A Critical Reflection on the Construction of the Cyberterrorist Threat in the United Kingdom of Great Britain and Northern Ireland

by Gareth Mott
Department of Politics and International Relations

A thesis submitted in partial fulfilment for the degree of Doctor of Philosophy at Nottingham Trent University

April 2018

Acknowledgements

This thesis would not have been possible without the scholarship generously provided by the department of Politics and International Relations at Nottingham Trent University. I am extremely grateful to the department, the school, and the university for entrusting me with this funding.

Before embarking on this PhD, I devoured several books along the lines of Phillips's and Pugh's (1994) *How to Get a PhD*. This was a bit like typing ailments into a search engine. Some students are lucky with the supervisory teams that they are landed with, others unlucky. I am fortunate to count myself in the very lucky cohort. Thank you, to my supervisory team, Dr Christopher Baker-Beall and Professor Matt Henn. You were instrumental in this project and in providing me a wealth of opportunities and guidance at Nottingham Trent University.

I would also like to thank Professor Lee Jarvis, not only for supervising my Master's dissertation at the University of East Anglia, but additionally for your encouragement in making an application to Nottingham Trent University and guidance in doing so. Had you not advised me of the available scholarship and encouraged me to apply, it is unlikely that I would have embarked on a PhD; I'd probably be selling car insurance!

Of course, thanks must be paid to Karen and Richard, my parents, whose patient parenthood I will always be grateful for.

Lastly – and I think I can get away with this in a cyber threat thesis! – I would like to thank my '88 US IBM Model M keyboard. Your mechanical keys have been irritating housemates and neighbours for years, but the clacks are music to my ears. You have seen me through my A-levels, my Bachelor's degree, my Master's degree and, hopefully, my PhD. Someday, I will let you retire. But not quite yet. Let's write a book together.

A Critical Reflection on the Construction of the Cyberterrorist Threat in the United Kingdom of Great Britain and Northern Ireland

Abstract

Cyberterrorism has not occurred. Furthermore, the definitional parameters of cyberterrorism have not been conclusively defined by either policymakers or academia. However, in 2010 the threat posed by the terrorist application of cyber weaponry to target British critical national infrastructure became a 'Tier One' threat to the UK. This thesis is the first comprehensive mapping and analysis of the official British construction of the threat of cyberterrorism between 12th May 2010 and 24th June 2016. By using interpretive discourse analysis, this thesis identifies 'strands' from a comprehensive corpus of policy documents, statements and speeches from Ministers, MPs and Peers. This thesis examines *how* the threat of cyberterrorism was constructed in the UK, and what this securitisation has made possible. In addition, this thesis makes novel contributions to the Copenhagen School's 'securitisation theory' framework. Accordingly: this thesis outlines the framework for a 'tiered', rather than monolithic audience; refines the 'temporal' and 'spatial' conditioning of a securitisation with reference to the unique characteristics of cyberterrorism; and lastly, details the way in which popular fiction can be ascribed agency in securitising moves to 'fill in' a lack of case studies of threat with gripping vicarious fictional narratives. It is identified that the 2010 British Coalition Government's classification of cyberterrorism as a 'Tier One' threat created a central strand upon which a discursive securitisation was established. Despite the absence of a 'cyberterrorist' incident across the period under scrutiny, the securitisation did not recede. The threat posed by cyberterrorism was articulated partially within a 'New Terrorism' frame, and it was deemed by Ministers, MPs and Lords to be a threat that was likely to escalate in both severity and possibility over time. A notable finding is the positioning of the securitisation against a particular 'cyberterrorist' identity epitomised by social *actors* using cyberspace, rather than the tangible environments of cyberspace.

Table of Contents

Chapter One: Introduction

Introduction

Following the establishment of a functional world-wide-web in 1990, the UK, along with international society at large, has become increasingly interconnected. Worldwide, there are roughly 3.58 billion people who regularly use the services of the world-wide-web (Statista, 2018). In the UK, 89% of adults were been identified as regular users of the internet (ONS, 2017). The number of devices connected to the internet has increased exponentially, and this is a trend set to continue; fuelled by the huge financial and capital investment into IT spending, which totalled $3.7 trillion in 2013 (Whitney, 2013). Consumer demand is also a significant force driving the proliferation of internet access, in part due to innovation that has produced increasing layers of 'killer programs'; computer programs that are highly desirable and perhaps necessary for modern living. Email and browser-based access to the world-wide-web are examples of such 'killer programs', but increasingly these extend beyond computers and mobile phones amidst the expansion of the 'Internet of Things'. Put simply, this ‘Internet of Things’ is the process in which physical objects such as refrigerators, ovens, heating systems and pet feeders can be embedded with electronics and software that permits them to both collect and exchange data, and to be controlled remotely. A study by Cisco has suggested that more than 50 billion 'things' will be connected to the internet by 2020 (Tillman, 2013).

The integral value of online services for economic prosperity is clear. Online services are so embedded into the functioning of modern society that any attempt to calculate the true 'value of the internet' would be perfunctory, although tentative figures are offered to contextualise analysis in Chapter Five. However, connectivity does not come without risk. Hacking, a term previously the preserve of students engaging in problem solving or practical jokes – not necessarily in electronic form – globally became increasingly legislated against in the 1980s and 1990s, and some forms of hacking have since constituted a criminal offence, thus integrating 'hacking' into a 'cybercrime' lexicon.

As the international economy rapidly became increasingly reliant on internet-mediated connectivity over the course of the 1990s and early 2000s, a malicious economy emerged, seeking to exploit vulnerabilities for financial gain. A *Center for Strategic and International Studies* report, sponsored by

McAfee, estimated that the likely annual cost to the global economy implicated by cybercrime exceeds $400 billion (McAfee, 2014). An estimate of levels of cybercrime was included in the national Crime Survey for England and Wales for the first time in 2015, immediately inflating the headline crime rate by 40% (Travis, 2015).

Nevertheless, cybercrime is not merely represented as a matter of criminality; indeed, the phenomenon is also considered to be a pressing concern for the national security of the UK. "Cyber attack, including by other states, and by organised crime and terrorists" was listed as a Tier One threat under the 2010 *National Security Strategy* (Cabinet Office, 2010a:11). The 2015 *National Security Strategy* notes that "the range of cyber actors threatening the UK has grown … non-state actors, including terrorists … can use easily available cyber tools and technology for destructive purposes" (Cabinet Office, 2015a:19). The 'Tier One' label is used to classify threats that are deemed to be of high probability and high impact. As a discursive tool, the 'Tier One' label is therefore of interest to practitioners of the Copenhagen School's 'securitisation theory'. This thesis is concerned with the official British discourse of the threat of cyberterrorism, a threat that has yet to occur. The term cyberterrorism gained traction amidst a post-Cold War re-evaluation of security threats, and an increased awareness of society's reliance on internet infrastructure (Whiting, 2013). However, cyberterrorism acquired greater prominence following 9/11, during a period of re-imagining of potential terrorist threats. The labelling of particular identities in cyberspace as 'threatening' legitimises public policies and expenditures in the furtherance of national security. In a July 2014 announcement by David Cameron, the then-British Prime Minister, he stressed that part of his £1.1 billion investment in the armed forces was designated for the specific purposes of combating 'unseen' cyber threats (Dominiczak, 2014).

The next section outlines the thesis aims and research question that underpin the analysis of this thesis project.

Thesis Aims and Research Questions

This thesis critically examines the British discourse of cyberterrorism, specifically for the purposes of revealing how a threat – real, in the sense that it has been socially constructed – but latent, because it has

not yet occurred, exists as a securitised phenomenon and has successfully maintained this securitised status over time. Through this process, this thesis will extend understanding regarding *how* a threat can be securitised. Without wishing to risk a recourse to generalisation, it is perhaps fair to suggest that most securitised threats maintain their status through 'events' and the discursive remembering and re-living of those events. Cyberterrorism is therefore novel because it has been 'spoken' into existence (Conway, 2005), and this novelty is further compounded because the public-facing 'speaking' of a threat of cyberterrorism has been conducted by politicians, authors and academics, but *not* proscribed terrorist organisations.

'Securitisation' is not a banal process involving rhetorical tools or arbitrary bureaucratic decisions. As will be detailed later in this thesis, securitisations entail 'extraordinary measures', which can be costly to a state's budgetary financing and can, context dependent, result in the criminalisation of individuals who would otherwise avoid sentencing. In some cases, the extraordinary measures justified through a securitisation can even entail the killing of individuals who would, in other circumstances, have enjoyed many more years of their natural lives. I empathise with calls for normative approaches to the study of security. Like many others engaged in the field of Security Studies, I am drawn to this endeavour because security is a universal desire – indeed, a fundamental right – for everyone. Securitisation, like Security Studies more broadly, engenders moral considerations. In discussing a securitised discourse, one almost inescapably assumes a role as a fire-lighter on an alarmist beacon, relaying and re-constituting a justification for a status of securitisation that may, or may not be, warranted. An unchecked engagement with a securitised discourse would ostensibly fuel a perception that immediate and undemocratic state-level action is the only viable method for the alleviation of security concerns (Charrett, 2009). By definition, a securitisation entails the curtailment of open and accountable government, and serves to mitigate democratic principle (Roe, 2012:252). The key, therefore, is to acknowledge that *some* re-publication of a phenomenon with potentially negative externalities is unavoidable, but also to simultaneously ruthlessly and consistently apply a critical lens. This critical lens facilitates the development of the 'new thinking' that assists the academic community in raising awareness of the subjectivities inherent within security discourses, that serve to regenerate particular political 'otherings' (Charrett, 2009:32). Theories are inherently subjective entities; as Cox states, there is "no such thing as theory in itself, divorced from a standpoint in time and space" (1981:128; 1986:207).

As Floyd (2007:338-339) has suggested, writing in a consistently critical manner permits one to critically evaluate one's own discursive engagement with security. The overarching ethos of this thesis is *not* normative – simply critical – but by opening the securitisation and scrutinising its constitutive strands, it is possible that weakness or deficiencies in the logic of the securitisation of cyberterrorism may be located. These deficiencies could provide an epistemic basis for counter-securitisation. Counter-securitisation is a concept that has been elucidated in an article by Stritzel and Chang, who suggest that counter-securitisations are "part of an interactive process of moves and counter-moves that are both linguistically regulated by the grammar and illocutionary logic of securitising speech acts and closely tied to processes of legitimisation and delegitimisation" (2015:552). This resistance against the (re)legitimisation of a securitisation could arise from a 'securitising agent', or, feasibly, from the audience that serves to either accept or reject a given securitisation. Whilst securitisation, as a process of security politics, can provide the fastest guarantor of security in extremis, it is a fundamentally undemocratic phenomenon. Consequently, even in circumstances where a securitisation may provide *some* guarantee of security, it is possible that this could be outweighed by the negative externalities a securitisation imposes on society and its functions. Furthermore, some *types* of threat may be more amenable to securitisation than others. For instance, a large asteroid that is expected to strike a large British city at a given date and time is quite a different threat to the perception of a ubiquitous, strike-at-any-time terrorist threat.

This thesis analyses the official UK discourse of the threat of cyberterrorism. The research questions underpinning the thesis are detailed as follows:

1. How has official discourse in the UK represented the threat posed by cyberterrorism to the UK?
2. How do securitising actors and members of the audience securitise a threat that does not exhibit a historical precedent?
3. Given that a cyberterrorist incident may not be attributable, could be delivered in a near-instantaneous fashion, and would rely on a man-made 'fifth sphere' of power, what novel contributions for the framework of securitisation theory, if any, can be inferred from this socially-constructed threat?

The remainder of this chapter introduces the fields of Critical Terrorism Studies and Critical Security Studies. These critical approaches possess efficacy for the analysis of cyberterrorism, because this is a discursively-constructed threat that has minimal, if any at all, public-facing objective data regarding its likelihood or potential for harm. There is also a relative dearth of current material applying critical approaches to the issue of cyberterrorism, either in a British or indeed an international context. This thesis is intended to partially address this deficiency in the study of official discourses of cyberterrorism, whilst contributing to the continued refinement of the Copenhagen School's securitisation theory. This introductory chapter will also include a brief overview of the remaining chapters contained in this thesis.

Critical Terrorism Studies

In the endeavour to engage with the discourse surrounding threat to the UK posed by cyberterrorism, I adopt an approach that aligns with the field of Critical Terrorism Studies. At present, there are few bona fide cases where a critical approach has been brought to bear in the study of cyberterrorism. This is a deficiency that warrants addressing. Critical Terrorism Studies is an established sub-discipline of Terrorism Studies that seeks to address significant analytical and normative limitations in Traditional Terrorism Studies literature. It has been suggested that such traditional literature typically operates with a narrowly essentialist framework that neglects the processes of terrorism's construction and serves to constrain opportunities to discuss the (il)legitimacy of particular instances of violence (Jarvis, 2009). Traditional Terrorism Studies, if one can term it as such, has been criticised for being relatively ignorant regarding the application of theory; indeed, prior to the emergence of Critical Terrorism Studies, engagement with conceptual issues was typically confined to matters of definition (Miller, 2011:146-147). In the obfuscation of the terrorist's status as a social construction, the Traditional Terrorism Studies field focuses on the terrorist actor to the extent that it disregards the processes through which that individual acquired a label for their specific brand of political violence. On this basis, Hulsse and Spencer (2008) argue that the terrorist actor can no longer be the primary unit of analysis. As Baker-Beall writes, the counter-terrorism discourse is based upon, and contributes to, the re-articulation of “an 'accepted knowledge' about what terrorism is, who the terrorists are, and what type of threat they represent” (2016:30). Through this critical lens, it would be misguided to take discourse as a

social fact that draws upon a plethora of fixed social facts. Rather, discourse is a fluid phenomenon that warrants scrutiny, because discourse inevitably entails the attribution and action of power relations. Furthermore, it would be poor practice to assume that there is just 'one discourse' on a subject or issue at any given instance; rather, there will be many discourses operating simultaneously. Even within governmental discourses, determining which actors and agencies speak with the 'official' voice can prove difficult, particularly if administrative wings are in contention. Chapter Two will introduce a novel ‘Pantomime’ framework of securitisation, which it is hoped can accommodate contestation, inconsistencies and contradictions in a given securitisation.

In what has been termed an 'epistemological crisis', this tendency – for meanings of terror to be malleable – has real-term consequences for the direction of counterterrorism policy (Jackson, 2015). Misguided judgements, made by either scholars or policy makers, concerning fundamental questions such as ‘what is a terrorist?’, or ‘what constitutes an act of terrorism or a will to terrorise’, have the effect of fuelling an environment in which poor policy decisions are likely to be made. In today's socio-political climate in the UK, the application of the label 'terrorist' carries enormous weight. The delineation between what does and does not constitute terrorism is a significant element of contemporary security politics. In the Terrorism Studies field, whole sections – or even chapters – entitled “Defining Terrorism” are so commonplace throughout articles and books that their appearance seems somewhat cliché. I do not say this to be tongue-in-cheek, or to disparage such efforts – indeed, reflection on definition is an earnest project – but an alternative approach is to recognise that definitions and interpretations of terrorism will always be intersubjective. A ‘true’ definition of cyberterrorism is a simulacrum. Another cliché – that “one person's terrorist is another person's freedom fighter” – is obviously a crude and over-simplified argument, but it aptly identifies the mechanics of this conceptual conundrum.

