2013/08/19/is-edward-snowden-the-new-che-guevara/
[Accessed 15 February 2018].

Fortune, 2012. *Google and Facebook's new tactic in the tech wars.* [Online] Available at: http://fortune.com/2012/07/30/google-and-facebooks-new-tactic-in-the-tech-wars/
[Accessed 15 February 2018].

Foucault, M., 1971. *The Order of Discourse,* s.l.: Gallimard.

Foucault, M., 1975. *Discipline and Punish.* s.l.:Pantheon Books.

Foucault, M., 2002. *The Subject of Power - Essential Works of Foucault - 1954-1984.* London: Penguin.

Foundation for Information Policy Research, 2005. *The Crypto Wars Are Over!.* [Online]
Available at: http://www.fipr.org/press/050525crypto.html
[Accessed 15 February 2018].

Fox, L., 2014. *Snowden leaks 'criminally irresponsible', MP Liam Fox says.* [Online] Available at: http://www.bbc.co.uk/news/uk-politics-27053116
[Accessed 15 February 2018].

Freeh, L. J., 1997. *The Impact of Encryption on Public Safety.* [Online] Available at: https://cryptome.org/jya/fbi090397.htm
[Accessed 15 February 2018].

Freiwald, S., 2014. *Nothing to Fear or Nowhere to Hide: Competing Visions of the NSA's 215 Program,* s.l.: Colorado Law Technology Journal.

Funnell, L. & Dodds, K., 2017. *Geographies, Genders and Geopolitics of James Bond.* 2 ed. s.l.:Palgrave Macmillan.

Gandy, O., 1993. *The Panoptic Sort: Political Economy of Personal Information.* s.l.:Westview Press Inc.

Ganguly, S. & Hagerty, D. T., 2006. *Fearful Symmetry: India-Pakistan Crises in the Shadow of Nuclear Weapons.* s.l.:University of Washington Press.

Gates, B., 2016. *Bill Gates backs FBI in battle with Apple over San Bernardino killer's phone.* [Online]
Available at: https://www.theguardian.com/technology/2016/feb/23/bill-gates-fbi-apple-san-bernardino-killer-phone
[Accessed 15 February 2018].

GCHQ Lawyer, 2013. *GCHQ taps fibre-optic cables for secret access to world's communications.* [Online]
Available at: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
[Accessed 15 February 2018].

GCHQ, 2014. *Investigatory Powers Tribunal rejects assertions of mass surveillance.* [Online]
Available at: https://www.gchq.gov.uk/news-article/investigatory-powers-tribunal-rejects-assertions-mass-surveillance
[Accessed 15 February 2018].

GCHQ, 2016. *GCHQ Minority Report.* [Online]
Available at: https://www.gchq.gov.uk/gchq-minority-report
[Accessed 15 February 2018].

GCHQ, 2016. *GCHQ Minority Report.* [Online]
Available at: https://www.gchq.gov.uk/gchq-minority-report

GCHQ, 2017. *National challenge will develop schoolgirls' cyber security skills.* [Online]
Available at: https://www.gchq.gov.uk/press-release/national-challenge-will-develop-schoolgirls-cyber-security-skills

Georgieva, M., 2015. *Contesting the State Securitisation of Cyberspace: The Impact of Alternative Securitizing Actors,* s.l.: Central European University.

Georgieva, M., 2015. *Contesting the State Securitisation of Cyberspace: The Impact of Alternative Securitizing Actors,* s.l.: s.n.

Georgieva, M., 2015. *Contesting the State Securitisation of Cyberspace: The Impact of Alternative Securitizing Actors,* s.l.: Central European University.

Ghost.org, 2015. *Ghost Moves to DigitalOcean Global Infrastructure.* [Online]
Available at: https://blog.ghost.org/digitalocean/
[Accessed 15 February 2018].

Gibson, W., 1984. *Neuromancer.* Paperback Edition 1985 ed. s.l.:Victor Gollancz.

Girvan, N., 2010. Technification, Sweetification and Treatyfication. *Interventions,* 12(1), pp. 100-111.

Glaser, C., 1997. The Security Dilemma Revisited. *World Politics,* 50(1), pp. 171-201.

Glaser, C., 1997. The Security Dilemma Revisited. *World Politics,* 50(1), pp. 171-201.

Glasgow University, n.d. *Metaphor Map of English.* [Online] Available at: http://mappingmetaphor.arts.gla.ac.uk/ [Accessed 15 February 2018].

Global Internet Forum to Counter Terrorism, 2017. *Global Internet Forum to Counter Terrorism to Hold First Meeting in San Francisco.* [Online] Available at: https://newsroom.fb.com/news/2017/07/global-internet-forum-to-counter-terrorism-to-hold-first-meeting-in-san-francisco/ [Accessed 15 February 2018].

Glynn, P., 1992. *Closing Pandoras Box: Arms Races,Arms Control and the History of the Cold War.* New York: Basic Books.

Google Transparency Project, 2017. *Investigating Google's European Revolving Door.* [Online] Available at: http://www.googletransparencyproject.org/articles/investigating-googles-european-revolving-door [Accessed 15 February 2018].

Google, 2013. *Snowden leaks: Google 'outraged' at alleged NSA hacking.* [Online] Available at: http://www.bbc.co.uk/news/world-us-canada-24751821 [Accessed 15 February 2018].

Google, 2017. *It's Lit - a guide to what teens think is cool,* s.l.: Google.

Gorr, D. & Schünemann, W., 2013. Creating a secure cyberspace – Securitization in Internet governance dis-courses and dispositives in Germany and Russia. *International Review of Information Ethics,* 20(1), pp. 37-51.

Granados, N., 2016. *Apple Can, Should, And Will Help FBI Unlock Shooter's iPhone.* [Online] Available at: https://www.forbes.com/sites/nelsongranados/2016/02/20/apple-can-should-and-will-help-fbi-unlock-shooters-iphone/#325f7e9331c4 [Accessed 15 February 2018].

Greenslade, R., 2013. *How Hitler suspended the right to mail and telephone privacy.* [Online] Available at: https://www.theguardian.com/media/greenslade/2013/dec/04/surveillance-adolf-hitler [Accessed 15 February 2018].

Greenwald, G., 2014. *No Place to Hide.* s.l.:Penguin Random House UK.

Greenwald, G., 2016. *The Snowden effect: Privacy is good for business.* [Online] Available at: https://www.cnet.com/au/news/the-snowden-effect-privacy-is-good-for-business-nsa-data-collection/ [Accessed 15 February 2018].

Grieve, D. & Laing, E., 2009. *Rise of the Surveillance State.* [Online] Available at: https://conservativehome.blogs.com/files/surveillance-state.pdf [Accessed 15 February 2018].

Guardian, 2013. *Leaked memos reveal GCHQ efforts to keep mass surveillance secret.* [Online]

Available at: https://www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secret-snowden
[Accessed 15 February 2018].

Guarnieri, C., 2016. *Twitter.* [Online]
Available at: https://twitter.com/botherder/status/684819562760634369
[Accessed 15 February 2018].

Guitton, C., 2013. Cyber insecurity as a national threat: overreaction from Germany,. *European Security,* 22(1), pp. 21-35.

Haiven, M. & Stoneman, S., 2004. *Wal-Mart: The Panopticon of Time,* s.l.: Institue of Globalization and the Human Condition.

Hammond, P., 2015. *For Philip Hammond, Britain's spies are unsung heroes of national security.* [Online]
Available at: https://www.theguardian.com/politics/2015/mar/10/philip-hammond-britain-spies-unsung-heroes-national-security

Hammond, P., 2016. *Fifth of GCHQ intelligence comes from hacking.* [Online]
Available at: http://www.telegraph.co.uk/news/uknews/defence/12154733/Fifth-of-GCHQ-intelligence-comes-from-hacking.html
[Accessed 15 February 2018].

Hammond, P., 2017. *Chancellor's speech at the National Cyber Security Centre opening.* [Online]
Available at: https://www.gov.uk/government/speeches/chancellors-speech-at-the-national-cyber-security-centre-opening
[Accessed 15 February 2018].

Hannigan, R., 2014. *The web is a terrorist's command-and-control network of choice.* [Online]
Available at: https://www.ft.com/content/c89b6c58-6342-11e4-8a63-00144feabdc0
[Accessed 15 February 2018].

Hannigan, R., 2014. *The web is a terrorist's command-and-control network of choice.* [Online]
Available at: https://www.ft.com/content/c89b6c58-6342-11e4-8a63-00144feabdc0
[Accessed 15 February 2018].

Hannigan, R., 2014. *The web is a terrorist's command-and-control network of choice.* [Online]
Available at: https://www.ft.com/content/c89b6c58-6342-11e4-8a63-00144feabdc0
[Accessed 15 February 2018].

Hannigan, R., 2016. *Front doors and strong locks: encryption, privacy and intelligence gathering in the digital era.* [Online]
Available at: https://www.gchq.gov.uk/speech/front-doors-and-strong-locks-encryption-privacy-and-intelligence-gathering-digital-era
[Accessed 20 October 2017].

Hansen, L. & Nissenbaum, H., 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly,* 53(1), pp. 1155-1175.

Hansen, L. & Nissenbaum, H., 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly,* 53(1), pp. 1155-1175.

Hare, N. P. & Collinson, P., 2012. Organisational culture and intelligence analysis: A perspective frmo senior managers in the Defence Intelligence Assessments Staff. *Public Policy Administration,* 28(2), pp. 214-229.

Harman, J., 2015. *Disrupting the Intelligence Community.* [Online] Available at: https://www.foreignaffairs.com/articles/united-states/2015-03-01/disrupting-intelligence-community
[Accessed 15 February 2018].

Harris Interactive, 2011. *What America Thinks,* s.l.: Metlife Foundation.

Haslam, N., 2006. Dehumanisation:An Integrative Review. *Personality and Social Psychology Review,* 10(3), pp. 252-264.

Hass, R., 2010. The Role of Media in Conflict and their Influence on Securitisation. *Italian Journal of International Affairs,* 44(2009), pp. 77-91.

Head, S., 2014. *Mindless: Why Smarter Machines Are Making Dumber Humans.* s.l.:Basic Books.

Hearn, M., 2013. *Google Plus.* [Online] Available at: https://plus.google.com/+MikeHearn/posts/LW1DXJ2BK8k
[Accessed 15 February 2018].

Herz, J., 1950. Idealist Internationalism and the Security Dilemma. *World Politics,* 2(2), pp. 157-180.

Herz, J., 1950. Idealist Internationalism and the Security Dilemma. *World Politics,* pp. 157-80.

Herz, J., 1950. Idealist Internationalism and the Security Dilemma. *World Politics,* 2(2), pp. 157-180.

Hill, A., 2005. *Reality TV.* 1 ed. s.l.:Routledge.

Hill, A., 2017. *Reality TV Crime Programs.* [Online] Available at: http://criminology.oxfordre.com/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-177
[Accessed 15 February 2018].

Hill, M., 2017. *Terror chief Max Hill warns risk of attacks in Britain is highest since dark days of IRA.* [Online] Available at: http://www.telegraph.co.uk/news/2017/02/25/terror-chief-max-hill-warns-risk-attacks-britain-highest-since/
[Accessed 15 February 2018].

Hjalmarsson, O., 2013. *The Securitization of Cyberspace: How the Web Was Won,* s.l.: Lund University.

HM Government, 1994. *Intelligence Services Act 1994,* s.l.: HM Government.

HM Government, 2010. *A Strong Britain in an Age of Uncertainty: The National Security Strategy ,* s.l.: HM Government.