It has been said that there are more than 100 definitions offered for terrorism (Weimann, 2005:132). In a slightly satirical manner, Tucker suggests that “above the gates of hell there is the warning that all that enter should abandon hope … less dire but to the same effect is the warning given to those who try to define terrorism” (1997:51). Cyberterrorism has inevitably inherited the conceptual challenges of definition that surrounds attempts to ascertain a universal definition of terrorism more broadly. As Jarvis, Nouri and Whiting note, “although [cyberterrorism as a term] has existed for over 30 years now, there remains very

little consensus on many of the fundamental questions surrounding this term" (2014; see also Jarvis and MacDonald, 2015). To some empirically-centric scholars, the search for an objective, fixed definition of terrorism is key, and in their view, the seeming inability of the Terrorism Studies field to cogently determine such a definition is a dour failure (Schmid and Jongman, 1988). Meisels urged that "terrorism ought to be strictly defined … it is too central a concept to the moral understanding of our contemporary world to remain obscure" (2009:348). Whilst the "you will know it when you see it" approach to labelling a terrorist incident appears to lack both academic and empirical rigour, the project to find a universal understanding of terrorism is considered by many in the Critical Terrorism Studies community to be defunct (Douglass and Zulaika, 1990; Erlenbusch, 2010; Jackson, 2007). This is *not* to imply that the Critical Terrorism Studies approach to the critique of (counter)terrorism discourse upholds a perception that terrorism does not exist as an avenue of violent resistance. Rather, proponents of Critical Terrorism Studies argue that there exists a misapplication of a terrorism label by governments – including the British Government – wherein legitimate forms of resistance, insurgency, or civil conflict are inappropriately termed incidents of terrorism (Erlenbusch, 2014).

This will-to-(mis-)label may be exerted as a means through which a government can legitimise its own (potentially terrifying) acts of violence and disruption. Examples of such acts of violence and disruption include the invasion of Afghanistan in 2001, the 2014 parliamentary support for the air-bombing of ISIS targets in Syria, the domestic power of detention without charge for up to 28 days under the 2006 modification to the *Terrorism Act*, and the *Investigatory Powers Act* of 2016. In the will-to-(counter)terrorise, the misuse of power can extend beyond a counterterrorism mandate. This was highlighted in the case of the detention of David Miranda, the partner of the investigative journalist, Glenn Greenwald[1], for nine hours under Schedule 7[2] of the *Terrorism Act* 2000. This detention had been undertaken in an attempt to seize documents leaked by the former NSA private contractor, Edward Snowden. An initial legal challenge by Miranda against this detention failed in the High Court in 2014 (Travis Taylor and Wintour, 2014), but an appeal in 2016 resulted in a verdict in favour of the detention but *against* the application of Schedule 7 in an effort to prise journalistic material, as this was considered incompatible with the Human Rights Act

[1] A former journalist for the US-wing of the *Guardian* newspaper. Glenn was one of two journalists contacted by Edward Snowden, and who flew to Hong Kong in 2013 to retrieve documents pertaining to the illegal online snooping and hacking committed American and British intelligence services, and the forced coercion of private communications companies including Google, Microsoft and Yahoo.

[2] Schedule 7 allows British police to stop, examine and search passengers at points of entry to the UK. 'Reasonable suspicion' of involvement in terrorist activity is not required.

(Bowcott, 2016). Invariably, for those who object to overreach by the state, such a misuse of power in the name of hampering the whistle-blowing of pre-existing abuses of power is a rallying call for Critical Terrorism Studies.

As Richard Jackson (2012:9) has suggested, Western discourses have exhibited a 'knee-jerk' reaction to terrorist incidents, viewing the phenomenon of terrorism in a de-contextualised manner, in which attention is both commanded and shaped by incidents as and when they occur. One consequence of this de-contextualised lens is that violent acts are classed as 'terrorism', often without due examination of the intentions of the perpetrators. An implicit assumption may be made; that is, it is presumed that the primary audience envisaged by the perpetrators were *not* the immediate victims (Richards, 2014). Perhaps the most accessible approach to defining terrorism is to regard it as a 'social construct' (Ramsay, 2015:211), a linguistic tool that contains implicit inferences of power and (il)legitimate uses of violence. Terror, manifest as an emotion, is arguably universal, a natural part of the trauma associated with threats to one's existence, but the labels of 'terrorist' and 'terrorism' inevitably mean differing things to different people, and will be applied in seemingly inconsistent instances.

In parts of this thesis, reference is made to the 'War on Terrorism'. It is worth taking a moment to pause and justify one's re-publication of this term. The term 'War on Terrorism' had been used as a frequent descriptor during the course of the George W. Bush administration, and naturally the term gained at least some traction within British media discourse. However, the Barack Obama administration (relatively) quickly dispensed with the phrasing – in a public announcement by John Brennan – stressing that the US was at war with Al-Qaeda only (Ward, 2009). Consequently, I acknowledge the risk of re-publicising the term, 'War on Terrorism' beyond its 'best-before-use date' could constitute a contribution to the (re)securitisation of terrorism. Further consideration regarding this issue of (re)securitisation will appear later in this chapter. I justify this continued re-publication because whilst the overt language of war may have dissipated, the wartime processes remain; police forces in the UK are increasingly militarised (BBC News, 2016; Whitehead, 2016), at present there are British airplanes aggressively bombing targets in Iraq and Syria specifically in an anti-terror endeavour (The Telegraph, 2016), and there is little sign of any incoming official curtailing of the surveillance apparatus. Furthermore, the 'War on Terror' mentality has, to some extent, been ingrained into the psyche of the public. Newspapers with a high newsprint readership and online presence,

such as the *Daily Mail*, continue to use the term 'War on Terror' in news headlines (for instance, see Schwab, 2015). The public also appears to endorse militaristic action against terrorist groups – specifically the so-called Islamic State – indicated in a November 2015 poll for *The Times*, in which a majority of respondents supported the concept of a US-UK ground-force coalition in both Iraq and Syria (Dahlgreen, 2015).

To sum, Critical Terrorism Studies forms a central component of the methodology applied in this thesis; this methodology will be discussed explicitly in Chapter Three. Discourse is central to the construction of any threat, but in the case of cyberterrorism it is official British discourse that has led to the securitisation of this threat in the UK. This does not necessitate that empirically-centred approaches to Terrorism Studies, utilising fixed meanings of 'terrorism' and 'terrorists', do not possess potential in the study of the threat of cyberterrorism. However, a critical approach is the most apt means by which to assess *how* a threat that has not occurred has been securitised.

Critical Security Studies

This thesis is underpinned by an application of – and contribution to – securitisation theory. This thesis examines the threat of cyberterrorism to the UK through the lens of Critical Security Studies, and this represents an approach to accessing the discourses of cyberterrorism that has thus far received limited attention. Of course, the research conducted by Jarvis and MacDonald, as well as the Cyberterrorism Project more broadly, represents a notable exception[3].

Critical Security Studies has developed, partly, as a critique of the historically dominant Structural Realist approach to the study of security. During the Cold War; a period in which formal studies of 'international security' came to the foreground of international politics, Structural Realism was the overriding vanguard of the field, championed by leading figures such as Kenneth Waltz (1990; see also Hall, 2013). This agenda sought to focus on what it held to be the most significant questions pertaining to international relations; that is, matters of direct nation-state security, and quantitative reflections on the state of nature in which states reside. Stephen Walt (1991) argued that studies outside of this paradigm could be regarded as 'counterproductive tangents', which, if engaged with, would diminish the practical value of Security Studies.

[3] See http://www.cyberterrorism-project.org/

Perhaps this phenomenon can be attributed to the political and geopolitical context that surrounded the emergence of contemporary Realist security thinking. Morgenthau (2005), as an influential Classical Realist scholar and one of the founding fathers of the international relations discipline, described the condition of the international system that he saw in the post-1945 world in dour terms. In some respects, one can observe how he was motivated to write by fear; indeed, he seemed "very pessimistic about the capabilities of the USA and the Soviet Union to maintain international peace" (Griffiths, Roach and Solomon, 2009:53). For Morgenthau, "peace was not an analytical puzzle but a desperate hope" (Lebow, 1994:252). Such was Morgenthau's personal interest in the avoidance of conflict – which he believed resulted through human nature – that he "provided both an explanation [of international politics] and a road map" (Hoffman, 1987:76) for the management of American foreign policy. This focus on great-power conflict, and assumptions regarding the condition of the international system, has seemingly pervaded throughout Realist conceptions of security and historical discourse (Sluga, 1996:75).

Infamously, the Structural Realist approach to international security failed to predict, or adequately explain, the end of the Cold War and Gorbachev's role in unilaterally dismantling the Soviet superpower. This failure endorsed the notion that *ideas* must "be conceptualised as intervening variables between structural conditions and the definition of actors' interests and preferences" (Risse-Kappen, 1994:212,214). The structure of the international system cannot omnipotently control state (and non-state) behaviour; aptly described in Wendt's widely-cited proclamation that "anarchy is what states make of it" (1992:424). Through the ideational capacity of security actors within nation-states, it is fully possible for states to overcome the Structural Realist's security dilemma, given that it, in itself, is a social construction (Wendt 1995:73). Citing events such as the abolition of slavery, Finnemore and Sikkink have propositioned that empirical research repeatedly demonstrates "how people's ideas about what is good and what 'should be' in the world become translated into political reality" (1998:916). Operating in a 'marketplace of ideas' (Snyder and Ballentine, 1996), language "binds together what *is* and what *ought*" (Kowert, 2001:279). Security is a mercurial and intersubjective phenomenon. As Hopf notes, "since what constitutes a threat can never be stated as an a priori, primordial constant, it should be approached as a social construction of an Other" (1998:199).

In contrast to Walt's (1991:2013) warning that the inclusion of issues such as human health, wellbeing, and the surrounding environment would constitute an 'excessive' expansion of Security Studies,

members of the Critical Security Studies community maintain that expansion is both warranted and necessary. Structural Realist thinking implicitly takes the nation-state as its focal point of study, but as Booth (1991:320) aptly notes with the analogy of a house requiring maintenance; the upkeep of the property (the state) is illogical if it comes at an excessive cost to the inhabitants (the citizenry). Irrespective of the stature of the state, the security of the human beings within the state should be considered primary. The UN's 1994 *Human Development Report* marked a refreshing invigoration of this new approach to what had been termed 'human security' (1994).

If one upholds and respects the duty of social scientific inquiry to maintain relevance to society, the idea that the study of security should be intrinsically militarised makes little sense, given that many people are likely to never (personally) encounter armed conflict in their lifetime. Many citizens will only experience armed conflict vicariously, through popular computer games, film, documentary, news and literature; thus, whilst state-level armed conflict may indeed factor in their perceptions of the security or insecurity, other security considerations will also be present, and may be prescient. A recent novel trend in the Critical Security Studies field is the emergence of 'vernacular security', wherein the security concerns of citizens are sought. This can involve the application of a focus group methodology, and examples include articles written by Vaughan-Williams and Stevens (2015), and Jarvis and Lister (2012, 2013). Such studies have highlighted pertinent issues; for instance, the sense of profiling and associated negative externalities experienced by Islamic communities. Vernacular research has the potential for significant policy relevance; for instance, in the Vaughan-Williams and Stevens (2015) study, members of the public stated that they were reluctant to contact the Government's anti-terror 'hotline', because friends who had done so had quickly suffered police surveillance and repeated telephone calls for further information. Job prospects and housing issues appear to be a significant security concern that is raised in the cited focus groups, but the top-down militaristic approach to security fails to incorporate these issues aptly into an appropriate analysis. Inter-subjectivity is not a nuisance to be disregarded, but a bona fide tenet to be considered seriously. Ultimately, as Booth writes, “security is what we make it. It is an epiphenomenon, inter-subjectively created. Different world views and discourses about politics deliver different views and discourses about security” (1994:15-16). Burke has suggested that the use an approach aligned with Critical Security Studies “is to see security as an interlocking system of knowledge, representations, practices, and institutional forms that imagine, direct, and act upon

bodies, spaces and flows in certain ways – to see security not as an essential value, but as a *political technology*" (2002:2, original emphasis).

Critical Security Studies is not necessarily a monolithic project, and indeed, one can delineate the approach in both narrow (for instance, Booth, 2005) and broad terms (for instance, see Krause and Williams, 1997). The aims and ontologies of the narrow and broad approaches differ. The narrow approach, such as that applied by the Welsh School, accepts a set logic of security in order to consider the issue of human security and emancipation, but in this endeavour it applies less critique and de-construction than the broad approach (Browning and MacDonald, 2011:242). Whilst I would not wish at all to disparage Booth's inspiring work on security and emancipation, this thesis aligns with the broad approach to Critical Security Studies; an approach that incorporates a range of "analyses drawing on elements of Marxism, Feminism, Critical Theory, Critical Constructivism and Post-Structuralism" (Browning and MacDonald:238). Krause and Williams have written of the paradox wherein it "may be necessary to broaden the agenda of Security Studies (theoretically and methodologically) in order to narrow the agenda of *security* (1996:249, original emphasis). In essence, in order to understand more explicitly the processes of a given security issue, and *how* that process occurs, one needs to move beyond the state-as-referent-object narrative of the Structural Realist community.

The Critical Security Studies approach to the study of cyberterrorism is pertinent, for several reasons, which will be briefly outlined here. Firstly, almost all commonly-found definitions of terrorism do *not* hold legitimate governments or institutions of nation-states to be culpable as terrorists; they are capable of causing atrocities, great crimes, and acts of war, but not acts of terror. Consequently, when we engage with the discourse of cyberterrorism, this is not a discourse of a structural, state-on-state violence, but rather, it is one of non-state actors causing violence against another entity. Furthermore, this entity-to-be-attacked is unlikely to be a nation-state per se (although the discourse may represent it as such); but rather it would be privately-owned assets, for instance, banks, telecommunication systems or power-grid systems. Cyberterrorism has not occurred during the time period scrutinised in this thesis, nor at the time of writing. This is a threat that has been discursively-created, and it is reasonable to presume that this discourse is *doing* something. Clearly, discourse is key, and it is through a Critical Security Studies approach that one can assess the implications of discourse for the British comprehension of the threat of cyberterrorism.

The next section considers the matter of defining cyberterrorism.

Defining Cyberterrorism and Cyberspace

It is not controversial to suggest that cyberterrorism is an example of a buzzword in the contemporary security lexicon. Certainly, the term has become popular within the news media in the years following the terrorist attacks against the World Trade Center and Pentagon in September 2001 (Gordon and Ford, 2002; Jones, 2005:7). As Weimann notes, "cyberterrorism, the media have discovered, makes for eye-catching copy" (2005:131). However, associated with the ease with which observers can apply a mercurial reading of what cyberterrorism *is*, the media has a habit of conflating cyberterrorism with the more generic entity of cybercrime (Ahmad and Yunos, 2012; Berner, 2003). Taliharm observes that "referring to various cyber incidents without full awareness of the opposing meanings of the concept has led to an unfortunate outcome of technological confusion and the media inadvertently encouraging the belief that any slightly eminent … cyberattack could be an act of cyberterrorism" (2010:62-63). The source of the popularity of the term cyberterrorism is perhaps not difficult to ascertain; the word combines two eye-catching phrases, 'cyber' and 'terrorism' respectively. When used as a prefix, cyber simply denotes an online activity; in essence, a modem must be involved (Iqbal, 2004). That being said, cyber can also be considered a verb. In the mid to late 1990s, to 'cyber' was to partake in online chatroom sex, although the usage of the term in this way now seems dated. However, as O'Connor states, regarding cyber there is "always action, movement, evolving motivations, adventure and interaction … it's impossible to just *be* cyber … there's no steady state of being cyber" (2011).