HM Government, 2010. *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review,* s.l.: HM Government.

HM Government, 2011. *The UK Cyber Security Strategy,* s.l.: HM Government.

HM Government, 2011. *The UK Cyber Security Strategy,* s.l.: HM Government.

HM Government, 2011. *UK Cyber Security Strategy,* s.l.: HM Government.

HM Government, 2011. *UK National Cyber Security Strategy,* s.l.: H M Government.

HM Government, 2016. *Google, Facebook and Twitter: countering extremism on social media.* [Online]
Available at: http://www.parliament.uk/business/committees/committees-a-z/commons-select/home-affairs-committee/news-parliament-2015/160129-countering-extremism-evidence/
[Accessed 15 February 2018].

HM Government, 2016. *Investigatory Powers Act 2016,* s.l.: HM Government.

HM Government, 2016. *Investigatory Powers Bill receives Royal Assent.* [Online]
Available at: https://www.gov.uk/government/news/investigatory-powers-bill-receives-royal-assent
[Accessed 15 February 2018].

HM Government, 2016. *Joint Committee on the Draft Investigatory Powers Bill - Oral Evidence,* s.l.: Joint Investigatory Powers Committee.

HM Government, 2016. *Joint Committee on the Draft Investigatory Powers Bill - Written Evidence,* s.l.: Joint Investigatory Powers Committee.

HM Government, 2016. *National Cyber Security Strategy 2016-2021,* s.l.: Crown.

HM Government, 2017. *Investigatory Powers Act,* London: HM Government.

Hobbes, T., 2016. *Leviathan.* s.l.:Penguin Classics.

Hoffman, A. M., 2002. A Conceptualization of Trust in International Relations. *European Journal of International Relations,* 8(3), pp. 375-401.

Hogan-Howe, B., 2014. *Internet is becoming a 'dark and ungoverned space', says Met chief.* [Online]
Available at: http://www.telegraph.co.uk/news/uknews/law-and-order/11214596/Internet-is-becoming-a-dark-and-ungoverned-space-says-Met-chief.html
[Accessed 15 February 2018].

Hogan-Howe, B., 2014. *Internet is becoming a 'dark and ungoverned space', says Met chief.* [Online]
Available at: http://www.telegraph.co.uk/news/uknews/law-and-order/11214596/Internet-is-becoming-a-dark-and-ungoverned-space-says-Met-chief.html
[Accessed 15 February 2018].

Hogan-Howe, B., 2014. *Internet is becoming a 'dark and ungoverned space', says Met chief.* [Online]
Available at: http://www.telegraph.co.uk/news/uknews/law-and-order/11214596/Internet-is-becoming-a-dark-and-ungoverned-space-says-Met-chief.html
[Accessed 15 February 2018].

Hollis, M. & Smith, S., 1990. *Explaining and Understanding International Relations.* s.l.:Clarendon Press.

Holmes, S. J., 2015. *Intelligence, security and privacy: A note by the Director.* [Online]
Available at: http://www.ditchley.co.uk/conferences/past-programme/2010-2019/2015/intelligence
[Accessed 15 February 2018].

Home Affairs Committee, 2014. *Seventeenth Report of Session 2013–14: Counter Terrorism,* s.l.: House of Commons.

House of Commons Science and Technology Committee, 2016. *Investigatory Powers Bill: technology issues,* London: House of Commons.

Huffington Post, 2015. *Jeremy Corbyn And Senior Shadow Cabinet Told By Intelligence Chiefs Of Scale Of ISIL Threat To Britain And British Citizens.* [Online]
Available at: http://www.huffingtonpost.co.uk/2015/11/25/jeremy-corbyn-and-senior-_n_8651014.html
[Accessed 15 February 2018].

Hughes, B., 2007. Securitizing Iraq: The Bush Administration's Social Construction of Security. *Global Change, Peace and Security,* 19(2), pp. 83-102.

Huhne, C., 2013. *Prism and Tempora: the cabinet was told nothing of the surveillance state's excesses.* [Online]
Available at: https://www.theguardian.com/commentisfree/2013/oct/06/prism-tempora-cabinet-surveillance-state
[Accessed 15 February 2018].

Huppert, J., 2013. *After the NSA leaks, we've got to talk about rebalancing security and privacy.* [Online]
Available at: http://www.theguardian.com/commentisfree/2013/oct/30/nsa-britain-balance-security-privacy
[Accessed 15 February 2018].

Huysmans, J., 2006. *The Politics of Insecurity: Fear, Migration and Asylum in the EU.* 1 ed. s.l.:Routledge.

Huysmans, J., 2006. *The Politics of Insecurity: Fear, Migration and Asylum in the EU.* 1 ed. s.l.:Routledge.

Ilves, T. H., 2014. *Rebooting Trust? Freedom vs Security in Cyberspace.* s.l.:Munich Cyber Security Conference.

Independent, T., 2017. *Facebook, Twitter and Google bosses to be grilled by Parliament over spread of 'fake news'.* [Online]
Available at: http://www.independent.co.uk/news/uk/home-news/facebook-

twitter-google-bosses-parliament-spread-fake-news-conspiracy-us-election-a7527956.html
[Accessed 15 February 2018].

Information Technology Industry Council, 2015. *Apple, Google and Microsoft: weakening encryption lets the bad guys in.* [Online] Available at: https://www.theguardian.com/technology/2015/nov/23/apple-google-microsoft-weakening-encryption-back-doors
[Accessed 15 February 2018].

InfoSecurity Group, 2014. *Global Academics Unite Behind Anti-surveillance Declaration.* [Online] Available at: https://www.infosecurity-magazine.com/news/global-academics-unite-behind-anti-surveillance/
[Accessed 15 February 2018].

Intelligence and Security Committee of Parliament, 2014. *Report on the intelligence relating to the murder of Fusilier Lee Rigby,* s.l.: Intelligence and Security Committee of Parliament.

Intelligence and Security Committee of Parliament, 2014. *Report on the intelligence relating to the murder of Fusilier Lee Rigby,* s.l.: ISC.

Intelligence and Security Committee of Parliament, 2014. *Report on the intelligence relating to the murder of Fusilier Lee Rigby,* s.l.: ISC.

Intelligence and Security Committee of Parliament, 2015. *Privacy and Security: A modern and transparent legal framework,* s.l.: Crown.

Intelligence and Security Committee of Parliament, 2016. *Report on the draft Investigatory Powers Bill,* s.l.: Crown.

Intelligence and Security Committee, 2009. *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005,* s.l.: HM Government.

Intelligence and Security Committee, 2013. *Privacy and Security: A modern and transparent legal framework,* s.l.: Crown.

Internet Live Stats, 2015. *Internet Users.* [Online] Available at: http://www.internetlivestats.com/internet-users/
[Accessed 15 February 2018].

Investigatory Powers Commissioner's Office, 2017. *Watching the watchers... Since September 2017.* [Online] Available at: https://twitter.com/IPCOffice/status/903489539062194176
[Accessed 15 February 2018].

Investigatory Powers Tribunal, 2016. *UKIPTrib 15_110-CH,* s.l.: HM Government.

Investigatory Powers Tribunal, 2016. *UKIPTrib 15_110-CH,* s.l.: October.

IPSOS Mori, 2016. *Veracity Index 2016,* s.l.: IPSOS MORI.

Iraq Survey Group, 2004. *Duelfer Report on Chemical Weapons in Iraq,* s.l.: Iraq Survey Group.

Ishaq, A., 2016. *Aisha Interview* [Interview] (29 June 2016).

Jackson, L., 2015. *Last Night.* [Online] Available at: https://wikileaks.org/podesta-emails/emailid/30593 [Accessed 15 February 2018].

Jackson, L., 2015. *Re: Last night.* [Online] Available at: https://wikileaks.org/podesta-emails/emailid/40214 [Accessed 15 February 2018].

Jackson, L., 2015. *Subject: Last night.* [Online] Available at: https://wikileaks.org/podesta-emails/emailid/30593 [Accessed 15 February 2018].

James Comey, 2014. *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?.* [Online] Available at: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course [Accessed 15 February 2018].

Jenner, L., 2018. *Backdoor: How a metaphor turns into a weapon.* [Online] Available at: https://www.hiig.de/en/blog/backdoor-how-a-metaphor-turns-into-a-weapon/ [Accessed 15 February 2018].

Jensen, D. & Draffan, G., 2004. *Welcome to the Machine: Science, Surveillance, and the Culture of Control.* s.l.:Chelsea Green Publishing.

Jervis, R., 1978. Cooperation Under the Security Dilemma. *World Politics,* 30(2), pp. 167-214.

Jervis, R., 1978. Cooperation Under the Security Dilemma. *World Politics,* 30(2), pp. 167-214.

Jervis, R., 1978. *Cooperation under the Security Dilemna,* s.l.: World Politics.

Jervis, R., 1988. Realism, Game Theory, and Cooperation. *World Politics,* 40(3), pp. 317-349.

Johnston, R., 2005. *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study,* s.l.: Center for Study of Intelligence,Central Intelligence Agency.

Jones, J., 2013. *Edward Snowden: 21st-century revolutionary icon?.* [Online] Available at: https://www.theguardian.com/world/shortcuts/2013/aug/20/edward-snowden-21st-century-revolutionary-icon [Accessed 15 February 2018].

Jones, J., 2015. *http://www.politics.co.uk/comment-analysis/2015/11/20/comment-david-cameron-should-remember-our-national-security.* [Online] Available at: http://www.politics.co.uk/comment-analysis/2015/11/20/comment-david-cameron-should-remember-our-national-security [Accessed 15 February 2018].

Jones, R. W., 1999. *Security, Strategy and Critical Theory.* s.l.:Lynne Rienner Publishers.

Kabanov, Y., 2014. *Information (Cyber-) Security Discourses and Policies in the European Union and Russia: A Comparative Analysis,* s.l.: Centre for German and European Studies.

Kabanov, Y., 2014. *Information (Cyber-) Security Discourses and Policies in the European Union and Russia: A Comparative Analysis,* Moscow: Higher School of Economics.

Kaminski, R. T., 2010. *Escaping the cyber state of nature: Cyber Deterrence and international institutions.* Tallinn, Estonia, s.n.

Kaplan, F., 2017. *The Leaky Myths of Snowden.* [Online] Available at: http://www.slate.com/articles/news_and_politics/war_stories/2016/09/what_snowden_gets_wrong_about_its_hero.html
[Accessed 15 February 2018].

Kassin, S. et al., 2015. *Social Psychology.* s.l.:Cengage Learning.

Kaufman, S., 1996. An International Theory of Inter-ethnic War. *Review of International Studies,* 22(2), pp. 149-171.

Kehl, D., WIlson, A. & Bankston, K., 2015. *Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s,* s.l.: New America.

Keizer, K., Lindenberg, S. & Steg, L., 2008. The spreading of disorder. *Science,* Volume 322, pp. 1681-1685.

Keller, R., 2006. Analysing Discourse. An Approach From the Sociology of Knowledge. *Historical Social Research,* 31(2), pp. 223-242.

Killock, J., 2013. *Europeans 'shocked and angry' by 'unaccountable' American surveillance.* [Online]
Available at: https://www.youtube.com/watch?v=Tf_9zbdu47w
[Accessed 15 February 2018].

Killock, J., 2014. *The courts should decide how much privacy we're entitled to - not GCHQ.* [Online]
Available at: http://www.independent.co.uk/voices/comment/the-courts-should-decide-how-much-privacy-were-entitled-to-not-gchq-9838882.html
[Accessed 15 February 2018].

Killock, J., 2015. *Minimal oversight of GCHQ hacking is 'a major scandal'.* [Online]
Available at: http://www.wired.co.uk/article/gchq-hacking
[Accessed 15 February 2018].

Killock, J., 2015. *Why are digital rights important?.* [Online]
Available at: https://www.openrightsgroup.org/blog/2015/why-are-digital-rights-important
[Accessed 15 February 2018].

Killock, J., 2016. [Online] Available at: https://twitter.com/jimkillock/status/796333214163992576 [Accessed 15 February 2018].

Killock, J., 2016. *Does the government want to break encryption or not?.* [Online] Available at: https://www.openrightsgroup.org/blog/2016/does-the-government-want-to-break-encryption-or-not [Accessed 15 February 2018].

Killock, J., 2016. *Investigatory Powers Act is UK's most extreme surveillance law.* [Online] Available at: https://www.openrightsgroup.org/press/releases/2016/investigatory-powers-act-most-extreme-surveillance-law [Accessed 15 February 2018].

Killock, J., 2016. *Investigatory Powers Act is UK's most extreme surveillance law.* [Online] Available at: https://www.openrightsgroup.org/press/releases/2016/investigatory-powers-act-most-extreme-surveillance-law [Accessed 15 February 2018].

Killock, J., 2016. *Investigatory Powers Act is UK's most extreme surveillance law.* [Online] Available at: https://www.openrightsgroup.org/press/releases/2016/investigatory-powers-act-most-extreme-surveillance-law

Killock, J., 2016. *Jim Interview* [Interview] (4 February 2016).

Killock, J., 2016. *Privacy experts fear Donald Trump running global surveillance network.* [Online] Available at: https://www.theguardian.com/world/2016/nov/11/trump-surveillance-network-nsa-privacy [Accessed 15 February 2018].

Killock, J., 2016. *Stop Rushing the Investigatory Powers Bill through Parliament.* [Online] Available at: https://www.openrightsgroup.org/press/releases/2016/stop-rushing-ipbill [Accessed 15 February 2018].

Killock, J., 2016. *The Investigatory Powers Bill's impact will reach beyond the UK.* [Online] Available at: https://www.openrightsgroup.org/press/releases/2016/ipb-will-reach-beyond-the-uk [Accessed 15 February 2018].

Killock, J., 2016. *Twitter.* [Online] Available at: https://twitter.com/search?q=%22Donald%20Trump%20has%20effective%20control%20of%20GCHQ%E2%80%99s%20technology%20and%20full%20access%20to

%20their%20data%20collection%22&src=typd
[Accessed 15 February 2018].

Killock, J., 2017. *Repeal the new Surveillance laws (Investigatory Powers Act).* [Online]
Available at: https://petition.parliament.uk/petitions/173199
[Accessed 15 February 2018].

Killock, J., 2017. *UK's flip-flops on encryption don't help anyone.* [Online] Available at: https://www.cnet.com/uk/news/british-government-amber-rudd-flip-flops-on-encryption/
[Accessed 15 February 2018].

Kingsmith, A. T., 2013. Virtual Roadblocks: The Securitisation of the Information Superhighway. *Conversations in Global Politics and Public Policy,* 2(1), pp. 1-14.

Kingsmith, A. T., 2013. Virtual Roadblocks: The Securitisation of the Information Superhighway. *Bridges: Conversations in Politics and Public Policy,* 2(1).

Kramer, R. M., 2001. Trust Rules for Trust Dilemmas: How Decision Makers Think and Act in the Shadow of Doubt. In: *Trust in Cyber-societies.* Berlin, Heidelberg: Springer.

Kremer, J., 2014. Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace. *Information and Communications Technology Law,* 23(3), pp. 220-237.

Kurbalija, J., 2016. *An Introduction to Internet Governance.* 7 ed. Geneva: Diplo Foundation.

Kurbalija, J., 2016. *An Introduction to Internet Governance: 7th edition.* s.l.:Diplo Foundation.

Laguna, R., 2015. *Could Hillary Clinton's Encryption 'Manhattan Project' Work?.* [Online]
Available at: http://www.nbcnews.com/tech/security/could-hillary-clinton-s-encryption-manhattan-project-work-n484086
[Accessed 15 February 2018].

Lanchester, J., 2013. *The Snowden files: why the British public should be worried.* [Online]
Available at: https://www.theguardian.com/world/2013/oct/03/edward-snowden-files-john-lanchester
[Accessed 15 February 2018].

Lapointe, A., 2011. *When good metaphors go bad: The Metaphoric "Branding" of Cyberspace,* s.l.: Centre for Strategic and International Studies.

Lash, S. & Wynne, B., 1992. Introduction. In: *Risk Society.* s.l.:SAge, p. 4.

Laux, D., 2016. *Q&A with Doug Laux, Former CIA Case Officer and Author of Left of Boom.* [Online]
Available at: http://www.criminalelement.com/blogs/2016/04/qaa-with-doug-laux-former-cia-case-officer-and-author-of-left-of-boom
[Accessed 15 February 2018].

Lavrov, G., 2013. *NSA methods reminiscent of those used in USSR under Stalin – Lavrov.* [Online]
Available at: https://www.rt.com/news/lavrov-nsa-private-life-427/
[Accessed 15 February 2018].

Lazaridi, G. & K. W., 2015. *The Securitisation of Migration in the EU.* 1 ed. s.l.:Palgrave Macmillan.

Lemke, T., 2001. *The birth of bio-politics: Michael Foucault's lectures at the College de France on neo-liberal governmentality.* s.l.:Economy and Society.

Lessig, L., 1999. *Code and Other Laws of Cyberspace.* s.l.:Basic Books.

Leswing, K., 2016. *Hillary Clinton and Apple are in lockstep on one critical issue.* [Online]
Available at: http://uk.businessinsider.com/hillary-clinton-language-about-encryption-echoes-apple-2016-6?r=US&IR=T
[Accessed 15 February 2018].

Lobban, I., 2014. *Sir Iain Lobban's valedictory speech - as delivered.* [Online]
Available at: https://www.gchq.gov.uk/speech/sir-iain-lobbans-valedictory-speech-delivered
[Accessed 15 February 2018].

Locke, J., 1689. *Two Treatises of Government.* s.l.:Awnsham Churchill.

Locke, J., 2009. *Second Treatise on Civil Government.* s.l.:World Library Classics.

Logan, R., 2014. *Uk Court Decision on Government Mass Surveillance: 'Trust Us' Isn't Enough.* [Online]
Available at: https://www.amnesty.org/en/press-releases/2014/12/uk-court-decision-government-mass-surveillance-trust-us-isnt-enough/
[Accessed 15 February 2018].

Lucas, E., 2014. *The Snowden Operation.* 1 ed. s.l.:Amazon.

Luhmann, N., 2000. Familiarity, Confidence, Trust: Problems and Alternatives. In: D. Gambetta, ed. *Trust Making and Breaking Cooperative Relations.* Oxford: Basil Blackwell, pp. 94-107.

Lyon, D., 2014. *CCTV Cambridge.* [Online]
Available at: https://www.cctvcambridge.org/SnoopingAfterSnowden
[Accessed 11 February 2018].

Lyon, D., 2014. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data and Society,* 1(2), pp. 1-13.

Lyon, D., 2015. *Surveillance After Snowden.* s.l.:Wiley.

Mangold, P., 1990. *National Security in International Relations.* s.l.:Routledge.

Mann, S., 1998. "Reflectionism" and "Diffusionism": New Tactics for Deconstructing the Video Surveillance Superhighway. *Leonardo,* 31(2), pp. 93-102.

Mann, S., Nolan, J. & Wellman, B., 2002. Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance and Society,* 1(3), pp. 331-355.

Martin, C., 2015. *GCHG: We don't have the manpower to spy on you.* [Online] Available at: http://www.cnbc.com/2015/06/02/gchq-we-dont-have-the-manpower-to-spy-on-you.html
[Accessed 15 February 2018].

Matt, 2016. *Matt Interview* [Interview] (1 April 2016).

Mayer-Schonberger, V., 2013. *Yahoo, Google, Facebook and more face fight to salvage reputations over NSA leaks.* [Online] Available at: https://www.theguardian.com/technology/2013/jun/10/apple-google-giants-nsa-revelations
[Accessed 15 February 2018].

May, T., 2014. *Commons passes emergency data laws despite criticism.* [Online] Available at: http://www.bbc.co.uk/news/uk-28305309
[Accessed 15 February 2018].

May, T., 2015. *https://www.gov.uk/government/news/home-secretary-introduces-draft-investigatory-powers-bill.* [Online] Available at: https://www.gov.uk/government/news/home-secretary-introduces-draft-investigatory-powers-bill
[Accessed 15 February 2018].

May, T., 2015. *Theresa May to revive her 'snooper's charter' now Lib Dem brakes are off.* [Online] Available at: https://www.theguardian.com/politics/2015/may/09/theresa-may-revive-snoopers-charter-lib-dem-brakes-off-privacy-election
[Accessed 15 February 2018].

May, T., 2015. *Theresa May: we must deny terrorists safe spaces to communicate.* [Online]
Available at: https://www.theguardian.com/politics/2015/jan/14/theresa-may-no-safe-spaces-terrorists-communicate
[Accessed 15 February 2018].

May, T., 2016. *Home Secretary leaves plenty unanswered after IP Bill debate.* [Online]
Available at: https://www.engadget.com/2016/01/15/theresa-may-ip-bill/
[Accessed 15 February 2018].

May, T., 2017. *May: Security services 'true heroes'.* [Online] Available at: http://www.bbc.co.uk/news/av/uk-politics-31677040

May, T., 2017. *PM statement following London terror attack: 4 June 2017.* [Online] Available at: https://www.gov.uk/government/speeches/pm-statement-following-london-terror-attack-4-june-2017
[Accessed 15 February 2018].

May, T., 2017. *Theresa May warns tech companies: 'no safe space' for extremists.* [Online]
Available at: https://www.ft.com/content/0ae646c6-4911-11e7-a3f4-c742b9791d43
[Accessed 15 February 2018].

McDonald, M., 2008. Securitisation and the Construction of Security. *European Journal of International Relations,* 14(4), pp. 563-587.

McLoud, K., 2015. *Treasonous Patriot: A Comparative Content Analysis of the Media's Portrayals of Daniel Ellsberg and Edward Snowden,* s.l.: University of Arkansas.

McSweeney, B., 1996. Identity and Security: Buzan and the Copenhagen School. *Review of International Studies,* 22(1), pp. 81-93.

Mearsheimer, J., 2001. *The Tragedy of Great Power Politics.* s.l.:W. W. Norton & Company.

Mehta, M. D. & Darier, E., 1998. Virtual Control and Disciplining on the Internet: Electronic Governmentality in the New Wired World. *The Information Society,* 14(2), pp. 107-116.

Merrill, N., 2016. *Privacy experts fear Donald Trump running global surveillance network.* [Online]
Available at: https://www.theguardian.com/world/2016/nov/11/trump-surveillance-network-nsa-privacy
[Accessed 15 February 2018].

Microsoft, 2013. *Protecting customer data from government snooping.* [Online]
Available at: https://web.archive.org/web/20131205100213/http://blogs.technet.com/b/firehose/archive/2013/12/04/protecting-customer-data-from-government-snooping.aspx
[Accessed 15 February 2018].

Microsoft, 2017. *The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack.* [Online]
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.0001b0gm51altf04xc91fxhoj5s14
[Accessed 15 February 2018].

Miller, C., 2016. *Google, Twitter, Facebook, & Microsoft to file court motions officially supporting Apple in FBI fight.* [Online]
Available at: https://9to5mac.com/2016/02/25/google-facebook-apple-fbi-fight/
[Accessed 15 February 2018].