Cyberspace – invariably the environment in which cyberterrorists operate – is a global sphere of power, in a similar sense to land, sea, air and space, but it is differentiated by its perceived ethereal nature. In pragmatic terms, no one country or geographical entity can be denoted as a 'cyberisland' (Aaviksoo, 2010). Cyberspace "is an intangible, fluid and counterintuitive phenomenon that defies the neat categorisations of the other strategic domains" (Sheldon, 2012:3,13). Cyberspace is also distinct in terms of the possibility for it to be constantly replicated (Libicki, 2007). One can further distinguish cyberspace from the other spheres of power because of its mercurial nature; whilst the fundamental characteristics of our land, sea, air and space

have remained relatively unchanged through history, we must acknowledge that cyberspace has no natural tendency, and that it is an environment that "morphs in continuous tension, creating new forms of agency that in turn produce effects that shape the internet itself" (Deibert and Rohozinski, 2008:147). The British Government currently defines cyberspace as "an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services" (Cabinet Office, 2011:11).

Certainly, a characteristic of the cyber landscape is that it has changed drastically over a short space of time. For instance, Internet Protocol Version 4 (IPv4), dominant since its establishment in 1981, is running out of viable IP addresses, and is due to be gradually replaced by Internet Protocol Version 6 (IPv6). Users of the internet will have noticed that over the course of the last two decades, the modem that they use to connect to the world-wide-web has changed, and that the volume and speed of the traffic they exchange will have drastically increased. Today's ubiquitous ADSL and cable modems may eventually be replaced by satellite versions. Web services and websites can emerge, flourish, and then die so quickly that they almost seem to represent their own miniature cyber geologic periods. Indeed, the seemingly dominant and hegemonic web services of today are unlikely to retain that status for many years. Researchers had previously suggested that *Facebook* was likely to lose 80% of its users by 2017 (Garside, 2014). Any prediction – even well-intended – of what the typical experience of the internet will look and feel like in twenty years' time is likely to be arbitrary. I am aware that, whilst all research will in essence be 'of its time', the rapid and marked technological evolution of cyberspace – as well as the possibility of an actual occurrence of a cyberterrorist incident – raises a particular vulnerability pertaining to the foreseeable longevity of the case studies that are applied in this thesis. Nevertheless, the contributions that this thesis makes to the development of securitisation theory will form part of the historiographical development of the discipline of Security Studies. There will also be scope for the methodology and analysis that is applied in this thesis to be transferred to other areas of Security Studies, for instance, cyber weaponry understood more broadly, cyber criminality, as well as other phenomena such as asymmetrical drone warfare. The extent to which this is possible will become clearer in later chapters.

A recent survey by Jarvis and MacDonald (2015) highlighted that there is divergence of opinion in the 'cyberterror' disciplinary field, regarding what cyberterrorism is, and indeed, whether cyberterrorism

represents a legitimate avenue of research. Green has previously suggested that, as cyberterrorism has not yet occurred, it is unlikely to do so in the foreseeable future, and he thus proposed that "there is no such thing as cyberterrorism … which is not to say that cybersecurity isn't a serious problem – it's just not one that involves terrorists" (2002). It is also plausible that speaking of 'cyberterrorism' is a discursive action that isolates or distinguishes an issue that *already* exists within the remit of 'terrorism'. For instance, Gordon and Ford have noted that "we do not use the term 'ice pick terrorism' to define bombings of ice-pick factories, nor would we use it to define terrorism carried out with ice picks" (2002:645). Through this purview, the use of computers to directly cause violence and destruction, and/or the sabotage of computer systems could be termed 'crimes', or 'acts of terror', without an obligatory requirement to use a 'cyber' prefix. The decision to include the 'cyber' prefix to describe human uses of computer technologies is a conscious one, variably reflecting particular biases. For instance, those who use the 'cyber' prefix may be adopting pre-existing 'common sense' interpretations of suitable language that we apply when discussing computers. They may also be influenced by a perception that computer technologies alter human behaviours and experiences to the extent that they are substantively different when juxtaposed with an 'analogue' alternative.

Nevertheless, as mentioned above, cyberterrorism *has* been explicitly noted in the two most recent *National Security Strategies* as being a distinct threat facing the UK. The threat of cyberterrorism was detailed as one aspect of the 'Tier One' category of cyber threat (Cabinet Office, 2010a:11). These Security Strategy documents were drafted in 2010 and 2015 during an epistemological environment in which no cyberterrorist incident had occurred. Given that the overarching intention of the *National Security Strategy* is to outline the perceived main threats to the nation for the ensuing duration of a Parliament, this means that there will be policy and resource implications. For instance, one consequence might be that capital at GCHQ could be invested into specifically combating the potential vulnerabilities in British critical infrastructure that terrorists may seek to exploit through digital means. This can therefore be regarded as a process in which cyberterrorism has been 'spoken' into existence, by policymakers, academics and journalists (Conway, 2005). Not only is a 'cyberterrorist' identity created, but policies and counter-identities are also implicated.

This thesis reflects on cyberterrorism as a distinct subsection of terrorism, but I do acknowledge the arguments against such an endeavour, such as those voiced by Green (2002), Gordon and Ford (2002). Whilst I adhere to the premise that cyberterrorism is a social construct, a guiding definition is helpful. The

2000 *Terrorism Act* included a clause that can be interpreted as being the British states' legal-remit for the incorporation of cyberattacks within anti-terrorism legislation. Accordingly, Section (2)(e) of the *Terrorism Act* mentions attacks that are "designed seriously to interfere with or seriously to disrupt an electronic system" (Legislation.gov.uk, 2000:1). In a discussion of this clause, Walker (2006:632) highlights that this was included to offer a legal outline of cyberterrorism, and it is of particular note because it distinguishes the dichotomy between 'costly nuisances' and bona fide 'cyberterrorism'. With this distinction made, one can isolate general acts of hacking (whether criminal or benign) from serious attacks that would constitute an act of terror. For the purposes of clarity, hypothetical cyberterrorist attacks could be: the altering of iron supplement levels in a cereal manufacturing plant; modification of formulas used by a pharmaceutical producer; seriously disrupting an air traffic control system; or seriously disrupting the services provided by financial institutions (Collin, 1997). Assessments of potential cyberterrorist attacks, particularly by the United States, typically revolve around a significant attack on the US powergrid (see Idaho National Laboratory, 2016; Natter and Chediak, 2017; Sanger and Broad, 2018). There was some (disproven) speculation that Chinese 'cyberterrorists' caused the 2003 blackout in eight North-Eastern US states (Poulsen, 2008). Following a discussion by Signer and Friedman at the launch of *Cybersecurity and Cyberwar: What Everyone Needs to Know*, the 'cyber squirrel' meme emerged, wherein the fairly routine inadvertent attacks that squirrels have successfully made against power systems were humorously juxtaposed against the precisely zero attacks contributed by cyberterrorists (see Dews, 2014).

In the endeavour for a narrower comprehension of cyberterrorism, and to pay homage to existing literature on cyberterrorism, I draw on the testimony that Denning provided to the United States Congress' House Armed Services Committee; in which she provided a definition of cyberterrorism that has correlations with the American legal definition of terrorism. In her testimony, Denning stated that:

> "Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not" (2000).

A definition with a markedly similar ethos has been suggested by Hua and Bapna, who described cyberterrorist incidents as “attacks implemented … via information systems to (1) significantly interfere with the political, social, or economic functioning of a critically important group or organization of a nation, or (2) induce physical violence and/or create panic” (2012:176). In one of her earlier pieces on cyberterrorism, Conway distinctly expressed that, in order to be considered as an act of cyberterrorism, the attacks must have “a terrorist component”, thereby installing “terror as commonly understood (that is, result in death and/or large-scale destruction), and they must have a political motivation” (2002). Succinctly surmised in a breviloquent phrase offered by Barry Collin, who originally coined the word in the 1980s, cyberterrorism could be regarded as ‘hacking with a body count’ (2002).

The focus on significant attacks causing death and/or destruction is not by default an effort to overlook or dismiss the significance of the potential harm that can arise from less severe attacks, what we might call 'routine' attacks. As the international economy increasingly relies upon world-wide-web-enabled digital connectivity, denial-of-service (DoS) attacks represent a potentially significant threat to national security (Rosenfield, 2009). Routine, less frequently reported attacks can form an element of a long-term, gradual sapping of an adversary's economy (Kumagai, 2001). Brill (2010) suggested that the worst-case scenario in a cyberterrorist breach is if the terrorist is able to gain access to critical systems, but stay below the 'radar' of defences whilst maintaining access to systems and information for months or years. In the remit of this thesis, however, such a breach is *not* an instance of cyberterrorism, merely criminal snooping. Granted, the ability to snoop on critical systems would be highly desirable to a well-furnished terrorist organisation, but an act of terror inherently revolves around spectacles of horror and violence, rather than data-gathering. A pertinent tenet of routine criminal attacks is that the companies receiving such attacks are often hesitant to publicly report the attack because they fear that there would be a public relations backlash, wherein their consumer base would lose confidence in the ability of the company to retain personal information securely. A December 2015 agreement between the European Parliament and member state governments legally forces companies to report cyber breaches, but only if that company is deemed to offer an essential public service (Teffer, 2015). A 'death by a thousand cuts' cyber incident is not particularly daunting or terrorising if people outside of the affected organisation are not aware of it occurring.

As mentioned previously, some commentators have argued that cyberterrorism does not warrant a separate sub-field for academic attention. Others have suggested that there are differentiations that can be made within cyberterrorism as an entity in its own right. For instance, an interesting continuum was propositioned by Devost, Pollard and Houghton (1997:78), who differentiated the entities of 'terrorism', 'information terrorism', and 'pure information terrorism'. Accordingly, if both the target and the tools of an attack are 'physical', the incident can be considered conventional terrorism. If either the tools or the target of the attack can be considered 'digital', then the attack can be labelled 'information terrorism'. And finally, if both the target and the tools are digital, the authors of the continuum would designate the attack an instance of 'pure information terrorism'. This thesis does not apply this continuum, but it is worth noting in this section that there exists a wide range of differing perspectives on how to approach the analysis of cyberterrorism, and indeed, how the phenomenon should be identified in the first instance.

'Terrorism' does not yet possess an adequate definition (Schmid and Jongman, 1988), nor does 'cyberterrorism' (Jarvis, MacDonald and Nouri, 2014). The broad approach that is taken with respect to the definition of 'cyberterrorism' throughout this thesis is to allow the speakers of the official British discourse of the threat of cyberterrorism to define for themselves – or to leave undefined, as the case may be – what is included and excluded from the notion of 'cyberterrorism'.

The next section considers the threat of cyberterrorism, drawing on the existing cyberterrorist disciplinary field.

The Threat of Cyberterrorism

Having isolated cyberterrorism as an *act* involving violence or significant destruction, one must simultaneously acknowledge that an event of this kind has not yet occurred. When we engage with the discourse of cyberterrorism, we are essentially engaging in a discourse of constructions of the future. As Cavelty writes:

> "at all times, the cyber threats debate was (and is) highly political. It is not only about predicting the future, but also about how to prepare for it in the present … As there have been no major destructive attacks on the cyber level, different scenarios, which are stories about possible futures, are providing the grounds on which decisions have to be

made. The different actors involved – ranging from government agencies – with their divergent interests are therefore competing with each other by means of constructed versions of the future" (2007:22; see also Bendrath, 2001,2003).

Because there is, at present, no grounds for the discourse of the threat of cyberterrorism to utilise narratives that are based on historically recorded events, media and policy-making agents use spectre-raising terminology such as an 'electronic Pearl Harbor' to artificially construct a historical analogy (Bendrath, 2003:50).

This process represents a discourse of engagement with 'worst-case scenario hypothesising' of imaginary terrifying futures (Goede, 2008; see also Grusin, 2004). As Thomas states, "cyberfear is generated by the fact that what a computer attack *could* do is too often associated with what *will* happen" (2003:115-116). The worst-case scenario hypothesising is regarded by the critical scholarly community as negative, as it distracts attention and diverts "social resources in a way that may not be warranted by a more pragmatic assessment and prioritisation of all the risks that we face" (Durodie, 2007:444). The disregarding of facts, and reliance on worst-case scenario projections based on the possible options that may be available to adversaries leads to a politics of zero risk that may serve to legitimise abuses of power by a leviathan (Cavelty and Mauer, 2009; see also Aradau and van Munster, 2007:103). Basing intelligence and resultant policies on a preferred scenario and then hunting for data that might support such a scenario is a distorted approach to defence (Ryan, 2006:287). Nevertheless, precisely for this reason, the consequence of this kind of discourse is marked and interesting. Ultimately, the potentiality of threat raised by nuance and exaggeration simultaneously imparts a greater risk on ignoring the warnings. This process is aptly described by Hansen and Nissenbaum, who write that "turning the absence of prior incidents in the opposite direction, the difficulty of saying that it could not happen also creates a space for the projection of the (im)possible" (2009:1164). As Donald Rumsfeld, the then-US Secretary of Defence, stated at a 2002 NATO press conference, "the absence of evidence is not evidence of absence" (2002).

It is important to note that fears exhibited regarding cyberterrorism are not necessarily without due reason or precedent. Computer-mediated attacks leading to damage on physical infrastructure have been demonstrated as being within the realm of possibility. In 2000, an Australian man became disgruntled after having a prospective job application rejected by his local council, provoking him towards the (eventual) successful hacking of the human waste management system, which his previous employer had been

contracted to install. The attack lead to millions of litres of raw sewage spewing into local parks, rivers, and a hotel ground (Smith, 2001). Over the course of ten months in 2009 and 2010, American and Israeli government-sanctioned hackers launched the Stuxnet attack against Iranian nuclear facilities, to disrupt the contentious enrichment programme. This attack occurred despite fears of a 'new Chernobyl' (Fildes, 2011). In 2014, it was disclosed that a cyberattack successfully lead to infrastructural failures at a German steel mill (BBC, 2014a; BSI, 2014:31). In January 2016, it was revealed that unidentified hackers had successfully caused a significant power outage in Ukraine, using malware known as *BlackEnergy* to enter the utility company's systems, before applying circuit breakers and using the wiper utility, *KillDisk* – bolstered with denial-of-services attacks – to thwart recovery attempts (Goodin, 2016).