Miller, L., 2008. Undercover Policing:. *Journal of Police and Criminal Psychology,* 21(2), pp. 1-24.

Mitrou, L., Kandias, M., Stavrou, V. & Gritzalis, D., 2014. *Social Media Profiling: A Panopticon or Omnioption tool?.* Barcelona, Surveillance and Society conference.

Mitrou, L., Kandias, M., Stavrou, V. & Gritzalis, D., 2014. *Social Media Profiling: A Panoptison or Omniopticon tool?.* Barcelona, Surveillance and Society Conference.

Monax, 2015. *Eris Industries Statement on the Reintroduction of the UK Investigatory Powers Bill.* [Online]
Available at: https://monax.io/2015/05/29/ei-comms-data-

bill/?redirect_from_eris=true
[Accessed 15 February 2018].

Money.com, 2014. *Money.com.* [Online]
Available at: http://money.cnn.com/2014/06/06/technology/security/nsa-turn-on-phone/
[Accessed 15 February 2018].

Moore, D. & Rid, T., 2016. Cryptopolitik and the Darknet. *Survival: Global Politics and Strategy,* 58(1), pp. 7-38.

Moore, D. & Rid, T., 2016. Cryptopolitik and the Darknet. *Survival,* 58(1), pp. 7-38.

Moore, D. & Rid, T., 2016. Cryptopolitik and the Darknet. *Survival,* 58(1), pp. 7-38.

Moore, D. & Rid, T., 2016. Cryptopolitik and the Darknet. 58(1).

Moretti, A., 2015. Whistleblower or Traitor: Edward Snowden, Daniel Ellsberg and the Power of Media Celebrity. *Global Media Journal,* Issue 1.

Morozov, E., 2012. *The Net Delusion: How Not to Liberate The World.* s.l.:Penguin.

Motter, A. & Lai, Y. C., 2003. Cascade-based attacks on complex networks. *Physical Review.*

Mueller, M. L., 2010. *Networks and States: The Global Politics of Internet Governance.* s.l.:MIT Press.

Muižnieks, N., 2013. *Human rights at risk when secret surveillance spreads.* [Online]
Available at: http://www.coe.int/en/web/commissioner/-/human-rights-at-risk-when-secret-surveillance-sprea-1
[Accessed 15 February 2018].

Muižnieks, N., 2013. *Human rights at risk when secret surveillance spreads.* [Online]
Available at: http://www.coe.int/en/web/commissioner/-/human-rights-at-risk-when-secret-surveillance-sprea-1
[Accessed 15 February 2018].

Muižnieks, N., 2013. *Human rights at risk when secret surveillance spreads.* [Online]
Available at: http://www.coe.int/en/web/commissioner/-/human-rights-at-risk-when-secret-surveillance-sprea-1
[Accessed 15 February 2018].

Musharraf, P., 2006. *In the Line of Fir:A memoir.* s.l.:Simon & Schuster Ltd.

National Crime Agency, 2015. *GCHQ and NCA join forces to ensure no hiding place online for criminals.* [Online]
Available at: http://www.nationalcrimeagency.gov.uk/news/736-gchq-and-nca-join-forces-to-ensure-no-hiding-place-online-for-criminals
[Accessed 15 February 2018].

NCA, 2015. *GCHQ and NCA join forces to ensure no hiding place online for criminals.* [Online]
Available at: http://www.nationalcrimeagency.gov.uk/news/736-gchq-and-nca-join-forces-to-ensure-no-hiding-place-online-for-criminals
[Accessed 15 February 2018].

Nellis, A. M., 2009. Fear of terrorism. In: *Terrorism in America.* s.l.:Jones & Bartlett Publishers, p. Chapter 6.

Neocleous, M., 2006. *Imagining the State.* s.l.:Open University Press.

Neocleous, M., 2007. Security, Liberty and the Myth of Balance: Towards a Critique of Security Politics. *Contemporary Political Theory,* 6(2), pp. 131-149.

New York Times, 2013. *Secret Documents Reveal N.S.A. Campaign Against Encryption.* [Online]
Available at: http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html
[Accessed 15 February 2018].

Ninja, 2016. *TechDirt.* [Online]
Available at: https://www.*TechDirt*.com/articles/20160106/09090233253/pioneer-internet-anonymity-hands-fbi-huge-gift-building-dangerous-backdoored-encryption-system.shtml
[Accessed 15 February 2018].

Nissenbaum, H., 2005. Where Computer Security meets national Security. *Ethics and Information Technology,* 7(1), pp. 61-73.

Nissenbaum, H., 2005. Where Computer Security meets National Security. *Ethics and Information Technology,* 7(1), pp. 61-73.

Nissenbaum, H., 2009. *Privacy in Context - Technology, Policy and the Integrity of Social Life.* s.l.:Stanford University Press.

Nojeim, G., 2013. *Yahoo, Google, Facebook and more face fight to salvage reputations over NSA leaks.* [Online]
Available at: https://www.theguardian.com/technology/2013/jun/10/apple-google-giants-nsa-revelations
[Accessed 15 February 2018].

Nolan, B. R., 2013. *Information sharing and collaboration inteh Untied States Intelligence Community: An ethnographic study of the NAtional Counter-Terrorism Centre,* s.l.: Princeton University.

Nyhan, B. & Reifler, J., 2010. When corrections fail: The persistence of political misperceptions. *Political Behaviour,* 32(2), pp. 303-330.

Obama, B., 2016. *Obama tells tech community to solve encryption problem now or pay later.* [Online]
Available at: https://www.theverge.com/2016/3/11/11207480/obama-sxsw-2016-fbi-apple-encryption
[Accessed 15 February 2018].

Off The Grid News, 2013. *NSA Cracks Encryption Codes, Can Read Email, Banking, Medical Records.* [Online]
Available at: http://www.offthegridnews.com/privacy/nsa-cracks-encryption-codes-can-read-email-banking-medical-records/
[Accessed 15 February 2018].

Ogilvie, S., 2016. *The dangers of counter-productive counter-terror strategy: a stark warning from Chilcot.* [Online]
Available at: https://www.liberty-human-rights.org.uk/news/blog/dangers-counter-productive-counter-terror-strategy-stark-warning-chilcot
[Accessed 15 February 2018].

Ohm, P. K., 2004. Parallel-Effect Statutues adn E-mail "Warrants": Reframing the Internet Surveillance Debate. *The George Washington Law Review,* 72(6), pp. 1599-1617.

OMD Blog, 2016. *Channel 4- Hunted.* [Online]
Available at: http://www.omdemeablog.com/news/channel-4-hunted/
[Accessed 15 February 2018].

Open Rights Group, 2007. *About the Open Rights Group.* [Online]
Available at: https://www.openrightsgroup.org/ourwork/annual-reports/review-of-activities/about-the-open-rights-group
[Accessed 15 February 2018].

Open Rights Group, 2008. *Chair's Forword.* [Online]
Available at: https://www.openrightsgroup.org/ourwork/annual-reports/review-of-activities-2008/chairs-foreword
[Accessed 15 February 2018].

Open Rights Group, 2009. *Annual Report 2009.* [Online]
Available at: https://www.openrightsgroup.org/assets/files/pdfs/Annual_Report_2009.pdf
[Accessed 15 February 2018].

Open Rights Group, 2009. *Annual Report 2009.* [Online]
Available at: https://www.openrightsgroup.org/assets/files/pdfs/Annual_Report_2009.pdf

Open Rights Group, 2009. *Interceptopm Modernisation or 'Protecting the Public'.* [Online]
Available at: https://www.openrightsgroup.org/ourwork/reports/interception-modernisation-or-protecting-the-public
[Accessed 15 February 2018].

Open Rights Group, 2010. *How to talk to your MP: training days.* [Online]
Available at: https://www.openrightsgroup.org/blog/2010/how-to-talk-to-your-mp-training-days
[Accessed 15 February 2018].

Open Rights Group, 2013. *'CDB: The Zombie Bill That Just Won't Die' and 'Reforming OSI'.* [Online]
Available at: https://www.meetup.com/ORG-Manchester/events/121186352/
[Accessed 15 February 2018].

Open Rights Group, 2013. *'CDB: The Zombie Bill That Just Won't Die' and 'Reforming OSI'.* [Online]
Available at: https://www.meetup.com/ORG-Manchester/events/121186352/

Open Rights Group, 2013. *Mass Surveillance Oversight Debate.* [Online]
Available at: https://www.openrightsgroup.org/ourwork/reports/mass-surveillance-oversight-debate
[Accessed 15 February 2018].

Open Rights Group, 2014. *Dear Theresa, see you in court.* [Online]
Available at: https://www.openrightsgroup.org/blog/2014/dear-theresa-see-you-in-court
[Accessed 15 February 2018].

Open Rights Group, 2014. *No Emergency! Stop the Data Retention Stitch Up!.* [Online]
Available at: https://www.openrightsgroup.org/campaigns/no-emergency-stop-the-data-retention-stitch-up
[Accessed 15 February 2018].

Open Rights Group, 2015. *2015 report about the Snowden leaks,* s.l.: Open Rights Group.

Open Rights Group, 2015. *2015 report about the Snowden leaks,* s.l.: Open Rights Group.

Open Rights Group, 2015. *We don't protect our civil liberties by attacking them..* [Online]
Available at: https://www.openrightsgroup.org/blog/2015/join-today-and-vote-for-digital-rights
[Accessed 15 February 2018].

Open Rights Group, 2016. *Digital Dystopias: Orwell's 1984 and the Internet Age.* [Online]
Available at: https://www.meetup.com/ORG-London/events/234732775/
[Accessed 15 February 2018].

Open Rights Group, 2017. *Digital Economy Bill: Briefing.* [Online]
Available at: https://www.openrightsgroup.org/ourwork/reports/digital-economy-bill-briefing
[Accessed 15 February 2018].

Open Rights Group, 2017. *ORG policy update/2017-w40.* [Online]
Available at: https://wiki.openrightsgroup.org/wiki/ORG_policy_update/2017-w40
[Accessed 11 February 2018].

Open Rights Group, 2017. *Please adopt your MP and visit them to explain why disconnection is wrong!.* [Online]
Available at: https://www.openrightsgroup.org/campaigns/disconnection/adopt-your-mp
[Accessed 15 February 2018].

Open Rights Group, 2017. *Sorry Amber Rudd, real people do value their security.* [Online]
Available at: https://www.openrightsgroup.org/blog/2017/sorry-amber-rudd-real-people-do-value-their-security
[Accessed 15 February 2018].

Open Rights Group, n.d. *About Page.* [Online] Available at: https://www.openrightsgroup.org/ourwork/ [Accessed 15 February 2018].

Open Rights Group, n.d. *Advisory Council.* [Online] Available at: https://www.openrightsgroup.org/people/advisory [Accessed 15 February 2018].

Open Rights Group, n.d. *CRYPTOPARTIES.* [Online] Available at: https://www.openrightsgroup.org/events/cryptoparties [Accessed 15 February 2018].

Open Rights Group, n.d. *GCHQ and Mass Surveillance.* [Online] Available at: https://www.openrightsgroup.org/ourwork/reports/gchq-and-mass-surveillance [Accessed 15 February 2018].

Open Rights Group, n.d. *Invasive collection: active signals.* [Online] Available at: https://www.openrightsgroup.org/assets/files/pdfs/reports/gchq/02-Part_One_Chapter_Two-Invasive_Collections.pdf [Accessed 15 February 2018].

Open Rights Group, n.d. *Invasive collection: active signals development.* [Online] Available at: https://www.openrightsgroup.org/assets/files/pdfs/reports/gchq/02-Part_One_Chapter_Two-Invasive_Collections.pdf [Accessed 15 February 2018].

Open Rights Group, n.d. *Investigatory Powers Bill - Guide for ORD Supporters.* [Online] Available at: https://www.openrightsgroup.org/assets/files/campaign_resources/investigatory_powers_bill/Briefing%20Doc%20150316%20WEB.pdf [Accessed 15 February 2018].

Open Rights Group, n.d. *Investigatory Powers Bill: Email Your MP.* [Online] Available at: https://www.openrightsgroup.org/campaigns/investigatory-powers-bill-email-your-mp/ [Accessed 15 February 2018].

Open Rights Group, n.d. *Orphan Works Hearing EU Commission.* [Online] Available at: https://www.openrightsgroup.org/ourwork/speeches/orphan-works-hearing-eu-commission [Accessed 15 February 2018].

Open Rights Group, n.d. *You can also join ORG to defend your digital rights.* [Online] Available at: https://www.openrightsgroup.org/updates/check-your-inbox-now/ [Accessed 15 February 2018].

Owen, B., 2016. *Ben Interview* [Interview] (30 March 2016).

Parker, A., 2015. *Director General speaks on terrorism, technology and oversight - See more at: https://www.mi5.gov.uk/news/director-general-speaks-on-terrorism-technology-and-oversight#sthash.TwZAtTsj.dpuf.* [Online] Available at: https://www.mi5.gov.uk/news/director-general-speaks-on-terrorism-

technology-and-oversight
[Accessed 15 February 2018].

Parker, A., 2016. *MI5 head: 'increasingly aggressive' Russia a growing threat to UK.* [Online]
Available at: https://www.theguardian.com/uk-news/2016/oct/31/andrew-parker-increasingly-aggressive-russia-a-growing-threat-to-uk-says-mi5-head
[Accessed 15 February 2018].

Parliament.uk, 2016. *Bill documents — Investigatory Powers Act 2016.* [Online] Available at: https://services.parliament.uk/bills/2015-16/investigatorypowers/documents.html
[Accessed 15 February 2018].

Pateron, K. et al., 2013. *Open Letter From UK Security Researchers.* [Online] Available at: http://bristolcrypto.blogspot.co.uk/2013/09/open-letter-from-uk-security-researchers.html
[Accessed 15 February 2018].

Paterson, K., Bellare, M. & Rogaway, P., 2015. *Security of Symmetric Encryption against Mass Surveillance.* s.l., International Cryptology Conference.

Paterson, K. et al., 2013. *Open Letter From UK Security Researchers.* [Online] Available at: http://bristolcrypto.blogspot.co.uk/2013/09/open-letter-from-uk-security-researchers.html
[Accessed 15 February 2018].

PEN America, 2014. *PEN Surveillance Metaphor Mapping Project.* [Online] Available at: https://pen.org/infographic/pen-surveillance-metaphor-mapping-project
[Accessed 15 February 2018].

PEN America, 2015. *Global Chilling: The Impact of Mass Surveillance on International Writers,* s.l.: PEN America.

Pew Research Centre, 2014. *Social Media and the 'Spiral of Silence'.* [Online] Available at: http://www.pewinternet.org/2014/08/26/social-media-and-the-spiral-of-silence/
[Accessed 11 February 2018].

Pew Research Centre, 2015. *Americans' Privacy Strategies Post-Snowden,* s.l.: Pew Research Centre.

Pew Research Centre, 2016. *15 Years After 9/11, a Sharp Partisan Divide on Ability of Terrorists to Strike U.S..* [Online] Available at: http://www.people-press.org/2016/09/07/15-years-after-911-a-sharp-partisan-divide-on-ability-of-terrorists-to-strike-u-s/?utm_source=adaptivemailer&utm_medium=email&utm_campaign=16-09-07%209/11&org=982&lvl=100&ite=254&lea=32754&ctr=0&par=1&trk=
[Accessed 15 February 2018].

Podesta, J., 2016. *Re: Happy New Year.* [Online] Available at: https://wikileaks.org/podesta-emails/emailid/33752
[Accessed 15 February 2018].

Politico, 2017. *Theresa May's Conservatives threaten social media crackdown if elected.* [Online]
Available at: http://www.politico.eu/article/theresa-mays-conservatives-threaten-social-media-crackdown-if-elected/
[Accessed 15 February 2018].

Pompeo, C. M., 2014. *Pompeo to SXSW Organizers: Don't Give Snowden a Platform.* [Online]
Available at: https://www.npr.org/sections/alltechconsidered/2014/03/10/288372317/sxsw-snowden-speech-has-conference-buzzing-congressman-stewing
[Accessed 15 February 2018].

Posen, B. R., 1993. The Security Dilemma and Ethnic Conflict. *Survival,* 35(1), pp. 27-47.

Qin, J., 2015. Hero on Twitter, Traitor on News: How Social Media and Legacy News Frame Snowden. *The International Journal of Press/Politics,* 20(2), pp. 166-184.

Reform Government Surveillance, 2015. *Voices For Reform.* [Online] Available at: https://www.reformgovernmentsurveillance.com/#may-19 [Accessed 15 February 2018].

Reuters, 2014. *NSA memo confirms Snowden scammed passwords from colleagues.* [Online]
Available at: http://www.reuters.com/article/us-usa-security/nsa-memo-confirms-snowden-scammed-passwords-from-colleagues-idUSBREA1C1MR20140213
[Accessed 15 February 2018].

Rid, T., 2013. *Cyber War WIll Not Take Place.* London: C. Hurst & Co. (Publishers) Ltd.

Roe, P., 2012. Is securitization a 'negative' concept? Revisiting the normative debate over normal versus extraordinary politics. *Security Dialogue,* 43(3), pp. 249-266.

Ronald Deibert, M. C.-N., 2012. Global Governance and the Spread of Cyberspace Controls. *Global Governance,* 18(3), pp. 339-361.

Rosen, J., 2005. *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age.* s.l.:Random House.

Ross, L. & Mark Lepper, M. H., 1975. Perseverance in self-perception and social perception: Biased attributional processes in the debriefing paradigm.. *Journal of Personality and Social Psychology,* 32(5), pp. 880-892.

Royal United Services Institute, 2015. *A Democratic Licence to Operate,* London: RUSI.

Royal United Services Institute, 2015. *A Democratic Licence to Operate,* s.l.: Royal United Services Institute.

Ruane, J. & Todd, J., 1996. *The Dynamics of Conflict in Northern Ireland: Power, Conflict and Emancipation.* s.l.:Cambridge University Press.

Rudd, A., 2017. *Amber Rudd : 'We must be able to access WhatsApp'.* [Online] Available at: http://www.bbc.co.uk/news/av/uk-politics-39398190/amber-rudd-we-must-be-able-to-access-whatsapp
[Accessed 15 February 2018].

Rudd, A., 2017. *Amber Rudd accuses tech giants of 'sneering' at politicians.* [Online] Available at: http://www.bbc.co.uk/news/uk-politics-41463401
[Accessed 15 February 2018].

Rudd, A., 2017. *Amber Rudd warns tech firms face 'ticking off' over terrorism.* [Online]
Available at: http://news.sky.com/story/amber-rudd-warns-tech-firms-face-more-than-a-ticking-off-10814608
[Accessed 15 February 2018].

Rudd, A., 2017. *UK home secretary Amber Rudd says 'real people' don't need end-to-end encryption.* [Online]
Available at: http://uk.businessinsider.com/home-secretary-amber-rudd-real-people-dont-need-end-to-end-encryption-terrorists-2017-8
[Accessed 15 February 2018].

Rudd, A., 2017. *We don't want to ban encryption, but our inability to see what terrorists are plotting undermines our security.* [Online]
Available at: http://www.telegraph.co.uk/news/2017/07/31/dont-want-ban-encryption-inability-see-terrorists-plotting-online/
[Accessed 15 February 2018].

Rudd, A., 2017. *WhatsApp accused of giving terrorists 'a secret place to hide' as it refuses to hand over London attacker's messages.* [Online]
Available at: http://www.telegraph.co.uk/news/2017/03/26/home-secretary-amber-rudd-whatsapp-gives-terrorists-place-hide/
[Accessed 15 February 2018].

Rudd, A., 2017. *WhatsApp accused of giving terrorists 'a secret place to hide' as it refuses to hand over London attacker's messages.* [Online]
Available at: http://www.telegraph.co.uk/news/2017/03/26/home-secretary-amber-rudd-whatsapp-gives-terrorists-place-hide/
[Accessed 15 February 2018].

Rue, F. L., 2011. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*,* s.l.: United Nations Human Rights Council.

Rueter, N., 2011. *The Cybersecurity Dilemma,* s.l.: Duke University.

Rueter, N., 2011. *The Cybersecurity Dilemma,* s.l.: Duke University.

Ruiz, J., 2016. *Data Privacy Day: the new EU Data Protection Regulation explained.* [Online]
Available at: https://www.openrightsgroup.org/blog/2016/data-protection-day-and-the-new-eu-regulation
[Accessed 15 February 2018].

Ruiz, J., 2016. *Javier Interview* [Interview] (4 February 2016).

Rusbridger, A., 2013. *Lib Dems at war over whether Snowden leaks 'entirely right'.* [Online]
Available at: http://www.telegraph.co.uk/news/uknews/defence/10371769/Lib-Dems-at-war-over-whether-Snowden-leaks-entirely-right.html
[Accessed 15 February 2018].

Salvo, P. D., 2016. Framing Edward Snowden: A comparative analysis of four newspapers in China, United Kingdom and United States. *Journalism,* 17(7), pp. 805-822.

Samson, R., 2017. *Twitter.* [Online]
Available at: https://twitter.com/renatesamson/status/892331408466771968
[Accessed 15 February 2018].

Savage, M., 2010. *Inside GCHQ: 'Caution: Here comes the BBC'.* [Online]
Available at: http://news.bbc.co.uk/1/hi/magazine/8589664.stm
[Accessed 15 February 2018].

Schelling, T., 1960. *The Strategy of Conflict.* s.l.:Harvard University Press.

Schmitt, C., 1932. *The Concept of the Political.* 1 ed. Munich: Duncker and Humblot.

Schneier, B., 1995. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* s.l.:John Wiley & Sons.

Schneier, B., 2000. *Books - Secretes and Lies - Preface.* [Online]
Available at: https://www.schneier.com/books/secrets_and_lies/pref.html
[Accessed 15 February 2018].

Schneier, B., 2004. *Secrets and Lies: Digital Security in a Networked World.* s.l.:John Wiley & Sons.

Schneier, B., 2013. *Revealed: how US and UK spy agencies defeat internet privacy and security.* [Online]
Available at: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
[Accessed 15 February 2018].

Schneier, B., 2015. *Bruce Schneier: David Cameron's proposed encryption ban would 'destroy the internet'.* [Online]
Available at: http://uk.businessinsider.com/bruce-schneier-david-cameron-proposed-encryption-ban-destroy-the-internet-2015-7
[Accessed 15 February 2018].

Schneier, B., 2015. *Bruce Schneier: David Cameron's proposed encryption ban would 'destroy the internet'.* [Online]
Available at: http://uk.businessinsider.com/bruce-schneier-david-cameron-proposed-encryption-ban-destroy-the-internet-2015-7
[Accessed 15 February 2018].

Schneier, B., 2016. *New leaks prove it: the NSA is putting us all at risk to be hacked.* [Online]
Available at: https://www.vox.com/2016/8/24/12615258/nsa-security-breach-hoard
[Accessed 15 February 2018].