Pertaining to the absence of a bona fide act of cyberterrorism up to the present day, there are several plausible explanations possible, and indeed these may be operating simultaneously rather than exclusively. Some possible examples include: today's terrorist organisations may lack the computer expertise required for a successful attack; the upper echelons of the groups may retain a worldview wherein delivery method does not involve bits and bytes; and much of the developed world's critical infrastructure uses private networks, which operate with the best possible internet security, which is to be completely disconnected from it (Iqbal, 2004:404-405). These ‘air gapped’ IT systems can still be attacked; indeed, the Stuxnet worm was delivered against an air gapped SCADA system. These air gapped systems are designed to be isolated from the internet, but banal or malicious code can still be entered into them, given that they are designed with removal storage ports so that patches and software updates can be installed.

Conversely, one could also proposition the possibility of an 'Edward Snowden effect', wherein terrorists – now aware of the continuous, pervasive data-mining conducted by Western governments and their associated intelligence services – eschew online methodologies in favour of 'offline' attacks that can be organised and delivered via conventional means. In 2013, Sir Andrew Parker (2013), the then-head of MI5, stated that the leaks concerning the methods of the intelligence services had been a 'gift' to terrorists. There are signs that terrorists have benefited from the leaks and become more conscious of surveillance; a German-language online Islamist magazine, *Kybernetic*, published in December 2015, advised Islamists not to

possess or use a smartphone[4], and detailed a step-by-guide on how to send and receive encrypted messages (see Flade, 2016). The front page of the magazine details two hands against a black background, with one hand holding a bullet, and the other a USB memory pen.

Because the will-to-violence exhibited by terrorists is typically beyond what is perceived to be rational intention and action, terrorists are sometimes believed to be psychopathic. However, no study cogently indicates that this is the case (Hudson, 1999; Keet, 2003; Krueger and Maleckova, 2003; McCormic, 2003; Post, 2007; Victoroff, 2005). Acknowledging the absence of insanity as a causal factor for terrorism allows us to examine the terrorist relationship with cyberattacks within the realm of a rational cost-benefit analysis, wherein the forces acting on the indifference curve are (a) the preferences of terrorists and (b) the effectiveness of cyberterrorism in achieving objectives (Giacomello, 2004:390). Because terrorists have a tendency to continue a methodology that is proven successful in the achievement of their objectives (Denning, 2000), the threshold point where cyberterrorist attacks begin to occur will be breached when an attack mediated by computers would be deemed to produce similar or greater results than that relying on conventional methods (Flemming and Stohl, 2001).

Psychology and emotions nonetheless play a pertinent role in the perceived efficacy of terrorism. A study by Lerner et al (2003) indicated that people exhibit greater negative emotion from stimuli that induce fear instead of anger. This may represent a structural inhibitor on the actuation of cyberterrorism, as people tend to be *irritated* rather than *fearful* in the midst of a power-cut, for instance. Given that the primary objective of terrorism is coercion through fear, terrorists may eschew certain types of cyberterrorism because the likely impact is perceived to be ineffective. Psychological exploration of cyberterrorism – and cybersecurity more broadly – is certainly a field that warrants greater attention, and it is notable that there are some existing forays into the role of psychology and its relationship with cyber specific threat (see McAlaney, Taylor and Faily, 2015).

The seeming adversity that some members of the scholarly community believe terrorists feel towards 'bits and bytes' is likely to recede over time, particularly as younger generations increasingly ascend to leadership roles in terrorist organisations (Rathmell, 2008:44; Prensky, 2001). Indeed, technology, broadly

[4] The Snowden revelations highlighted that the NSA possessed the ability to remotely activate the microphone of most brands of smartphone (even if the phone was switched off), and use the phone as a bug (for instance, see Rosenbach, Poitras and Stark, 2013).

perceived, converges with images of masculinity and power (Faulker, 2001), and the ability to conduct cyberterrorist attacks would allow a terrorist to cause death and destruction without needing to put themselves in direct harm. That being said, given that the training associated with reaching the capability where an organisation can conduct significant cyber attacks on infrastructure is typically associated with state-level resources – with 20 to 30 states today believed to have offensive cyberwarfare capabilities (Paganini, 2015); cyberterrorism can be considered to possess a high barrier to entry. However, terrorists, like large criminal organisations have demonstrated resourcefulness, a factor that led Glenny to write that terrorists are excellent capitalists and "every bit as cosmopolitan as Shell, Nike or McDonalds" (2009:5-6). Given that in some cases, terror-crime syndicates may be capable of handling their entire chain of operations along an in-house, de-centralised vertical command – in some cases even possessing their own military force to protect their assets – it is possible that terrorists could hire competent computer hackers on a long-term basis (Furnell and Warren, 1999:33-34). These assertions about the nature of contemporary terrorist groups partially befit the 'New Terrorism' thesis. The ramifications of the New Terrorism thesis for the official British discourse of cyberterrorism will be examined in detail in the fifth chapter of this thesis.

The next section outlines the structure of the ensuing chapters of the thesis.

Structure of the Thesis

Chapter Two, 'Theory', begins by detailing why the Copenhagen School's securitisation theory is relevant to critical analysis of the discourse of cyberterrorism. Whilst a broad framework for the study of securitisation does exist, 'securitisation theory' itself is not monolithic, and approaches can vary markedly on elements such as the audience, the 'speech act', as well as the means by which the analyst can gauge whether or not a securisation has been successful (or indeed, whether such a measurement is in fact plausible). The chapter addresses these nuances, and expresses justifications for this thesis's application of components of *both* the 'traditional' framework offered by the Copenhagen School, and the alternative approach offered by the Parisian School, as pioneered by Didier Bigo (2006). The 'Pantomime' audience, an alternative framework for the agency of the 'audience' in securitisation is outlined. Through this 'Pantomime' framework, multiple tiers of an audience can be ascribed varying levels of access to, and influence over, a

securitisation. It is suggested that this 'Pantomime' framework would be useful for both democratic and totalitarian contexts, and whilst only three audience 'tiers' are considered in this thesis, the framework could be used to articulate many more distinctive tiers.

Chapter Three, 'Methodology', begins by detailing the 'interpretive approach' to the study of Social Science, reflecting on both its pertinence to the study of the threat of cyberterrorism, and its drawbacks. Throughout this chapter, the impetus is not simply to detail *how* I undertook analysis and drew my findings, but also to convey *why* I undertook a given approach to analysis. There exists a wide range of approaches that could justifiably be used to scrutinise a securitisation, but for the purposes of this thesis I determined that an approach aligning with the interpretive ethos was most apt.

The thesis is, fundamentally, an analysis of discourse and the construction of identities; particularly the identity of threatening individuals and collectivities in cyberspace. Consequently, the chapter pays homage to what discourse is, and the matter of how identities are articulated by vested actors. From the standpoint of public-facing open source knowledge, it is unclear whether cyberterrorists objectively exist outside of discourse. In the corpus, a range of discursive tools have been used by actors to socially-construct the threat of cyberterrorism, but two tools, 'metaphor' and 'narration' are of particular interest given that these are popular means by which to project existing knowledge onto an event before it has occurred and also onto a 'cyberterrorist' identity that may or may not exist. Consequently, included in Chapter Three is an engagement with existing academic literature that concerns the functionality of metaphors in security discourses.

Chapter Three will then elaborate on the process of source acquisition that was conducted in order to gather relevant documents, statements and other materials. In order to adequately scrutinise the sources to ascertain meaningful findings regarding the securitisation of cyberterrorism, I asked a series of questions. I deemed this interpretive method to be more transparent than a fully open-ended approach. Explicitly listing the questions that I have asked of the sources serves to make clear to readers how I arrived at particular findings, and simultaneously gives an indication of *why* I have designed questions with a particular phrasing. Listing these questions also means that I have been able to be explicit about the efficacy of particular sources in answering the questions.

Having asked these questions of the 110 unique sources that I collected, I was able to ascertain four central strands, and four sub-strands, which underpinned the 'official' British discursive construction of the threat of cyberterrorism. The final section of Chapter Three details these strands.

Chapter Four concerns the central pillar of the construction of the threat of cyberterrorism to the UK via the 'official' British discourse; the notion that cyberterrorism represented a 'Tier One', or severe, threat to the UK. This chapter explores how cyberterrorism emerged as a socially-constructed 'Tier One' threat to the UK as a result of the British National Security documents released by the Coalition and Conservative Governments. The 2010 *National Security Strategy* and *Strategic Defence and Security Review* documents (Cabinet Office, 2010a; 2010b) were regarded as the securitising 'acts' that established the securitisation of cyberterrorism. This style of 'securitising moment', a statement published in a document with an expected lifespan of a full Parliament, fits relatively comfortably with the traditional 'Copenhagen' framework of securitisation theory. However, the public-facing articulation of cyberterrorism as a 'Tier One' threat did not rely on these documents alone; Ministers, MPs and Peers also espoused the idea that cyberterrorism represented one of the most significant threats to the UK. Cabinet Ministers with Privy Council access could, quite feasibly, be assimilated within securitisation theory under the guise of 'securitising actors', but the idea that they performed as securitising actors for the full duration of May 2010 to June 2016 would not be satisfactory. More fitting is a framework that allows a securitising actor to depart the stage and return to a seat amongst the audience, whilst retaining their right to ascend to the stage. In essence, one's position as a securitising actor should not exclude a genuine capacity to serve a dual purpose as an audience member. Furthermore, the 'cyberterrorism as a Tier One threat' construct could remain intact even if the stage were empty; rather than passively offer a binary 'affirmative' or 'negative' to a proffered securitisation, members of the audience are able to repeat and echo the discursive construct. When a backbench MP 'echoes' a securitisation in this fashion in the Commons Chamber, they are not simply affirming their agreement with the securitisation, but they are actively trying to persuade other members of the audience (not simply their colleagues present in the Chamber but also viewers of the televised feed from the Chamber, and readers of Hansard) of the necessity for extraordinary measures to be enacted against an exceptional threat. Whilst audience members may not have the legitimacy to *create* a securitisation, they nevertheless possess the capacity to *renew* it and perhaps even *alter* it. Accordingly, Chapter Four maps the discursive 'securitising

moments' identified from the corpus that engaged with the notion of cyberterrorism as a 'Tier One' or severe threat.

It is argued in Chapter Four that the securitisation of cyberterrorism was not necessarily first and foremost concerned with eradicating the perceived threat of terrorists conducting significant cyber attacks against the UK. Instead, it is proposed, the securitisation of the threat of cyberterrorism served as a tacit endorsement of the UK's own cyber weapons program. By categorising cyberterrorism as a Tier One threat, the Government created a partially-fixed nodal point that labelled cyber mediated violence by non-state actors as illegitimate. By default, the creation and maintenance of this partially-fixed nodal point endorsed a socially-constructed reality in which legitimate cyber mediated violence could exist. This notion – that the British securitisation of cyberterrorism *makes possible* particular assumptions about the role of the British state in cyber security – feeds into the analysis in the fifth and sixth chapters of the thesis.

Chapter Five maps further components from the corpus of the official British construction of the threat of cyberterrorism, specifically those which adhere to the notion the securitisation of cyberterrorism is 'temporally' unique. These components from the official discourse align with one of two sub-strands; the first is the idea that cyberterrorism befitted a 'New Terrorism' hypothesis, and the second was a fear that cyberterrorism was a threat deemed to be escalating over time. It is argued that the 'New Terrorism'-esque aspects of the cyberterrorism-as-threat discourse acted as an entrenchment of the discursive social-construction of an illegitimate violent identity in cyberspace. Ministers, MPs and Lords elaborated on the narration of the perceived threat of cyberterrorism, and it is suggested that their 'chanting' endorsed and evolved the discursive existence of a threatening cyberterrorist identity. The second sub-strand – the notion that cyberterrorism was a threat that would escalate over time – was found to exist both in the initial securitising act and in the mediation of the securitisation by the audience. It is suggested that repeated narration of an increasing threat of cyberterrorism was a discursive process that sought to increase the lifespan of the securitisation in the absence of a cyberterrorist event that would have both legitimised and justified the discourse of cyberterrorism-as-threat. In effect, this process served as a discursive 'insurance policy' against the perennial discursive risk of 'crying wolf'.

Chapter Six, the final mapping and analysis chapter of the thesis, maps the remaining components from the corpus of the official British construction of the threat of cyberterrorism. This chapter is divided

into two distinct parts. The first section is a mapping and analysis of items from the corpus that related to the notion that cyberterrorism was a 'spatially unique' threat. According to the discursively-constructed identity, to be a cyberterrorist was to operate in a landscape deemed to be distinct from that utilised by 'analogue' or 'conventional' terrorists. This spatial-uniqueness was divided into two distinct sub-strands. The first of these strands was the concept of the terrorist 'Safe Haven'. It is found that the use of linguistics associated with narratives of terrorist 'Safe Havens' was a process of 'Othering' that served to distinguish between legitimate and illegitimate forms of *being* in cyberspace. The second sub-strand was the notion that 'physical' and 'cyber' spaces were distinct. In the analysis of this sub-strand, it is argued that the securitisation of cyberterrorism revolved not around the *technical* space of the internet – which enabled cyberterrorism to exist as a possibility – but instead the *identities* of particular users of the internet.

The second section of Chapter Six draws on the final mapped components of the corpus to elucidate the way in which popular fictional narratives can be used by securitising actors and members of the audience to 'fill in' an epistemic void in the cyberterrorism discourse. Cyberterrorism has not yet been experienced directly by anyone either in the UK or abroad, but cyberterrorism can still be vicariously experienced through the reading or viewing of popular fictional narratives. Specifically, the 'cyberterrorist' narratives depicted in the 2012 installation of the James Bond franchise, *Skyfall*, and William Forstchen's (2009) *One Second After* are scrutinised, as these were referenced by some members who were included in the corpus.

Lastly, Chapter Seven, the concluding chapter of the thesis, summarises the findings of the thesis. This concluding chapter also considers the limitations of the approach that has been taken in conducting this research, suggests further research endeavours that would be fruitful for further engagement with this thesis's research questions, and offers some final remarks.

Conclusion

This chapter has sought to establish several key points that will underpin the ensuing analysis and findings. The chapter detailed the thesis aims and research questions that drive the analysis; obviously these are integral, and adherence to these throughout the ensuing chapters has helped to develop a coherent argument. The second section of this chapter reviewed the subject of cyberterrorism, emphasising that the

term is a discursively-created threatening phenomenon and that there is, at present, no uniform acceptance of what cyberterrorism *is*, or indeed whether cyberterrorism warrants its own independent discourse separated from a monolithic 'terrorism' entity. The fluidity of the definition and meaning of cyberterrorism is a significant tenet that surrounds the official discourse of cyberterrorism, and is a matter that will be returned to in the analysis. A fluid definition could serve as a means to encourage misinformation amidst securitising acts, thereby denying the audience a sufficient toolkit to dispute the securitisation. Similarly, a fluid definition could also make the securitisation more permeable, particularly in the case of cyberterrorism, a threat that has yet to occur. If the securitisation of cyberterrorism is loosely defined, this would permit the securitisation to assimilate affiliated cyber threats to the UK as and when they arise.

The schools of Critical Terrorism Studies and Critical Security Studies were both introduced in this chapter, as they represent the approaches that are most concordant with the methods adopted in the thesis. Specifically, their position on the construction of meaning – that meanings are not fixed, but are instead in a state of constant flux – is useful in the analysis of a phenomenon that has been 'talked into existence'.

Lastly, this introduction detailed an overview of the chapters that follow in the thesis. The next chapter engages with the method that will be used to analyse the official British discourse surrounding the threat of cyberterrorism, detailing the efficacy of securitisation theory. The chapter will also outline the nuances that are entailed within this approach to Security Studies, with the intention of highlighting this thesis's contribution to theory.

Chapter Two: Theory

Securitisation Theory

In the field of Security Studies, the 1980s embodied a 'return to theory', a process that had been influenced, in part, by the developing Critical Studies branch of International Relations. This ‘return to theory’ occurred in concurrence with a heightened awareness of the relationship between the study of security and normativity (Waever and Buzan, 2007). Within this evolution of the approach to Security Studies, the Copenhagen School emerged, which sought to move beyond the debate concerning 'true meanings' of security (Buzan, Waever and Wilde, 1998:2). Instead of being implacably fixed in meaning, security is considered fluid and changeable; as Buzan writes, “security means survival in the face of existential threats, but what constitutes an existential threat is not the same” (1997:27). As a case-in-point, an example that has been used elsewhere is that of a theoretical gargantuan asteroid striking the planet Earth, which represents a threat of potentially society-destroying magnitude, but is arguably a threat that has not been securitised (Buzan, 2010). In contrast, more mundane threats such as the consumption of illicit narcotics *have* been securitised. In their seminal book, *A New Framework for Analysis*, Buzan, Waever and Wilde defined the raison d’etra of the Copenhagen School, writing that: “based on a clear idea of the nature of security, securitisation studies aims to gain an increasingly precise understanding of who securitises, on what issues, for whom, why, with what results and, not least, under what conditions” (Buzan, Waever and Wilde, 1998:32).

Securitisation theory is an attractive framework that one can use to scrutinise how some security issues take a greater precedence over others, particularly in cases where an issue that is perceived to be more pressing is not, objectively speaking, the greatest threat to human life (Taureck, 2006). Securitisation theory allows scholars of security to pinpoint processional stages in the discursive handling of a given security issue, which mark its rise and decline in prominence and prioritisation. These processional labels can then be used to critique how shifts in perceived prioritisation of a security issue occur. In this regard, securitisation theory is an accessible but powerful tool.

In the original incantation of process-driven securitisation theory Buzan, Waever and Wilde (1998:6) identified three stages to a securitisation, which are, accordingly: 1) identification of existing threats; 2) emergency action; and 3) effects on inter-unit relations by breaking free of rules. Scholars can, and do, disagree on whether these three stages are sufficient; indeed, it is my view that the audience(s) involved in a securitisation are given insufficient agency in the above three-step framework. Nevertheless, a framework that highlights processes whereby security issues are prioritised through discourse is an invaluable asset in the scrutinisation of cyberterrorism, a phenomenon that has essentially been spoken-into-existence.

In what Balzacq has termed the 'internalist approach', there are three units of analysis incorporated within the securitisation framework: 1) the referent object, 2) the securitising actor, and 3) functional actors (Balzacq, 2005; Buzan, Waever and Wilde, 1998). Such an internalist approach, Balzacq has argued, "overstates the intrinsic power of a rule-governed use of concepts … to move an audience's attention toward an event or a development construed as dangerous, the words of the securitising actor need to resonate with the context within which his/her actions are collocated" (2005:182). In essence, Balzacq suggests that we can conceive of securitising acts as a contestation – or mediation – of the 'symbol' of security, which is an isomorphic frame shaped by a given context, and the influence of the speaker's discourse (2004, 2005). Buzan and Waever eluded to this phenomenon, admittedly in somewhat clouded terms, as an 'intellectual process'; wherein securitising actors and audiences construct a 'shared understanding' of the threat in question (Buzan, Waever and Wilde, 1998:26,41; Buzan and Hansen, 2009:34; Oren and Solomon, 2015:320-321). Greater detail will be paid to the matter of the audience later in this chapter.

Securitisation theory entails a relatively straightforward and accessible framework, but that does not necessitate that the approach to the study of securitisation is monolithic. Indeed, there are differing approaches to the study of securitisation, and securitisation theory represents a contested field. It is therefore important to place this thesis coherently within the ongoing development of securitisation theory. What could be termed 'traditional' securitisation studies typically focuses on the enunciation of an exceptional speech act, which, if accepted by a relevant audience, establishes a securitisation permitting radical (perhaps military) measures against a designated threat. An alternative approach is suggested by Didier Bigo (2004, 2006), who proposed that we can conceptualise 'professional managers of unease'. These 'managers of unease', assisted by their access to technology and statistical analysis, are able to prioritise threats and determine what

constitutes 'security' in a given context (Bigo, 2004; 2006). This approach to the study of securitisation has been termed the 'Paris School'. The key contribution of the Parisian School is this: rather than relying upon spectacular events and grand pronouncements, the 'management of unease' is instead said to operate as a 'routine' form of securitisation. Here, 'routine' represents a cumulative development of everyday practices and often seemingly minor legislative changes over an extended period of time. Aradau and Munster (2007, see also Beck, 1992), drawing on Beck's elucidation of the 'risk society', argue that in the case of counter-terrorism, this cumulative and 'routinised' process has effectively blurred the distinction between war and policing, as exhibited by a culture of precaution. This approach to the analysis of securitisation seems suitably apt, given that there has not yet been an incident that can be labelled cyberterrorism. In the absence of a bona fide case of cyberterrorism, professional managers of unease (for instance, British Ministers, the intelligence services or police spokespeople) are only able to speculate the potential scope of a future incident.

In his book, *Securitising Islam*, Croft (2012) sought to ‘loosen’ some of the constraints that were self-imposed by the Copenhagen School, so that he could apply securitisation theory in a context and purpose-specific setting. Similarly, I will draw on the Copenhagen School’s ubiquitous grammar of security and ‘loosen’ some of the constraints. Specifically, I reconfigure the relationship of securitisation theory with the role – and constitution – of the participatory audiences. I also loosen the temporal scale of securitisation theory. Cyberterrorism does not fit the model of a threat that is presented with immediacy and which can be solved with emergency measures before being returned to a status of a ‘politicised’ issue. Such a loosening of the constraints of the theory is not an attack on the mainstream – either Copenhagen or Parisian – blueprints of securitisation theory. Rather, what I offer here is a context-specific approach to securitisation theory that is suitable for analysing the construction of the threat of cyberterrorism. Certainly, what follows below could be applied as a blueprint in other contexts; however, I do not proclaim my reading of securitisation theory to be universally suitable, and indeed insist that in many cases it may be misaligned. In the context of a threat epitomised by a threatening identity (cyberterrorists), a successful securitisation effectively gives the securitising actor the right – in the Weberian sense (Chatterjee, 2005) – to enact a monopoly of legitimate violence.

Different threats understandably may require different proscriptions; for instance, a securitisation of a threat emanating from our natural environment is likely to differ because the natural environment does not have human agency. The environment was considered by Buzan, Waever and Wilde (1998) to be one of the four 'sectors' that are securitisable, with the other sectors being military, economic and societal. The "environment itself rarely becomes a referent object", and instead "it is in fact civilisation dependent upon the environment that is the referent object to be securitised" (Vogler, 2002:185). Climate change in particular is regarded as a threat multiplier, and the political attention provided to this matter has been highlighted by some as evidence of a securitisation (Schafer, Scheffran and Penniket, 2015:78; Brzoska and Oels, 2011; Oels, 2012; Methmann and Rothe, 2012). Whilst there are some environmental issues that *can* be secured with violent means, such as anti-poaching measures in Kenya, broadly speaking the military and the use of force is unsuitable to the guaranteeing of environmental security as the natural environment (for instance, rising sea levels) will not react to a threat of violence. In fact, the military is often the antithesis to environmental security, with environmental issues surrounding phenomena such as nuclear weapons testing, the burning of oil fields, or the intentional demolition of forested and shrubbed areas, such as that committed by the Israeli forces on borderlands with Palestinian territories (see Lynfield, 2015). Conversely, in the sense of something to be securitised *against*, the environment cannot be considered a conscious actor, unless one assumes that the legal term "An Act of God" operates in a literal sense. This is not to conflate securitisation with militarisation. The key point here is that this thesis considers the labelling of acts of violence as either legitimate or illegitimate to be a central component of a securitisation framework that posits a process-driven perspective akin to that of the Parisian School. Because an ascribed identity can be feasibly be securitised, this allows security scholars to observe a securitisation even in the absence of a particular security-detracting event. The possibility of securitising identities on the basis of their possible future actions, in essence, permits preventative rather than reactive securitisation. In the case of the securitisation of cyberterrorism, what is securitised is not a tangible reality based on an explicit historical cyberterrorist event, but rather the *possibility* that individuals or groups may utilise computer systems as a direct means of sowing death and destruction. This is distinct from the framework of 'riskification', which will be detailed shortly.

There are, particularly within the discourse of climate change, some exhibited symptoms of securitisation that make a claim of 'the environment is securitised' tempting. The 21st Conference of the

Parties to the United Nations Framework Convention on Climate Change in Paris in 2015 demonstrated that – at least on a rhetorical basis – major industrialised states took the threat of climate change seriously (Harvey, 2015). In an example of media influence, the BBC Trust forced senior managers to stop inserting 'false balance' in issues that are deemed to be non-contentious, such as the human causation of climate change (Knapton, 2014). This is resultant from the culture within the climatic scientific community.

'Cyberspace', as has been detailed in the previous chapter, is an environment of sorts. However, as will be found in the analysis chapters of this thesis, the securitisation of cyberterrorism revolves not around the 'technical' environment of cyberspace, but instead the identities of particular actors who use it.

A more appropriate security framework to scrutinise the issue of 'security and the environment' could be that of 'riskification', which is aptly detailed by Olaf Corry (2012). A framework of riskification posits that risks – differentiated from 'existential threats' – cannot be eradicated, simply managed. The projected time-frame involved with a 'risk-ified' threat is therefore a long term, generational one, rather than a threat that can be temporarily securitised, reduced to an inconsequential significance through emergency measures, and then returned to the realm of normal politics. In a 'riskified' discourse, the measures and policies targeted against a threat seek to reduce vulnerability and the exposure to the implied risks. Given that issues pertaining to the environment are broad, complex, and inherently contextual, this framework is better suited to analysing efforts to manage human relations with the environment. There is, to an extent, a case to suggest that the riskification framework is a more suitable toolkit for the critique of counterterrorism discourse than the framework offered by securitisation theory. Given that political violence – whether perpetrated through digital or analogue means – is an avenue of political activism that is unlikely to cease in the foreseeable future, a framework that permits one to see a discourse of security as *long-term* rather than immediate and temporary appears more apt.

As was discussed in the first chapter, cyberspace can be considered the 'fifth sphere' of power projection, an environment reliant on computers, servers, cables and exchanges posited in the physical environments of land, sea and space, but nevertheless constitutive of a new sphere in its own right. In an article, Adam Kingsmith has referred to 'digital macrosecuritisations', noting that "the object to be secured is a borderless world of free-flowing information, a single seamless environment where ideas can be shared fluidly within a cyberspace that is not controlled by spatial and temporal conceptualisations of security"

(2013:4). This thesis takes critical infrastructure as the object to be secured. The internet is a revealing entity because its origins date back to a Defense Advanced Research Projects Agency (DARPA) programme, instigated as a means of ensuring that American military communications as a whole would remain functional if one part of the network was attacked. However, whilst the internet began its life as a response to a securitisation (in this case the Soviet Union as an existential threat to American military operability), there is now a cogent and widespread belief that the internet should remain 'neutral' (no web traffic is given priority over any other), free (as in freedom, not 'free beer') and uncensored. Undoubtedly, some states have sought to explicitly link even banal internet usage with matters of national security, for instance China and Saudi Arabia, but these restrictions do not represent a desirable state of affairs. The infringements on privacy, security and liberty that are detailed in the *Freedom House* "Freedom on the Net" reports make for sobering reading (Kelly et al, 2016).

To reiterate, this thesis takes the critical infrastructure of computer systems as the referent object of securitisation most implicated in the securitisation of cyberterrorism. Examples of such infrastructure could be water utility control systems, or integrated navigation for a particular brand of electric car. These physical spaces are distinct from, say, the 'virtual environment' of a webpage. Ultimately, the implication that the environment – whether land, sea or cyberspace – could be securitised would contribute to a process of a seemingly ever-expansive parameter of security. This is absolutely not to detract from the security issues surrounding environmental degradation, but securitisation cannot be a limitless concept, and effort should be made to restrict analysis. Indeed, whilst this thesis is concerned with securitisation theory and its alignment with the securitisation of a 'risk' (the risk that proscribed terrorist entities may conduct a cyber attack), it is possible that a 'riskification' model would better elucidate threats emanating from, within and against targets in the virtual environment of cyberspace.

This chapter will now consider an elementary component of the securitisation framework: the audience. The audiences have the capacity to accept or reject a call for a securitisation, and it is therefore of central importance to capture a logic through which appropriate agency can be ascribed to the audience participants.

The Securitisation of Cyberterrorism in Relation to the 'Traditional' Framework of Securitisation

The mapped discursive construction of the threat of cyberterrorism that follows in Chapters Four, Five and Six – that terrorist application of computer systems for the purposes of wrecking death and/or destruction represents a severe threat – befits the 'traditional' model of securitisation theory. This framework is articulated in the seminal book, *Security: A New Framework for Analysis* (Buzan, Waever and de Wilde, 1998:35-39). This framework is a speech-act based model, which distinguishes between referent objects, securitising actors, and functional actors. The referent object is the 'thing' that is deemed to be existentially threatened. In the case of the securitisation of cyberterrorism, this referent object is, chiefly, the critical national infrastructure underpinning key utilities in the UK. This infrastructure is ascribed a preferential status because of its role in the functioning of the British state, as well as the reliance that everyday British society places on its continued and uninterrupted operation. To contextualise this point, one could consider the unprecedented 'brute force' attack[5] conducted against British Parliamentarians in June 2017, in which up to 90 parliamentary staff email accounts were compromised, leading to the temporary suspension of off-site access (Maidment, 2017). Andrew Bridgen, the Conservative MP for North-West Leicester, was perhaps astute when he told the Press Association that the breach could usher in blackmail attempts (see The Guardian, 2017), given that Parliamentarian's inboxes are likely to contain confidential information from both colleagues and constituents. However, even if this attack were conducted by terrorists – although at the time of writing, Russia appears to be regarded as the most likely culprit (MacAskill and Syal, 2017) – this would not be an instance of cyberterrorism, given that death and destruction has not been caused, nor is there an existential threat at a societal level.

In the case of the securitisation of cyberterrorism, the 'securitising agent' is, most expressly, the Cabinet Office, which was responsible for the publishing of the National Security Strategies and for directing Government policy relating to the prioritisation of security threats. Buzan, Waever and de Wilde (1998:40) allowed for a relatively flexible remit in terms of who could, or could not be, a securitising agent; acknowledging that, conceptually, deciding who represents the securitising actor is more challenging than

[5] A 'brute force' attack spams a password database with password guesses for a given user entry. This is a crude form of attack that is effective on vulnerable databases (particularly those which have not been 'salted'), or for individual users who have inadequate password protection (for instance, those who have set their password as 'password' or their constituency name).

isolating the referent object. However, given that the attempted move to securitise cyberterrorism in the UK first appeared in the 2010 version of the *National Security Strategy*, and the ability to publish this document was restricted to the Cabinet Office, it is not without basis to suggest that the Cabinet Office is the primary legitimate securitising agent in this instance.