Schneier, B., 2016. *The Importance of Strong Encryption to Security.* [Online] Available at: https://www.schneier.com/blog/archives/2016/02/the_importance_.html [Accessed 15 February 2018].

Schneier, B., 2016. *The Importance of Strong Encryption to Security.* [Online] Available at: https://www.schneier.com/blog/archives/2016/02/the_importance_.html [Accessed 15 February 2018].

Schneier, B., 2016. *The Importance of Strong Encryption to Security.* [Online] Available at: https://www.schneier.com/blog/archives/2016/02/the_importance_.html [Accessed 15 February 2018].

Schuurman, E., 1997. Philosophical and Ethical Problems of Technicism and Genetic Engineering. *Techne: Research in Philosophy and Technology,* 3(1), pp. 27-44.

Schwarz, K. J., 2016. *The Securitization of Cyberspace through Technification,* s.l.: Virginia Tech.

Schwarz, K. J., 2016. *The Securitization of Cyberspace through Technification,* s.l.: Virginia Polytechnic Institute and State University.

Scribble, 2013. *Record-Breaking One Million Viewers Simultaneously Stream ScribbleLive Coverage of Apple Event.* [Online] Available at: http://www.scribblelive.com/press-release/record-breaking-one-million-viewers-simultaneously-stream-scribblelive-coverage-of-apple-event/ [Accessed 15 February 2018].

Sears, J., 1995. "Crimewatch" and the rhetoric of verisimilitude. *Critical Survey,* 7(1), pp. 51-58.

Secondat, C. d., 1749. *The Spirit of the Laws,* Amsterdam: Chatelain.

Sell, N., 2016. *Encrypted Messaging App Co-Founder: Tim Cook Is A 'National Security Hero'.* [Online] Available at: http://www.npr.org/2016/02/18/467253429/encrypted-messaging-app-ceo-tim-cook-is-a-national-security-hero [Accessed 15 February 2018].

Senft, A. et al., 2014. *Information controls during Thailand's 2014 Coup,* s.l.: Citizen Lab.

Senft, A. et al., 2014. *Iraq Information Controls Update: Analyzing Internet Filtering and Mobile Apps,* s.l.: Citizen Lab.

Shlaim, A., 2007. *Lion of Jordan: The Life of King Hussein in War and Peace.* s.l.:Penguin Books Ltd.

Shmueli, D., Elliott, M. & Kaufman, S., 2006. Frame Changes and the Management of Intractable Conflicts. *Conflict Resolution Quarterly,* 24(2), pp. 207-218.

Shore, S. M., 1998. No Fences Make Good Neighbours: The Development of the US-Canadian Security Community, 1871-1940. In: E. Adler & M. Barnett, eds. *Security Communities.* s.l.:Cambridge University Press, pp. 333-367.

Snowden, E., 2013. *Edward Snowden Interview.* [Online]
Available at: http://www.thejustice.org/article/2015/11/reevaluate-international-opinion-of-snowdens-actions
[Accessed 15 February 2018].

Snowden, E., 2013. *Edward Snowden Interview.* [Online]
Available at: http://www.thejustice.org/article/2015/11/reevaluate-international-opinion-of-snowdens-actions

Snowden, E., 2013. *Edward Snowden, after months of NSA revelations, says his mission's accomplished.* [Online]
Available at: https://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html?utm_term=.3d770c2120da
[Accessed 15 February 2018].

Snowden, E., 2013. *Edward Snowden, NSA files source: 'If they want to get you, in time they will.* [Online]
Available at: https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why
[Accessed 15 February 2018].

Snowden, E., 2013. *Edward Snowden, NSA files source: 'If they want to get you, in time they will'.* [Online]
Available at: https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why
[Accessed 15 February 2018].

Snowden, E., 2013. *Edward Snowden: I'm Still Working for NSA and am not Helping Russia.* [Online]
Available at: http://www.ibtimes.co.uk/edward-snowden-im-still-working-nsa-am-not-cahoots-russia-1430190
[Accessed 15 February 2018].

Snowden, E., 2013. *Edward Snowden: NSA whistleblower answers reader questions.* [Online]
Available at: https://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower
[Accessed 15 February 2018].

Snowden, E., 2013. *Edward Snowden: NSA whistleblower answers reader questions.* [Online]
Available at: https://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower
[Accessed 15 February 2018].

Snowden, E., 2013. *Edward Snowden: the whistleblower behind the NSA surveillance revelations.* [Online]
Available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
[Accessed 15 February 2018].

Snowden, E., 2013. *Edward Snowden: the whistleblower behind the NSA surveillance revelations.* [Online] Available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
[Accessed 15 February 2018].

Snowden, E., 2013. *Edward Snowden: the whistleblower behind the NSA surveillance revelations.* [Online] Available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
[Accessed 15 February 2018].

Snowden, E., 2013. *Edward Snowden's Christmas Message 2013.* [Online] Available at: https://www.youtube.com/watch?v=MjOACWG0oW8
[Accessed 15 February 2018].

Snowden, E., 2013. *Interview on NSA Whistleblowing* [Interview] (6 June 2013).

Snowden, E., 2013. *NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things' – video.* [Online] Available at: https://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video
[Accessed 15 February 2018].

Snowden, E., 2013. *Statement by Edward Snowden to human rights groups at Moscow's Sheremetyevo airport.* [Online] Available at: https://wikileaks.org/Statement-by-Edward-Snowden-to.html
[Accessed 15 February 2018].

Snowden, E., 2014. *Edward Snowden.* [Online] Available at: https://www.wired.com/2014/08/edward-snowden/#ch-1
[Accessed 15 February 2018].

Snowden, E., 2014. *Edward Snowden interview - the edited transcript.* [Online] Available at: https://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript
[Accessed 15 February 2018].

Snowden, E., 2014. *Edward Snowden tells NBC: I'm a patriot.* [Online] Available at: http://edition.cnn.com/2014/05/28/us/edward-snowden-interview/
[Accessed 15 February 2018].

Snowden, E., 2014. *Edward Snowden: A 'Nation' Interview.* [Online] Available at: https://www.thenation.com/article/snowden-exile-exclusive-interview/
[Accessed 15 February 2018].

Snowden, E., 2014. *Edward Snowden: A 'Nation' Interview.* [Online] Available at: https://www.thenation.com/article/snowden-exile-exclusive-interview/
[Accessed 15 February 2018].

Snowden, E., 2014. *Edward Snowden's Motive Revealed: He Can 'Sleep at Night.* [Online]

Available at: http://www.nbcnews.com/feature/edward-snowden-interview/edward-snowdens-motive-revealed-he-can-sleep-night-n116851
[Accessed 15 February 2018].

Snowden, E., 2014. *Here's how we take back the Internet.* [Online]
Available at: https://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet/transcript?language=en
[Accessed 15 February 2018].

Snowden, E., 2015. *Edward Snowden Supports Apple's Public Stance On Privacy.* [Online]
Available at: https://techcrunch.com/2015/06/17/but-bring-the-hammer-if-it-betrays-us/#.zoowaq:5Ij7
[Accessed 15 February 2018].

Snowden, E., 2015. *Edward Snowden Supports Apple's Public Stance On Privacy.* [Online]
Available at: https://techcrunch.com/2015/06/17/but-bring-the-hammer-if-it-betrays-us/#.zoowaq:5Ij7

Snowden, E., 2015. *Twitter.* [Online]
Available at: https://twitter.com/Snowden/status/678396357145686016
[Accessed 15 February 2018].

Snowden, E., 2016. *Edward Snowden Responds to Critics.* [Online]
Available at: http://www.wnyc.org/story/edward-snowden-responds-critics/
[Accessed 15 February 2018].

Snowden, E., 2016. *'Extreme surveillance' becomes UK law with barely a whimper.* [Online]
Available at: https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper
[Accessed 15 February 2018].

Snowden, E., 2016. *'Extreme surveillance' becomes UK law with barely a whimper.* [Online]
Available at: https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper
[Accessed 15 February 2018].

Snowden, E., 2016. *Snowden: The 'Myth' of Going Dark.* [Online]
Available at: http://www.gjil.org/2016/11/by-boris-lubarsky-photo-boris-lubarsky.html
[Accessed 15 February 2018].

Soghoian, C., 2016. *Twitter.* [Online]
Available at: https://twitter.com/csoghoian/status/684730921153609728
[Accessed 15 February 2018].

Solove, D., 2011. *Nothing to Hide: The False Tradeoff Between Privacy and Security.* s.l.:Yale University Press.

Southwood, B., 2017. *Lackademia: Why do Academics lean left?,* s.l.: Adam Smith Institute.

Spectator Events, 2017. *Spectator Events.* [Online] Available at: https://twitter.com/SpectatorEvents/status/914911027422269440 [Accessed 15 February 2018].

Statista, 2013. *1.17 Billion People Use Google Search.* [Online] Available at: https://www.statista.com/chart/899/unique-users-of-search-engines-in-december-2012/ [Accessed 15 February 2018].

Stewart, 2016. *GCHQ - coming out and proud.* [Online] Available at: https://www.gchq.gov.uk/news-article/gchq-coming-out-and-proud

Stewart, J., 2011. *Business Insider.* [Online] Available at: http://www.businessinsider.com/jon-stewart-mark-zuckerberg-goldman-sachs-2011-1?IR=T [Accessed 15 February 2018].

Stohl, M., 2006. Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?. *Crime, Law and Social Change,* 46(4-5), pp. 223-238.

Stowsky, J., 2003. *Secrets or Shields to Share? New Dilemmas for Dual Use Technology Development and the Quest.* s.l., Berkeley Roundtable on the International Economy.

Sullivan, J., 2013. Uncovering the data panopticon: The urgent need for critical scholarship in an era of corporate and government surveillance. *The Political Economy of Communication,* 1(2).

Sullivan, J. L., 2013. Uncovering the data panopticon: The urgent need for critical scholarship in an era of corporate and government surveillance. *The Political Economy of Communication,* 1(2).

Tang, S., 2009. The Security Dilemma: A Conceptual Analysis. *Security Studies,* 18(3), pp. 587-623.

Tarand, I., 2014. *Is Russian and Chinese spying a bigger threat to Europe than the NSA?.* [Online] Available at: http://www.debatingeurope.eu/2014/03/24/russian-chinese-spying-nsa-eu/#.WL_Tu_nyiUk [Accessed 15 February 2018].

Taylor, N., 2002. State Surveillance and the Right to Privacy. *Surveillance & Society,* 1(1), pp. 66-85.

Taylor, P., 2012. *What are spies really like?.* [Online] Available at: http://www.bbc.co.uk/news/magazine-17560253

Tech Crunch, 2013. *Yahoo Will Follow Google In Encrypting Data Center Traffic, Customer Data Flow By Q1 '14.* [Online] Available at: https://techcrunch.com/2013/11/18/yahoo-will-follow-google-in-encrypting-data-center-traffic-all-traffic-between-company-and-customers-by-q1-

14/
[Accessed 15 February 2018].

Tech Crunch, 2017. *Facebook now has 2 billion monthly users… and responsibility.* [Online]
Available at: https://techcrunch.com/2017/06/27/facebook-2-billion-users/
[Accessed 15 February 2018].

Tech Dirt, 2016. *James Comey Claims He Wants An 'Adult Conversation' About Encryption; Apparently 'Adults' Ignore Experts.* [Online]
Available at: https://www.*TechDirt*.com/articles/20160831/00094935397/james-comey-claims-he-wants-adult-conversation-about-encryption-apparently-adults-ignore-experts.shtml
[Accessed 15 February 2018].