Buzan, Waever and de Wilde defined the 'functional actors' as those actors "who affect the dynamics of a sector" (1998:36). This definition purposefully permits a broad remit of who can be considered a functional actor, and, I would suggest, effectively designates this third category of actor as a 'stakeholder' in a given securitisation. These 'stakeholders' are ascribed some agency to influence a given securitisation, whether directly or indirectly. The staff of Cabinet members, the civil service, employees of the Houses of Parliament estate, Select Committees, not to mention MPs themselves and members of the public are amongst what is, effectively, a complex network of actors who could be included in a framework of securitisation. In the case of the securitisation of cyberterrorism, significant non-governmental organisation stakeholders might be: internet infrastructure providers; computer hardware manufacturers; social networking, internet search and advertising firms; or critical national infrastructure providers. Indeed, given that a significant and sustained attack against critical national infrastructure would feasibly have the capacity to harm security at a 'societal' level, everyone who is aware of the threat of cyberterrorism could be considered a stakeholder. However, by mapping and analysing the discourse offered by the Cabinet Office, MPs and Lords, this thesis limits the categories of possible stakeholders. This serves two functions. Firstly, mapping and analysing an entirety of the British discourse of the threat of cyberterrorism would not be feasible within the limitations of a PhD thesis. Secondly, to isolate a 'Whitehall' securitisation of cyberterrorism is to map and analyse the UK's highest tier of discursive environment in which policies relating to mitigating cyberterrorism can be debated, challenged, and re-affirmed.

Of particular interest for the novel contributions to theory offered by this thesis is the notion of the 'audience'. In the next section of this chapter I will introduce a framework for a 'Pantomime' model of securitisation. Audience members included in the corpus and conceptualised as part of this framework are Ministers, MPs and Lords. The political figures are regarded as having engaged with the securitisation through Hansard contributions, public speeches and interviews with the media. This reduction of engagement to recorded 'moments' in which an individual or collective have expressed their views or their intentions,

misses that which is not recorded, and indeed, that which has not been said, but may have still been felt or experienced. Furthermore, as noted in Chapter Three, this thesis takes recorded statements at face value. It is not my place to 'project' meaning onto the discourse, but rather, to infer meaning from the recorded 'moments' in the corpus. Consequently, when I state that this thesis is the first comprehensive overview of the official securitisation of cyberterrorism in the UK, it is, more accurately, a mapping of the recorded – and open-source – 'moments' in which a distinct and exclusive section of the British population have engaged with this particular articulation of threat.

The 'Pantomime' Model of Securitisation

The 'audience' is the site at which an issue can acquire the status of securitisation. The 'security utterance' enunciated by the securitising actor is, first and foremost, directed at the audience; Balzacq (2005:183) has labelled these utterances 'linguistic marks', which direct the attention of an audience to a given being or object that relates to their security. The concept of the audience, however, is not without controversy. For instance, McDonald has suggested "that dynamics such as the role of 'facilitating conditions' and the 'audience' are so under-theorised as to ultimately remain outside the framework itself" (2008:564). It is crucial to elaborate on the issue of the 'audience' in securitisation theory and resist the urge to leave it in a state of cultivated ambiguity.

Johnson-Laird referred to security discourse as "a blueprint for a state of affairs: it relies on the [audience] to flesh out the missing details" (1983:471). It would thus not be inaccurate to say that securitisations are audience-centric phenomena, in which the audience is given the capacity to either enable or render ineffective a securitising utterance (Balzacq, 2005:184; Balzacq, Leonard and Ruzicka, 2016:499). Granted, agreement between the securitising actor and the audience is *not* likely to be on the basis of power parity; as Roe highlights, "actors often possess, and indeed employ, the resources to cajole and bully audiences into acquiescing to their depiction of events", although of course it is important to note that "some kind of agreement is nevertheless required" (2012:255).

The audience and the securitising actor operate within embedded power structures in which some members of the audience are – for reasons of national security, wilful deceit, or in some cases simple

ignorance – deprived of knowledge. This deprivation of knowledge bequests the securitising actor with "a privileged position in signalling important developments and in establishing the meaning of those developments" (Watson, 2012:286). Hagmann and Cavelty (2012:87) have convincingly argued that – in the case of the documents pertaining to the British *National Security Strategy* and *National Risk Register* – the Cabinet Office expresses the enclosed information in a 'scientific', technical manner. This tendency has a depoliticising effect, as otherwise non-invested members of the public are denied the ability to effectively engage in informed debate in support of, or against, a given securitisation.

The speaker *does* have to convey an alarmist message of an existential threat with at least some efficacy to the public. In order to achieve a successful perlocutionary effect, the securitising actor must tune his or her language to the pre-existing experiences and perceptions of the audience (Balzacq, 2005:184; Edelman, 1988). In essence, the securitising actor represents the threat "by *other* things, which are then 'packaged' and 'sold' as containing threats or promoting security" (Schouten, 2014:28; Salter, 2008a:258). To cite an example, it is, to a venerable extent, to the aforementioned phenomenon that one can attribute the then-Prime Minister David Cameron's reference to criminals plotting to do 'bad things' on the internet, when he was interviewed on a popular morning television programme in November 2015 (Deacon, 2015).

To refer simply to 'an audience' is an insalubrious move. In reality, it is instead sound to discuss the existence of "not one single audience but rather several possible audiences" (Balzacq, Leonard and Ruzicka, 2016:499). Indeed, it is entirely feasible that the primary audience is *not* the general public, and it is instead the political, military and intelligence elites who require convincing, even if they are close (professionally and/or personally) to the securitising actor (Taureck, 2006:20). This author agrees with Williams's (2011a) contention, that the receptive audience can be seen to be created by a securitisation. Specifically, I suggest this means that the securitising actor is able to actively pursue the audience whom they believe they need to convince; simply trying to rally 'everyone' around a securitisation would be a waste of time and resources. The audience that is 'created' for any given securitisation would also be influenced by structural factors, such as the level of accountability and transparency within national or local government, the role of invested NGOs, and the general public/media interest in an issue or policy. Consequently, the 'audience' could be as small as a crisis response committee in the Cabinet Office Briefing Room (COBR), or indeed as large as a national or multinational public. Clearly, context is key here; the 'created audience' will often depend on the

level of legitimacy that the securitising agent perceives they will require in order to enact the policies they believe will counter an identified threat.

This is, however, not to imply that the 'general public' would be redundant in the theorisation of a securitisation, if the securitising moves were, for instance, confined to COBR meetings and Select Committees. In the event of an existential threat, one would expect at least *some* level of public engagement, or awareness. A securitisation is likely to have several audiences (Stritzel, 2007:363), and, in the case of an 'elitist' securitisation, we could therefore discern the public as a separate tier of an audience. The status of being 'lower tier' would entail *some* influence over a securitisation, but one would presume that policies could still be enacted through a securitised discourse without the full assent of the secondary audience. It is foreseeable that, particularly over an extended period of time, a secondary audience could have a direct influence not necessarily over the securitising actor, but of the 'primary audience'. For instance, a securitisation might require Members of Parliament to comprise part of a higher audience tier, and these figures will be accountable to their constituents, who would form a lower tier of the audience. If a prominent piece of legislation that had been implicated in a securitisation became controversial in the public sphere, it is understandable that an MP might seek to withdraw their support for the legislation, particularly towards the end of an election cycle. Given this phenomenon, it would be foolhardy to consider a given securitisation to be a fixed entity. Rather, securitisations are contested, fluid and mercurial; the audience that engages with an initial securitising move may be substantively different to audiences that become involved with re-securitising or counter-securitising moves at a later stage.

In the case of this thesis, which scrutinises official discourse between 12th May 2010 and 24th June 2016, no major changes were identified in the constitution of the audience. The 2015 election ousted the Liberal Democrats from the Coalition Government and reshuffled Parliament, but the discursive handling of the threat of cyberterrorism was not altered. However, were this research to be retrospectively updated to account for new discourse in, say, 2025 or 2030, it is possible that trends and substantive shifts in the agency composition of the discourse could be identified.

It is the view of this author that the role of a lower tiered audience extends beyond simply influencing the higher tiered audiences, however. All tiers of the audience can play a subtle, certainly not always overt, role in (re)securitising a perceived threat. This is achieved in a process that has been termed by

Oren and Solomon (2015) as 'ritualised chanting'. In essence, there is no implicit need for an audience to be genuinely convinced by a securitising move. Instead, in order for a securitisation to be successful, there simply needs to be a repetition of the requisite phrasing (for example, 'radicalisation' or 'Islamic extremism'). This chanting forms a performance, and this performance acts as an implicit – whether intentional or unintentional – endorsement for a securitisation. The ingenuity of the 'ritualised chanting' approach to audience participation is that it allows for the incorporation of sceptical or dissenting voices amongst the respective audiences *without* having to resort to labelling these voices as counter-securitising, when this label would be misrepresentative. As Oren and Solomon note, observing "that a significant number of people express doubts or even oppose these policies is perfectly compatible with securitisation so long as the doubters/opponents join in the ritualistic uttering of the securitising phrase" (2015:327). To illustrate this point, one could use the example of the securitisation of Islamic terrorism in the UK; whilst labels such as 'Islamic terror', or 'radical cleric' may be prejudice, ignorant and lazy identifiers that are used to endorse or enhance particular policies, legislation and security cultures, the act of even the dissenters repeating the phrases is a performance that serves to endorse the meanings of the terms, and this, by implication, is an endorsement of the securitisation. Simply by repeating these securitised terms here, in a professional capacity as a Doctoral Researcher and Lecturer, or a personal capacity amongst friends, *I* myself am an actor in this ritualised performance.

Understandably, such inadvertent chanting has implications for the British discourse of the threat of cyberterrorism. Cyberterrorism, like many words adorned with the 'cyber' prefix, is a buzzword that both implies risks to security, and also encapsulates a sense of modernity; of forward-thinking. This thesis will argue that cyberterrorism – possessing no pre-existing case study – exhibits a reduced, or even non-existent, common definitional grounding in British discourse. The malleable nature of the term therefore makes the recourse-to-ritualised-chanting *more* pervasive, because speakers are able to draw on the alluring, alarmist language of cyberterrorism irrespective of whether or not they are objectively speaking of cyberterrorism. Reference to the term 'cyberterrorism', without a consistent understanding of what speakers believe this term represents, will have at least some impact on the degree of ambiguity regarding how a cyberterrorist incident would be *performed* and *experienced*.

A securitisation, created and sustained through discourse, is a fluid and potentially changeable phenomenon, rather than a fixed 'fact'. This is where this thesis breaks away from the 'traditional' approach to securitisation, as established by Buzan, Waever and de Wilde (1998), and instead advocates a Post-Structural perspective. As will be demonstrated in Chapters Four, Five and Six, this thesis has consulted the full official corpus of cyberterrorism in the UK between 12th May 2010 to 24th June 2016 to be able to map and understand how cyberterrorism came to be established as a severe threat to the UK. In this regard, this thesis is empathetic to Snetkov's suggestion, "that Critical Security Studies would benefit from a greater use of longitudinal methods of analysis" (2017:270). Simply scrutinising a singular 'moment', or 'snapshot' of the process implicated in the securitisation of cyberterrorism would, by default, inhibit the analysis of the evolutionary dynamics underpinning this discursive and relational construct.

When a securitising actor attempts a securitisation, the 'thing' that they are attempting to create is not just the new (or pre-existing but perhaps overlooked) conception that something existentially threatens something else. The moment at which the actor makes their securitising attempt is also the moment at which the audience(s), who can either consent to the securitisation or can reject it, are formed. Not everyone will be interested in partaking in the discourse of a securitisation. Perhaps more importantly, not all voices amongst an audience are equal.

Here, Wilhelmsen is instructive:

> "what Buzan et al (1998:27) talk about as 'acceptance of that designation by a significant audience' is, then, in the sense of Laclau and Mouffe, a situation when a particular securitising discourse has become *hegemonic* by naturalising this particular intervention and overpowering others in the broader public (Torfing, 1999:103). Empirically, this is the situation when the description of the threat as 'existential' and of 'the point of no return' and the 'way out' given in a securitising move has gained enough resonance and response in the representations of the audience for emergency action to be undertaken legitimately" (2017:177, original emphasis).

In the context of the UK, the Parliament is the body with the capacity to draft and legitimise new legislation and to amend existing legislation. Where extraordinary measures must be incorporated within legislation, it is clear that, within the context of securitisation, the Members of the Parliament represent a more powerful audience body than those who do not have parliamentary authority.

Analytically, the success (or not) of an attempted securitisation has always depended upon a given audience's consent; however, the underlying conception of the audience as offered by the traditional

framework of securitisation theory has been labelled as 'radically underdeveloped' (Williams, 2011a:212), 'negated' (Balzacq, 2005:179), and a "normative concept in disguise" (Floyd, 2010:50). This under-development has meant that there is an insufficient framework to understand the way in which a securitising act or a series of acts perform in different ways to alternative audiences. For Floyd (2010:51), the original audience was an expression of what security politics *ought* to be, instead of what is. This does not, however, mean that the notion of the audience is redundant. To do away with the audience altogether would be unsatisfactory, but so too would be allowing the audience to remain in a state of cultivated ambiguity. There is a pressing need to develop a framework of the audience that arrests this ambiguity, which is nevertheless sufficiently flexible to maintain utility across differing security issues, legal territories, scales and timeframes.

With respect to the audience, this thesis is positioned within the field of literature that advocates a 'capabilities'-based understanding of the audience. Vouri, for instance, has proposed that audiences are comprehensible by their "ability to provide the securitising actor with whatever s/he is seeking to accomplish with the securitisation" (2008:72). The key characteristic of an audience, therefore, is that they themselves perform a central function in the success or failure of an offered securitisation. Similarly, Balzacq, Léonard and Ruzicka talk of an 'enabling' audience that 'empowers' a given securitising actor (2016:499). In other words, without the active discursive consent of members of the audience, a securitisation may be regarded as either partial or as having failed. The alternative to this conception of an 'enabling' audience, would, in effect, be that which advocates that the audience(s) are what Côte has aptly called 'agents without agency' (2016:543). An audience without agency would not be able to significantly influence a given securitisation process. In effect, the audience's significance within the securitisation framework would be reduced to a symbolic or decorative level. This would question the utility of securitisation theory; if a securitising agent does not meaningfully need to acquire the assent of an audience, their efforts to 'persuade' an audience through securitising moves would be irrelevant to the success or failure of a securitisation.

One of the novel contributions to theory that this thesis offers is the delineation between primary, secondary and tertiary 'tiers' of the securitising audience. Traditional securitisation theory as upheld by the Copenhagen School takes 'the audience' as a monolithic construct. But this lens is too narrow and limits the explanatory power of the theory. In reality, not only do different audience members have differing capacities

to engage with a securitisation, but a securitising actor – if they intend their securitisation to be successful – will be obligated to tailor their message to the specific audience that they are talking to. Certain messages, for instance, the concept of cyberterrorism existing as a Tier One threat to the UK, is a soundbite that could conceivably be successfully assimilated across several if not all audiences. Conversely, a technical paper detailing partnership between public and private bodies in relation to cyber security may be of interest to a smaller or more exclusive audience.

For the purpose of this thesis, I divide the audience(s) involved in the securitisation of cyberterrorism into three distinct 'tiers'. The first tier is the most exclusive, and is comprised of individuals who can also perform as securitising actors. This tier is formed of senior members of the Cabinet Office. The second tier incorporates MPs and Lords, including the opposition Frontbench, and Junior Ministers. Lastly, the third tier, which is theorised but not analysed in this thesis, incorporates the audiences outside of Whitehall who may still be interested in understanding and speaking about the threat of cyberterrorism. Professional figures such as journalists could be considered members of this third tier, as could the public at large. Certainly, I could create further divisions in the audience. Adopting the framework for another securitisation – say, the macrosecuritisation of the Global War on Terrorism during the tenure of the 2001-2008 George W. Bush administrations – could perhaps only be rendered meaningful with a double-digit level of tiers. The Global War on Terrorism engaged a vast array of government and non-government bodies in many nation-states which will have experienced this trans-national endeavour differently and will have been speaking to differing audiences. Theorising the Congress of the USA as an entity that is directly relatable to the German Bundestag would not adequately capture the organisational context in which these two political bodies operate. There would be a risk that nuances in the speech acts exhibited in the respective legislative bodies could be overlooked.

Furthermore, this thesis only handles audience tiers in a 'vertical' fashion, wherein each tier is differentiated by its capacity to influence a securitisation. The top, or first tier, incorporates those who, as a result of their position and authority, are able to engage also as securitising agents. Each subsequent tier has a correspondingly lower degree of authority to directly influence the British securitisation of cyberterrorism. However, it is within reason that one could also map tiers on a 'horizontal' basis in addition to the vertical. In the case of the international Global War on Terrorism, for example, the acting governments of France and

Germany could be differentiated as separate 'horizontal' tiers. By drawing tiers on a horizontal basis, one could actively account for the relatively similar capacity of each government to influence a securitisation on an international and domestic level, whilst acknowledging that each of the two horizontal tiers may be speaking to some shared, and some distinct, other audience tiers (for instance, the European Commission, the French public and the German public).

In this thesis, the vertical three tiers are differentiated by their capacity to engage with the securitisation of cyberterrorism in the UK. These tiers are not fixed, and it is entirely possible to conceive of an individual crossing two or more tiers. For instance, an individual may be able to listen, speak and/or write professionally as a vested actor in a security-relevant field and do so as a member of a higher tier of the audience than they would if, say, they were speaking informally in summer attire and sandals at a barbeque party. Accordingly, these three tiers are as follows.

The first tier incorporates the securitising actors themselves; when they are not speaking directly on the matter of the securitisation of cyberterrorism, it is reasonable to assume that a securitising actor can themselves return to membership of the audience. The first tier of the audience is also distinguishable by the degree to which they are privy to classified or restricted information. In order for a securitising call to feasibly be heard by all tiers of the audience, the call has to be declassified and at an open-source, non-technical level. Realistically, it would be possible to incorporate within securitisation theory the possibility to securitise behind closed doors; even if we cannot empirically analyse these securitising calls until the relevant information is disclosed either through successful freedom of information requests or the expiration of confidentiality. For instance, were a COBR meeting convened amidst a significant cyber breach in the UK, this meeting would, in and of itself, be a symbolic securitising gesture capable of rippling across all tiers of the audience, assuming that the meeting were publicly disclosed. Whilst this thesis analyses spoken and written discourse and does not pay great attention to the function of symbolism and gesture, the potential for gestures to play a role in securitisation and security politics more broadly should not be overlooked (Jarvis, 2015; Jarvis and Legrand, 2017). A discursive moment that is relevant to a securitisation does not exist in a vacuum, but is instead inscribed with meaning through the paraphernalia surrounding the performance. The act of a Minister appearing in the Commons chamber, standing before the dispatch box is, potentially, a substantively different performance to them standing before a conference audience to deliver a similar

statement. On paper, the words of these two theoretical addresses may be much the same, but the context of the respective performances would matter. For instance, the intended direct and indirect audiences may differ and the tone of the speaker may be more relaxed in a congenial conference hall than in the adversarial Commons chamber.

Whilst the discussions within the briefing room would only be privy to a select and vested group of actors, this discussion could have a paramount significance for the course and nature of the securitisation of cyberterrorism. By creating 'tiers' in the audience, one is able to accommodate within the securitisation framework the exclusionary 'spaces' in which an overarching securitisation can be heard and mediated. Granted, it is somewhat unsatisfactory to incorporate into analysis that which one is excluded from and cannot access (although this analysis could be 'filled in' in subsequent publications when, or if, classified documents, minutes, telephone conversations or instant messaging communications are released), but simply eschewing outright the existence of these spaces would detract from the accuracy of securitisation theories' explanatory power. Acknowledging that securitisations can be mediated in exclusionary spaces and that the government itself can be an audience participant would also ease the legitimate criticism of securitisation theory relating to its perceived Western democratic centricism (Roe, 2008; Salter, 2008b; Vouri, 2008). In the context of an authoritarian state with limited democratic accountability, for example, insisting that the broader populace must be an element of the empowering audience would theoretically enfranchise people who may not possess meaningful means to engage with a securitisation. In this case, the securitisation theorist would be imposing a normative preference for liberal democracy onto structures of meaning-making security discourse. The delineation between 'securitised' and 'politicised' would be blurred, given that wider aspects of societal life in a non-democratic society may not offer a general population avenues for civic engagement and critique.

The second tier of the audience is the one on which this thesis places greatest emphasis, given this thesis's focus on the *official* (as opposed to, say, 'general') narrative of the securitisation of cyberterrorism in the UK. For the purpose of this thesis, this second tier of the audience is comprised of MPs and Lords. This second tier is distinguished from the next tier – the third – because these figures are able, potentially, to directly influence legislation, and certainly to voice their views on a given issue in both a privileged and on-record environment. For many Members of the Parliament, particularly those beholden to party whips who

are not on the front benches nor significantly involved in committees, the ability to stand up during a debate, catch the Speaker's attention and speak on record is a key outlet for them to advocate on behalf of their constituents on the central matters of the day.

The mechanisms of process and debate within Parliament are mechanisms of ritual, even, as Jarvis (2015) has noted, during the pre-determined debates regarding intended additions to the list of proscribed terrorist groups in the UK[6]. As noted earlier in this chapter, this thesis is in part informed by Oren and Solomon's "WMD, WMD, WMD: Securitisation through Ritualised Incantation of Ambiguous Phrases", in which they propose with respect to the 'WMD' discourse surrounding the 2003 invasion of Iraq:

> "that the acceptance of this oft-repeated utterance by an audience consists not in becoming 'convinced' or 'persuaded' so much as in the audience echoing the phrase, joining in a chorus-like fashion with the securitising actor to produce a repetitive, ritualised chant … the audience is not being performed *to* – it is not akin to theatre spectators who sit inertly in their seats during the play before applauding the stage performers at the end of the evening. The audience rather partakes in the production of the 'political spectacle'" (2015:315-316, original emphasis).

The crux of the matter is this; even if the members of the audience do not have a firm grasp of what cyberterrorism is, nor the technical specifics entailed within a hypothetic cyberterrorist attack, they are still capable of reinvigorating the securitisation of cyberterrorism by repeating the term 'cyberterrorism'. This is especially so when they make this repetition in the same breath as the term 'Tier One' or a similar sentiment expressing severe risk. For Oren and Solomon (2015:317), the idea that the securitisation framework should be underpinned by a 'marketplace of ideas' essentially casts back to a bygone era; today, and indeed, during the period May 2010 to June 2016 under scrutiny in this thesis, commercial marketing revolves less around detailed descriptions of a product, but instead more around aggressive marketing of brands through repetition, catch-phrasing and sloganeering. Securitisation, as a discursive political process that seeks to capture attention and assert the immediacy of a given threat, adheres to a similar tenet. Phrases such as 'WMD' and 'cyberterrorism' cultivate an ambiguity through multiple instances of repetition, driven by two common properties of ritual symbolism: condensation and multi-vocality (Oren and Solomon, 2015:326; Kertzer, 1988:11). Condensation refers to the way in which a particular symbolic entity can possess a variety

---

[6] British law proscribes terrorist organisations as per Section 3 of the Terrorism Act 2000. The Home Secretary lays an order before Parliament, which must be debated (but cannot be amended) by both Houses. A proscription order has yet to be rejected. See Home Office (2017) for a list of proscribed terrorist groups in the UK. Notably, 'hacking', or 'cyber' specific entities such as 'LulzSec', 'Anonymous' or 'Fancy Bear' are absent from this list.

of ideas, and multi-vocality refers to the way in which a given entity can be understood by different actors in different ways (Kertzer, 1988:11). As will be identified in the ensuing analysis chapters of this thesis, the agents that comprise the qualitative corpus of the British securitisation of cyberterrorism demonstrated both condensation and multi-vocality in their utterances.

The third and final tier of the audience that I have conceptualised for the securitisation of cyberterrorism in the UK is the largest and least exclusive. This third tier incorporates the myriad of members of the public who have elected to express a view on the threat of cyberterrorism, either by providing responses to a poll, by expressing sentiment on social media, writing to a national or local newspaper, or by authoring articles. Given the feasibly almost indefinite size of this third tier, and the vast plethora of spaces and forums in which members of this tier can discuss cyberterrorism (as opposed to, say, the exclusive space of the Commons Chamber), this is potentially the largest of the tiers. Analysis has already been conducted with respect to the cyberterrorism discourse exhibited in the global news media (see Jarvis, MacDonald and Whiting, 2016a; 2016b). Unless intrigue in the field of cyberterrorism diminishes, it is likely that future research will examine data from sources such as popular technology forums, Twitter, polling, psychological studies and other empirical material, to compile a better comprehension of public awareness of this threat. The Cyberterrorism Project, based at Swansea University, and the Global Cyber Security Capacity Centre, based at Oxford University, would both be excellent launchpads from which to invigorate such research. However, due to the time and word-count constraints of thesis research, this thesis under-analyses this third, but nevertheless potentially significant, tier. Given that the members of this third tier are likely to be constituents of the MPs and Ministers who comprise the second and first tiers of the audience – and, in some cases, those who can act as securitising agents – this third tier of the audience possesses agency in their capacity to influence the 'official' securitisation of cyberterrorism. This influence could be exerted in the vast ether of communicative spaces in online social media, blogging, newsletters and awareness campaigns; although these spaces can be unwieldy for the analysis of securitising 'moments'. Influence over the 'official' securitisation of cyberterrorism could also come in the form of frequenting constituency clinics, writing to an MP or Lord, attending local party committees, protesting, signing a petition and offering statements to a parliamentary committee. Were cyberterrorism to become a contested electoral issue, voters could conceivably vocalise an expression in the symbolic act of casting their ballot.

For the securitisation analyst, in cases where confidentiality issues do not apply, these spaces in which the public can engage with British political process could provide more accessible securitisation 'moments' vis-a-vis the more ethereal landscape of general public discourse. Just as with the first and second tiers of the audience, this third tier engages with the securitisation of cyberterrorism through the process of ritualistic chanting, wherein they are able to 'speak back' or 'speak to' fellow members of their tier, as well as members of the other tiers and the securitising agents themselves.

Conclusion

This chapter has detailed the core components of the 'securitisation theory' framework that emerged from the Copenhagen School of Security Studies during the 1990s (Buzan, Waever and Wilde 1998). Whilst this thesis moulds securitisation theory beyond the 'vanilla' 1998 version 1.0 to appropriately make sense of the socially-constructed threat of cyberterrorism in the UK, the fundamental logic of the original framework remains. Given that cyberterrorism has been 'spoken' into existence by British policymakers (Conway, 2005), the threat has not yet occurred, and there is an absence of proscribed terrorist organisations actively championing their desire to attack the UK with internet-mediated weaponry, the framework offered by securitisation theory offers marked utility for the breaking down of the official discourse and the examination of its constituent components.

This thesis does not view the speech-acts that underpin a securitisation as necessarily relying on singular or infrequent grand speeches articulating a threat and the requirement to implement extraordinary measures against it. Instead, inspiration is drawn from Bigo (2006) and Oren and Solomon (2015) to propose a novel relationship between securitising actor and audience. Accordingly, it is suggested that a securitisation is maintained through an ongoing mediation between the vested securitising actors and a 'tiered' audience in an auditorium of a theoretical pantomime performance. This framework offers those who engage in the scrutinisation of securitisations a framework that can take a more comprehensive account of the inter-relationship between securitising actors and audiences, moving beyond the binary response of 'yes, we accept your securitising motion' or 'no, we do not accept your securitising motion' that the vanilla framework ascribed to the audience. By ascribing an audience greater flexibility within a 'tiered' model, the

framework can take account of varying levels of exclusivity amongst the audiences that are inclined to actively partake in the securitisation-making process. For instance, the shadow Home Secretary of the British Government is likely to have a greater scope than a trainee police constable for direct critical engagement with a securitisation ordained by the Prime Minister and Cabinet, but the trainee police constable would still retain *some* capacity to influence a given securitisation, even if this is mostly confined to 'ritualistic chanting' which may be directed at other audience members as opposed to the securitising actor directly.

The next chapter outlines the methodology that has been used to acquire and map documents for the corpus of the official British discourse of the threat of cyberterrorism, and the 'interpretive' method that has been used to analyse these sources.

Chapter Three: Method

Interpretive Approaches

The approach taken in this thesis is broadly situated within an 'interpretive' movement that has developed within International Relations and Security Studies respectfully. This interpretive movement shares common features with Constructivism and Post-Structuralism, particularly with regards to the operational power of ideas and norms in the shaping of policy, whether foreign, domestic or security (Bevir, Daddow and Hall, 2013:166). Importantly, these approaches also reject the positivism that underpins traditional approaches to Security Studies, such as Realism and its variants, because it is believed that this positivism "rests on the erroneous philosophical idea that knowledge of the world can come from pure reason or pure experience" (Bevir, Daddow and Hall, 2013:166). Interpretive approaches differ in several substantive ways. For instance, unlike Structural Realism, the interpretive movement does not consider the structures of an a priori international system to impose limits on the actions and behaviours of agents. Instead, agents (for instance, the Prime Minister, the Home Secretary, or a police spokesperson) are able to adapt and alter norms directly or indirectly, either through conscious or unconscious action. The actions of agents are not conducted in an isolated vacuum; rather, actions are taken in a cumulative, layered history, where each action could be seen to have been influenced by previous actions before it (Daddow, 2011; Lynch, 2014:2). In order to engage with this model of cumulative actions, interpretivists conceive of 'traditions' and 'dilemmas'. Accordingly, "a tradition captures the historical inheritance against the background of which individuals act. A dilemma captures the way people are capable of modifying this inheritance to incorporate novel experiences or ideas" (Bevir, Daddow and Hall, 2013:167).