Tech World, 2016. *Too many UK politicians are clueless about tech.* [Online]
Available at: https://www.techworld.com/security/too-many-uk-politicians-are-clueless-about-tech-3625100/
[Accessed 15 February 2018].

TechDirt, 2014. *Peek-A-Boo: GCHQ Has Been Checking You Out Through Your Webcam.* [Online]
Available at: https://www.*TechDirt*.com/articles/20140227/09452426376/peek-a-boo-gchq-has-been-checking-you-out-through-your-webcam.shtml
[Accessed 15 February 2018].

TED, 2014. *Here's how we take back the Internet.* [Online]
Available at: https://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet
[Accessed 15 February 2018].

Telegraph, 2013. *Yes, Big Brother is watching you. But for a good reason.* [Online]
Available at: http://www.telegraph.co.uk/news/politics/10107489/Yes-Big-Brother-is-watching-you.-But-for-a-good-reason.html
[Accessed 15 February 2018].

The Atlantic, 2016. *Public Opinion Supports Apple Over the FBI—or Does It?.* [Online]
Available at: http://www.theatlantic.com/national/archive/2016/02/apple-fbi-polls/470736/
[Accessed 15 February 2018].

The Baha Mousa Public Inquiry, 2011. *The Baha Mousa Public Inquiry Report,* s.l.: House of Commons.

The Berkman Centre, 2016. *Don't Panic. Making Progress on the 'Going Dark' Debate,* s.l.: The Berkman Centre for Internet and Society at Harvard University.

The Guardian, 2001. *NHS faces huge damages bill after millennium bug error.* [Online]
Available at: https://www.theguardian.com/uk/2001/sep/14/martinwainwright
[Accessed 15 February 2018].

The Guardian, 2012. *Google privacy policy slammed by EU data protection chiefs.* [Online]
Available at: https://www.theguardian.com/technology/2012/oct/16/google-privacy-policies-eu-data-protection
[Accessed 15 February 2018].

The Guardian, 2013. *BT and Vodafone among telecoms companies passing details to GCHQ.* [Online]
Available at: https://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq
[Accessed 15 February 2018].

The Guardian, 2013. *Edward Snowden NSA files: Guardian should be prosecuted, says Tory MP.* [Online]
Available at: https://www.theguardian.com/politics/2013/oct/22/edward-snowden-guardian-should-be-prosecuted-tory-mp
[Accessed 15 February 2018].

The Guardian, 2013. *Katharine Gun: Ten years on what happened to the woman who revealed dirty tricks on the UN Iraq war vote?.* [Online]
Available at: https://www.theguardian.com/world/2013/mar/03/katharine-gun-iraq-war-whistleblower
[Accessed 15 February 2018].

The Guardian, 2013. *Mastering the internet: how GCHQ set out to spy on the world wide web.* [Online]
Available at: https://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet
[Accessed 15 February 2018].

The Guardian, 2013. *Microsoft and Yahoo voice alarm over NSA's assault on internet encryption.* [Online]
Available at: https://www.theguardian.com/world/2013/sep/06/yahoo-nsa-gchq-decryption-abuse
[Accessed 15 February 2018].

The Guardian, 2013. *Revealed: how US and UK spy agencies defeat internet privacy and security.* [Online]
Available at: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
[Accessed 15 February 2018].

The Guardian, 2013. *Revealed: how US and UK spy agencies defeat internet privacy and security.* [Online]
Available at: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
[Accessed 15 February 2018].

The Guardian, 2013. *Spy agency chiefs defend surveillance – as it happened.* [Online]
Available at: https://www.theguardian.com/world/2013/nov/07/heads-of-gchq-mi5-and-mi6-appear-before-intelligence-committee-live
[Accessed 15 February 2018].

The Guardian, 2013. *UK gathering secret intelligence via covert NSA operation.* [Online]
Available at: https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism
[Accessed 11 February 2018].

The Guardian, 2014. *Actors, musicians and journalists sign statement supporting Edward Snowden.* [Online]
Available at: https://www.theguardian.com/media/greenslade/2014/nov/13/edward-snowden-the-nsa-files
[Accessed 15 February 2018].

The Guardian, 2014. *Facebook reveals news feed experiment to control emotions.* [Online]
Available at: https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds
[Accessed 18 February 2018].

The Guardian, 2014. *Facebook's secret mood experiment: have you lost trust in the social network?.* [Online]
Available at: https://www.theguardian.com/technology/poll/2014/jun/30/facebook-secret-mood-experiment-social-network
[Accessed 15 February 2018].

The Guardian, 2014. *GCHQ has tools to manipulate online information, leaked documents show.* [Online]
Available at: https://www.theguardian.com/uk-news/2014/jul/14/gchq-tools-manipulate-online-information-leak
[Accessed 15 February 2018].

The Guardian, 2014. *Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ.* [Online]
Available at: https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo
[Accessed 15 February 2018].

The Guardian, 2015. *Legal experts call for greater scrutiny of surveillance laws.* [Online]
Available at: https://www.theguardian.com/technology/2015/may/26/legal-experts-greater-scrutiny-surveillance-laws
[Accessed 15 February 2018].

The Guardian, 2015. *MPs David Davis and Tom Watson in court challenge over surveillance act.* [Online]
Available at: https://www.theguardian.com/world/2015/jun/04/mps-david-davis-and-tom-watson-in-court-challenge-over-surveillance-act
[Accessed 15 February 2018].

The Guardian, 2016. *Edward Snowden makes 'moral' case for presidential pardon.* [Online]
Available at: https://www.theguardian.com/us-news/2016/sep/13/edward-

snowden-why-barack-obama-should-grant-me-a-pardon
[Accessed 15 February 2018].

The Guardian, 2016. *Extreme surveillance' becomes UK law with barely a whimper.* [Online]
Available at: https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper

The Guardian, 2016. *Google agrees to pay British authorities £130m in back taxes.* [Online]
Available at: https://www.theguardian.com/technology/2016/jan/22/google-agrees-to-pay-hmrc-130m-in-back-taxes
[Accessed 15 February 2018].

The Guardian, 2016. *Privacy experts fear Donald Trump running global surveillance network.* [Online]
Available at: https://www.theguardian.com/world/2016/nov/11/trump-surveillance-network-nsa-privacy
[Accessed 15 February 2018].

The Guardian, 2016. *Worth it': FBI admits it paid $1.3m to hack into San Bernardino iPhone.* [Online]
Available at: https://www.theguardian.com/technology/2016/apr/21/fbi-apple-iphone-hack-san-bernardino-price-paid
[Accessed 15 February 2018].

The Guardian, 2017. *Who is to blame for exposing the NHS to cyber-attacks?.* [Online]
Available at: https://www.theguardian.com/technology/2017/may/15/who-is-to-blame-for-exposing-the-nhs-to-cyber-attacks
[Accessed 11 February 2018].

The Independent, 2013. *MPs question Guardian editor Alan Rusbridger's patriotism over Edward Snowden leaks.* [Online]
Available at: http://www.independent.co.uk/news/media/press/mps-question-guardian-editor-alan-rusbridger-s-patriotism-over-edward-snowden-leaks-8981167.html
[Accessed 15 February 2018].

The Independent, 2014. *'Facebook has blood on its hands' for failing to raise alarm, says Lee Rigby's sister.* [Online]
Available at: http://www.independent.co.uk/news/uk/home-news/lee-rigby-report-facebook-has-blood-on-its-hands-for-failing-to-raise-alarm-sister-says-9883539.html
[Accessed 15 February 2018].

The Independent, 2015. *Tory MP Richard Graham accused of quoting Joseph Goebbels in defence of new surveillance bill.* [Online]
Available at: https://www.indy100.com/article/tory-mp-richard-graham-accused-of-quoting-joseph-goebbels-in-defence-of-new-surveillance-bill--bklSCE9nOg
[Accessed 15 February 2018].

The Intercept, 2011. *Behavioural Science Support for JTRIG'S Effects and Online HUMINT Operations.* [Online] Available at: https://theintercept.com/document/2015/06/22/behavioural-science-support-jtrig/
[Accessed 15 February 2018].

The Investigatory Powers Tribunal, 2014. *Liberty/Privacy No 1,* London: The Investigatory Powers Tribunal.

The Register, 2016. *FBI Director wants 'adult conversation' about backdooring encryption.* [Online] Available at: https://www.theregister.co.uk/2016/08/31/fbi_wants_adult_conversation_about_backdoors/
[Accessed 15 February 2018].

The Register, 2017. *Home Sec Amber Rudd: Yeah, I don't understand encryption. So what?.* [Online] Available at: https://www.theregister.co.uk/2017/10/03/amber_rudd_still_does_not_understand_encryption/
[Accessed 11 February 2018].

The Telegraph, 2009. *Iraq war: timeline of conflict.* [Online] Available at: http://www.telegraph.co.uk/news/worldnews/middleeast/iraq/6278938/Iraq-war-timeline-of-conflict.html
[Accessed 15 February 2018].

The Telegraph, 2015. *George Osborne announces 1,000 extra intelligence staff to tackle threat of Isil.* [Online] Available at: http://www.telegraph.co.uk/news/politics/11984575/George-Osborne-announces-1000-extra-intelligence-staff-to-tackle-threat-of-Isil.html
[Accessed 15 February 2018].

The Telegraph, 2015. *George Osborne announces 1,000 extra intelligence staff to tackle threat of Isil.* [Online] Available at: http://www.telegraph.co.uk/news/politics/11984575/George-Osborne-announces-1000-extra-intelligence-staff-to-tackle-threat-of-Isil.html
[Accessed 15 February 2018].

The Telegraph, 2017. *Government 'blocked' from accessing Twitter data to help spot terrorist plots.* [Online] Available at: http://www.telegraph.co.uk/news/2017/04/25/government-blocked-accessing-twitter-data-help-spot-terrorist/
[Accessed 15 February 2018].

The Telegraph, 2017. *Government 'blocked' from accessing Twitter data to help spot terrorist plots.* [Online] Available at: http://www.telegraph.co.uk/news/2017/04/25/government-blocked-accessing-twitter-data-help-spot-terrorist/
[Accessed 15 February 2018].

The TOR Project, n.d. *TOR: Overview.* [Online] Available at: https://www.torproject.org/about/overview.html.en [Accessed 15 February 2018].

The Verge, 2015. *Edward Snowden issues 'call to arms' for tech companies in secret SXSW meeting.* [Online] Available at: https://www.theverge.com/2015/3/15/8218659/edward-snowden-secret-sxsw-2015-meeting [Accessed 15 February 2018].

Toft, P., 2005. John J. Mearsheimer: an offensive realist between geopolitics and power. *Journal of International Relations and Development,* 8(4), pp. 381-408.

Tohn, D., 2009. *Digital trench warfare.* [Online] Available at: http://www.boston.com/bostonglobe/editorial_opinion/oped/articles/2009/06/11/digital_trench_warfare/ [Accessed 15 February 2018].

Torpey, J., 2000. *The Invention of the Passport: Surveillance, Citizenship and State.* s.l.:Cambridge University Press.

Travis, A., 2015. *Snowden leak: governments' hostile reaction fuelled public's distrust of spies.* [Online] Available at: https://www.theguardian.com/world/2015/jun/15/snowden-files-us-uk-government-hostile-reaction-distrust-spies [Accessed 15 February 2018].

Trump, D., 2016. *Trump and His Advisors on Surveillance, Encryption, Cybersecurity.* [Online] Available at: https://www.eff.org/deeplinks/2016/12/trump-and-his-advisors-surveillance-encryption-cybersecurity [Accessed 15 February 2018].

Twitter, 2016. *Developer Policies to Protect People's Voices on Twitter.* [Online] Available at: https://blog.twitter.com/developer/en_us/topics/community/2016/developer-policies-to-protect-peoples-voices-on-twitter.html [Accessed 15 February 2018].

Twitter, 2016. *Developer Policies to Protect People's Voices on Twitter.* [Online] Available at: https://blog.twitter.com/developer/en_us/topics/community/2016/developer-policies-to-protect-peoples-voices-on-twitter.html [Accessed 15 February 2018].

United States Air Force, 2006. *Cyberspace.* [Online] Available at: http://www.af.mil/About-Us/Speeches-Archive/Display/Article/143968/cyberspace-as-a-domain-in-which-the-air-force-flies-and-fights/ [Accessed 15 February 2018].

US House of Representatives, 2016. *Review of the Unauthorised Disclosures of Former National Security Agency Contractor Edward Snowden,* s.l.: US House of Representatives.

US House of Representatives, 2016. *Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden,* s.l.: US House of Representatives.

US House of Representatives, 2016. *Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden,* s.l.: US House of Representatives.

US Justice Department, 2016. *FBI escalates war with Apple: 'marketing' bigger concern than terror.* [Online] Available at: https://www.theguardian.com/technology/2016/feb/19/fbi-apple-san-bernardino-shooter-court-order-iphone [Accessed 15 February 2018].

US Justice Department, 2016. *FBI escalates war with Apple: 'marketing' bigger concern than terror.* [Online] Available at: https://www.theguardian.com/technology/2016/feb/19/fbi-apple-san-bernardino-shooter-court-order-iphone [Accessed 15 February 2018].

US Researchers in Cryptography and Information Security, 2014. *An Open Letter from US Researchers in Cryptography and Information Security*. [Online] Available at: http://people.csail.mit.edu/rivest/pubs/Ax14.pdf [Accessed 15 February 2018].

US Researchers, 2014. *An Open Letter from US Researchers in Cryptography and Information Security.* [Online] Available at: http://masssurveillance.info/ [Accessed 15 February 2018].

Utz, S. & Kramer, N. C., 2009. The privacy paradox on social network sites revisited - The role of individual characteristics and group norms. *Journal of Psychosocial Research on CyberSpace: CyberPsychology,* 3(2).

Vales, T. P., 2016. Brazil´s cyberspace politics: Combining emerging threats with old intentions. *IAPSS Political Science Journal,* 29(1), pp. 295-309.

Vaughan-Williams, N., 2007. The Shooting of Jean Charles de Menezes: New Border Politics?. *Alternatives,* 32(2), pp. 177-195.

Verton, D., 2003. *Black Ince: The invisible threat of cyber-terrorism.* s.l.:McGraw-Hill Osborne.

Vlissidis, P., 2016. *Paul Interview* [Interview] (30 March 2016).

Vultee, F., 2010. Securitization - A new approach to the framing of the 'war on terror'. *Journalism Practice,* 5(1), pp. 33-47.

Waever, O., 1989. *Security, the Speech Act - Analysing the Politics of a Word,* s.l.: Centre of Peace and Conflict Research.

Waever, O., 1995. Securitisation and Desecuritisation. In: *On Security.* s.l.:Columbia University Press.

Waever, O., 2014. *On Securitisation Theory.* [Online] Available at: https://www.youtube.com/watch?v=wQ07tWOzE_c [Accessed 15 February 2018].

Waldron, J., 2003. Security and liberty: the image of balance. *Journal of Political Philosophy,* 11(2), pp. 191-210.

Wallace, B., 2013. *Google and Facebook are 'bigger risk to privacy than state snooping': Parliament told internet giants are 'harvesting' data.* [Online] Available at: http://www.dailymail.co.uk/news/article-2482813/Google-Facebook-bigger-risk-privacy-state-snooping.html
[Accessed 15 February 2018].

Wallace, B., 2013. *Google and Facebook are 'bigger risk to privacy than state snooping': Parliament told internet giants are 'harvesting' data.* [Online] Available at: http://www.dailymail.co.uk/news/article-2482813/Google-Facebook-bigger-risk-privacy-state-snooping.html
[Accessed 15 February 2018].

Washington Post, 2013. *Google encrypts data amid backlash against NSA spying.* [Online]
Available at: https://www.washingtonpost.com/business/technology/google-encrypts-data-amid-backlash-against-nsa-spying/2013/09/06/9acc3c20-1722-11e3-a2ec-b47e45e6f8ef_story.html?utm_term=.2d13a42bbdc5
[Accessed 15 February 2018].

Washington Post, 2013. *How we know the NSA had access to internal Google and Yahoo cloud data.* [Online] Available at: https://www.washingtonpost.com/news/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/?utm_term=.2ee944dc41a7
[Accessed 15 February 2018].

Washington Post, 2013. *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program.* [Online] Available at: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.0474134380e9
[Accessed 15 February 2018].

Washington Post, 2014. *Apple, Facebook, others defy authorities, increasingly notify users of secret data demands after Snowden revelations.* [Online] Available at: https://www.washingtonpost.com/business/technology/apple-facebook-others-defy-authorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html?utm_term=.0089338d3c39
[Accessed 15 February 2018].

Washington Post, 2017. *NSA officials worried about the day its potent hacking tool would get loose. Then it did.* [Online]
Available at: https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html?utm_term=.e7a2389742d1
[Accessed 15 February 2018].

Watson, S. D., 2012. 'Framing' the Copenhagen School: Integrating the Literature on Threat Construction. *Millenium: Journal of International Studies,* 40(2), pp. 279-301.

Webb, A. & Wang, S., 2016. *Apple's Cook Picks Up Where Snowden Left Off.* [Online]
Available at: https://www.bloomberg.com/news/articles/2016-02-29/apple-s-cook-picks-up-where-snowden-left-off-in-privacy-debate
[Accessed 15 February 2018].

Weimann, G., 2016. Going Dark: Terrorism on the Dark Web. *Studies in Conflict and Terrorism,* 39(3), pp. 195-206.

Weinstein, M., 2014. *Is Silicon Valley More Dangerous to Your Privacy Than the NSA?.* [Online]
Available at: https://www.huffingtonpost.com/mark-weinstein/silicon-valley-privacy-concerns_b_5483008.html
[Accessed 15 February 2018].

WhatsApp, 2016. *end-to-end encryption.* [Online]
Available at: https://blog.whatsapp.com/10000618/end-to-end-encryption
[Accessed 15 February 2018].

White, R., 1984. *Fearful Warriors: A psychological profile of U.S.-Soviet relations.* 1 ed. s.l.:Free Press.

Williams, M. C., 2003. Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly,* 47(4), pp. 511-531.

Williams, M. C., 2011. Securitisation and the liberalism of fear. *Security Dialogue,* 42(4-5), pp. 453-463.

Williams, M. C., 2011. Securitization and the liberalism of fear. *Security Dialogue,* 42(4-5), pp. 453-463.

Winder, S., 2006. *The Man Who Saved Britain.* Main Market Edition ed. s.l.:Picador.

Windsor, P., 1990. *Reason and History or only a History of Reason?.* s.l.:The University of Michigan Press.

Wired, 2010. *Exclusive: Google, CIA Invest in 'Future' of Web Monitoring.* [Online]
Available at: https://www.wired.com/2010/07/exclusive-google-cia/
[Accessed 15 February 2018].

Wired, 2016. *The Father of Online Anonymity has a plan to end the Crypto Wars.* [Online]
Available at: https://www.wired.com/2016/01/david-chaum-father-of-online-

anonymity-plan-to-end-the-crypto-wars/
[Accessed 15 February 2018].

Wispe, L., 1968. Sympathy and Empathy. In: D. L. Sills & R. K. Merton, eds. *The International Encyclopedia of Social Science.* 15 ed. New York: Macmillan and Free Press, pp. 441-6.

Wizner, B., 2016. *Privacy experts fear Donald Trump running global surveillance network.* [Online]
Available at: https://www.theguardian.com/world/2016/nov/11/trump-surveillance-network-nsa-privacy
[Accessed 15 February 2018].

Woods, A. K., 2016. *Encryption Substitutes,* s.l.: Hoover Institute.

World Summit on the Information Society, 2003. *Declaration of Principles.* [Online]
Available at: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html
[Accessed 11 February 2016].

Wray, B., 2015. *35 academics sign letter calling for transparency in new UK Government data surveillance proposals.* [Online]
Available at: https://www.commonspace.scot/articles/1439/35-academics-sign-letter-calling-transparency-new-uk-government-data-surveillance
[Accessed 15 February 2018].

Yoon, P. Y., 2016. *It's hypocritical to expect to have it both ways, Mr Zuckerberg.* [Online]
Available at: https://www.ft.com/content/8f8eef46-f2a9-11e5-9f20-c3a047354386
[Accessed 15 February 2018].

YouGov, 2013. *Public opinion and the Intelligence Services.* [Online]
Available at: https://yougov.co.uk/news/2013/10/11/british-attitudes-intelligence-services/
[Accessed 15 February 2018].

YouGov, 2014. *People in Britain divided over use of torture.* [Online]
Available at: https://yougov.co.uk/news/2014/12/11/people-in-Britain-divided-over-use-of-torture/
[Accessed 15 February 2018].

YouGov, 2015. *GCHQ, resource and capability to intercept, invasion of privacy.* [Online]
Available at: https://yougov.co.uk/news/2015/03/13/gchq-resource-and-capability-intercept-invasion-pr/
[Accessed 15 February 2018].

YouGov, 2016. *Terrorist attack in Britain expected by 84% of people.* [Online]
Available at: https://yougov.co.uk/news/2016/08/04/terrorist-attack-britain-expected-84-people/
[Accessed 15 February 2018].

YouGov, 2016. *UK is Europe's favourite tech centre for global tech professionals.* [Online]

Available at: http://www.londonandpartners.com/media-centre/press-releases/2016/20160310-uk-is-europes-favourite-tech-centre-for-global-tech-professionals
[Accessed 15 February 2018].

Zimmerman, P., 1995. *PGP Source Code and Internals.* 1 ed. s.l.:MIT Press.

Zovi, D. D. et al., 2016. *Brief of amici curiae iPhone security and applied cryptography experts in support of apple INC.'s motion to vacate order compelling apple Inc. to assist agents in search, and opposition to government's motion to compel assistance,* s.l.: United States District Court Central District of California Eastern Division.

Zuboff, S., 1989. *In The Age Of The Smart Machine: The Future of Work and Power.* s.l.:Basic Books.

Zuckerberg, M., 2014. *Mark Zuckerberg.* [Online] Available at: https://www.facebook.com/zuck/posts/10101301165605491 [Accessed 15 February 2018].

ACKNOWLEDGEMENTS

My sincere thanks to Professor Pete Adey and Professor Keith Martin for their continuous support, mentoring and patience throughout this research. I hope it has been as much a journey of discovery for you as it has been for me.

Many thanks to the Information Security Group, the Department of Geography and the Centre for Doctoral Training in Cyber Security at Royal Holloway for providing the resources, expertise and ideas that have helped shape my research. It was a privilege to have spent a period of my life working within these departments.

Thanks to the EPSRC for funding my PhD and the whole of the CDT programme. It really is a wonderful way to study. Thanks also to GCHQ, Open Rights Group and Shine TV for facilitating this research and participating in my interviews and ethnographic work.

Finally, and most importantly a million thanks to my patient wife Felicity, who wisely ensured we continued living our lives despite the all-consuming nature of thesis writing. PhD's are a marathon, but I never expected to be married with 3 children by the time I had finished.