The interpretive approach offers a dynamic roadmap through which one might resist an urge for flagrant positivism, which, if treated as an object of faith in Social Science, can support or spur potentially misaligned or even disastrous policy decisions. This approach is particularly pertinent in the context of Critical Terrorism Studies, in which the comprehension of terrorism not as a criminal matter but instead as a concern of politically-motivated pseudo-warfare has encouraged a self-fulfilling prophecy where manufactured fear of 'terrorism' in British society feeds a demand for such attacks to be carried out, because

of the disproportionate reporting and reciprocity that such an attack would receive. To an interpretivist, facts are not established on a neutral, vacuumed playing field in which all vested commentators have dutifully purged themselves of their pre-existing biases, experiences and knowledge before entering. Even if one ardently sought to purge oneself of pre-existing bias and subjective experience that might interfere with an objective identification, this would be a fruitless endeavour. Knowledge is acquired when human beings interpret new experiences through a continually fluid prism that is unconsciously tempered by what we have already experienced and learned (Hay, 2011:168). To point this out is absolutely not to undermine the facility of human knowledge, but rather to emphasise the inherently intersubjective nature of our processes of understanding and to introduce measures that we may take in order to assuage the potential net harms that can arise from drawing conclusions of knowledge. Indeed, whilst *all* knowledge is tainted with subjectivity, not all knowledge is tainted equally.

Bevir and Rhodes (2005), whose co-authored publications on British politics and interpretivism have been integral to the formation of the interpretive approach, have sought to justify to the linking of the concept of 'belief' with the concept of 'practice'. This linkage is elucidated by the following excerpt: "whenever we act, we commit ourselves to certain concepts. For example, if we use a pen to fill in our tax form, take it to the tax office, and pay by cheque, we commit ourselves to beliefs about the existence of certain objects" (Bevir and Rhodes, 2005:179). In conducting an activity such as paying taxes, one also engages with one's own identity role; for instance, one would have to assess whether one is implicated in the obligation to pay tax. Alternatively, if there was an opportunity to avoid taxation, one would not only make a rational cost-benefit analysis of the benefits of supplemented income versus the risk of penalty (with this rational calculation itself a form of belief influenced by other beliefs), but also whether one would self-identify as a criminal or not.

Some people choose to avoid paying their full, bona fide tax, whilst others do not. To an extent, structure will play a significant role in the decision to pay or not pay tax; some individuals will have practical access to the means of tax avoidance whilst others face a barrier to entry. However, two people in the exact same circumstances may elect to act differently. As Bevir and Rhodes note, whilst we cannot know a priori how people may respond to a specific circumstance, we can make conjectures "that seek to explain practices and actions by pointing to the conditional connections, beliefs, traditions, and dilemmas" (Bevir and Rhodes,

2005:181). In this context, practice is "a move or thrust into an only partly known and knowable world"; in acting, an individual extends their "intentions and understandings into this indeterminate world without being able to predict how its agency will effectuate itself and impact us" (Wagenaar, 2012:92). Beliefs inform an actor of the likely 'feedback' that they will receive from a particular practice, allowing for some degree of conjecture towards a desired outcome, and indeed, that given practice may lead to other agents altering or reinforcing their beliefs.

Drawing data and findings from such inferences of the inter-connection between belief and practice has not been without contention within the field of Social Science. Whilst practices can be observed and recorded, beliefs are decidedly less tangible. Colin Hay voiced perhaps a widely-felt concern when, in a published symposium, he noted that it is "not clear why those wedded to a foundational epistemology should have any confidence in the inferences drawn by interpretivists" (2004:145). Indeed, to voice this bluntly, to some figures in Social Science, the interpretive approach – which in essence involves interpreting others' interpretations – may appear as a form of social commentary with little objective merit; a pithy endeavour in re-publication. It is easy to empathise with this concern. Issues for the purposes of peer-review are also obvious; if one follows the logic of the interpretive approach, scholars themselves are not immune from the scourge of pre-existing bias and knowledge, and two scholars can disagree on their respective interpretations of an interpretation.

Bevir and Rhodes acknowledge this concern (2005:183-184), but they maintain that there is likely to be at least some form of bedrock of socially determined facts that a given community (scholarly or otherwise) would accept as true in a given time and space. Furthermore, in order for interpretive research to have merit, Bevir and Rhodes proposed 'rules of thumb' that aim to encourage intellectual honesty; consequently, scholars engaging with an interpretive approach should take criticism seriously, prefer standard rules of evidence and reason, and align with positive, speculative responses rather than those that attempt to merely block or distort criticism (Bevir and Rhodes, 2005:184). In essence, a model interpretive account should be accurate, comprehensive and consistent. Bevir and Rhodes (2004:159) maintain that to view belief and tradition as independent of one another would be to tread the path of a 'mysterious' concept of scientific rigour that is inappropriate for human action.

The research approach of this thesis draws upon the interpretive school because it offers opportunities that cannot be afforded with more dogmatic schools of thought. Cyberterrorism, at least in the British state's understanding of the term has not, at the time of writing, occurred; indeed 'kosher' cyberterrorism can be considered a belief. This is the belief that there are, presently and in the foreseeable future, terrorist groups operating inside or outside of the UK who actively wish to attack British critical national infrastructure with cyber weapons and who may possess the capacity to develop or to acquire such weapons. As Converse noted in the 1960s, "belief systems have never surrendered easily to empirical study … indeed, they have often served as primary exhibits for the doctrine that what is important to study cannot be measured and what which can be measured is not important study" (1964:205). Applying an interpretive approach allows one to critique how agents engage with their perceptions of cyberterrorism. These perceptions are, to a certain extent, elucidated in the narratives that vested actors provide in public-facing spaces. Such public-facing narratives can be scrutinised through securitisation theory, in order to assess their interplay with security politics in practice.

The next section provides some elaboration on the respective notions of 'discourse' and 'identity'. These are central concepts that underpin the ensuing analysis in Chapters Four, Five and Six.

Discourse and Identity: Some Basics

Discourse, and the scrutiny of discourse, is a central component of this thesis. In this section, I will explain what is involved in a discourse analysis approach to social scientific enquiry, as well as why this approach is well-suited to the study of the socially-constructed cyberterrorist threat to the UK. I will outline the sources that will be drawn upon in the analysis chapters that follow, and I will also specify how these documents are handled in order to arrive at meaningful findings.

What is a discourse? The Oxford English Dictionary defines discourse as "written or spoken communication or debate" (2016a); in essence, 'discourse' is the term applied to the material that human beings write or say about a given issue. Laclau and Mouffe note that it is only through meaning-making that real world phenomena can become real to ourselves as social beings, and it is this articulation of the social world that is characterised as discourse (2001:105). Discourse is said to be "coterminous with the social"

(Torfing, 2005:8), and it is upheld as the central system of social interaction (Phillips and Jorgensen, 2002:35).

It is important to note that discourses are not fixed, a priori perceptible objects 'out there' and categorisable in the agreeable fashion that one might see, touch, smell and categorise flora and fauna. A fitting analogy might be that discourses are a sort of Play Doh forged and moulded collectively by a given group of human beings; discourses are malleable, transferable, duplicable and also vulnerable. Many discourses surround the same issue simultaneously, often overlapping, complementing and contesting. For instance, if one took the discourse(s) surrounding the consumption of tobacco in the UK, one would likely find an 'official' discourse from the Government that endorses high tobacco duties and prohibitive legislation, a complementary discourse from NGOs such as ASH, and competing discourses from smoking advocacy groups such as Forest, along with the public relations departments of multinational tobacco firms. Furthermore, the public would nurture a plethora of varying discourses in pubs, on web forums and at the water cooler. Because discourses are not a priori entities to be seen and discovered, we can say that discourses are actualised in their usage by people in 'discursively ordered' relationships (Shapiro, 1989:11). What is meant by this is that people communicate on a given issue or topic using pre-constructed or pre-ordained language practices (such as terms, adjectives, or any signifying means of expression). Words such as 'good', 'bad', 'terrifying', 'illegal' all serve to shape the communication between human beings, identifying phenomena in mutually agreeable packages that reside in human languages. As Baker-Beall writes, discourse refers to "systems of thought composed of ideas, beliefs and practices … that structure how we think about a particular subject" (2016:31). Applied in sufficient volume (either absolute or relative), language practices acquire traction and acceptability, potentially to the extent that one could identify a discourse as being hegemonic. Discourse analysis approaches the study of discourse not as a Fox Mulder-esque endeavour to discover hitherto concealed 'truths' behind such hegemonic discourses, but instead seeks to scrutinise the rhetorical bases underpinning the efficacy of particular discourses (Zulaika and Douglass, 1996:xi).

In her excellent defence of discourse analysis as a method of social enquiry, Milliken (1999) stresses some 'commitments' that are held by those who utilise this approach. The first of these, she wrote, was to the "concept of discourse as structures of signification which construct social realities" (Milliken, 1999:229).

This construction is achieved through the establishment of 'common sense' (Ashley and Walker, 1990). An example of such a common sense could be thus: the inhalation of tobacco smoke is carcinogenic and public policy should aim to decrease smoking behaviour as part of an endeavour to maximise the longevity of human lifespan and wellbeing in elderly life. To place oneself in a counter position to this discourse is, increasingly, to ostracise oneself, to appear as irrational or even encroaching instability in its Foucauldian sense, as the language of cigarettes-as-health-concern is upheld beyond controversy (Foucault, 2006; Holzscheiter, 2005:733). In essence, a discourse formation can be said to place limits on the epistemic, subjective and ethical bases within which a range of possible statements is possible (McKenna, 2004:14). This is important; discourse analysts do not deny that structures of human relations exist. Rather, any structures that do exist are partially instead of permanently fixed, rely on discursive construction and mediation, and could be subject to cessation if participants will it so.

Remaining on this analogy, the aforementioned common sense did not always exist. Although anti-tobacco sentiment is recorded as early as the beginning of the 17th Century, with King James I's *A Counterblaste to Tobacco* (1604), it was arguably not until the US Surgeon General's *Report on Smoking and Health* (1964) that expert and official discourses spurred the wheels of international policy making into the task of reducing tobacco consumption. The 1931 image of a otolaryngologist (or at least a male model dressed as a stereotypical doctor) recommending the smoking of a 'fresh' Camel cigarette to give one's "throat a vacation" (see Stanford School of Medicine, 2016) today appears absurd, but it is indicative of the substantial changes that can occur within a discourse – whether scientific, governmental, or cultural – and the impact that undulations within discourse can have on real-term policy. This is a universal quality of discourse; the discourse of the threat posed by cyberterrorism to the UK is no exception. Discourses, including discourses of security, are not fixed phenomena (Doty, 1998:92); they are man-made and susceptible to change either because agents within the discourse alter them (internal), or factors outside of the discourse force a structural change, such as a scientific revelation or an otherwise significant incident (external).

That being said, discourse *has* to have at least some temporarily fixed meaning in order to exert influence on policy and human action. A completely ethereal and ever-mercurial discourse would not be able to exert such an influence because the agents engaging with that discourse would be unable to find mutually

agreeable definitions and 'nodal' points of discussion. As Baker-Beall has noted, the "partial fixing within discourse is important in the sense that it allows us to 'know' and act upon what we 'know'" (2016:32). Identifying this partial fixing can be described as locating the 'momentary essence'; "the aspect of its structure by which it is able to have an effect at some specified moment" (Banta, 2012:391).

By definition, the condition of 'knowing' something relies upon a knowledge of what it 'is not'. The tenet of identity and the process of identification are both key here. As Aradau has written, "all signification is based on differentiation … no identity can be self-identical and no alterity is pure – both are enmeshed and identities are dependent upon the traces of other identities" (2010:108). Consequently, we can describe discourse as a process that categorises and packages phenomena through binary classifications, so that human language can interpret and redistribute knowledge, much like a computer's CPU relies upon the conversion of signals into binary code. Influenced by Derrida's (1981) philosophical writing, this is Milliken's (1999:229) second commitment of discourse studies. Importantly, this binary opposition engenders a power relation; one element of the binary opposition is said to be privileged against the other. In the case of a securitisation, a thing to be securitised, such as an IBM Bank Communication System[7], is identified as a referent object and placed in a privileged position in a binary formation against threatening hackers. Under certain circumstances, the characteristics by which the threatening hackers can be identified could be categorised as sufficiently risk-worthy to justify potentially extraordinary measures. As Edkins and Pin-Fat note (1999), a point of significance is that identities (and identifications) are inherently fluid; identities cannot be considered 'settled', nor can an identity ever be 'complete' or finalised, because identities are inherently harassed by the phenomena that must be excluded in order for the identities to exist in the first place.

I refer to the IBM Bank Communications System as an example of IT architecture because in this thesis, the identified thing-to-be-secured is critical infrastructure and information systems, wherein a compromising of these systems could endanger lives or cause significant disruption and/or panic. An inanimate piece of critical infrastructure acquires this significance (and indeed, is assigned its 'critical' identifier) because of real-term ramifications to human life that could arise from its compromising or

[7] A modular system supporting financial transactions including SWIFT, CHIPS, DTC, FEDWIRE, NBES and TELEX.

malfunction. Infrastructure cannot 'talk back', nor can it form or articulate its own identity. Nevertheless, identities can be said to be attributed to the infrastructure because human actors assign them and (re)articulate them so that the otherwise inanimate architecture acquires conveyable meaning. Consequently, this thesis is not concerned with the threat that cyberterrorism poses to other internet users, but rather the epicentre is an overarching 'common sense' *British security* entity, concentrated on critical national infrastructure.

From the early 1990s onwards, there has been a significant degree of literature produced that discusses the potential for a disconnect between 'virtual' and 'real' activities, experiences and communities. These discussions, pertaining to the usage of computers, were reminiscent of similar debates that had occurred a few years earlier, concerning the (un)reality of television viewing (Heeter, 1992; Reeves, Detenber and Steuer, 1993; Reeves, Lombard and Melwani, 1992; Sheridan and Furness, 1992; Zeltzer, 1992). Whilst contention can certainly surround a binary divide between what can be determined 'real' and 'virtual', it remains that the then newly-acquired ability of individuals and communities around the world to communicate inexpensively and instantaneously – with people whom they may never physically meet – presented a distinct environment that had not existed beforehand in such an inclusive format. Reactions to the 'real' and 'virtual' juxtaposition were mixed; Bingham, Valentine and Holloway (1999; see also Valentine and Holloway, 2002) distinguish between what they call 'boosters', who were those who saw the emergence of the virtual as a positive development (for instance, see Heim, 1991; Kollock and Smith, 1996; Thu-Nguyen and Alexander, 1996; Wellman and Gulia, 1999), and 'debunkers', who regarded virtual phenomena as inauthentic (for instance, see McLaughlin, Osbourne and Smith, 1995; Stoll, 1995:24).

Some users of internet-mediated communication and services will not report a disjoint between 'real' and 'virtual' experience, and such a distinction between analogue and digitally mediated experiences may appear counter-intuitive. For these users, the twinned experiences are one and the same. In the mid-1990s, committed "researchers at the MIT Media Lab carried computers and radio transmitters in their backpacks, keyboards in their pockets, and digital displays embedded in their eyeglass frames" (Turkle, 2008:121). These researchers persevered with their 'cyborg' endeavour, despite physical wounds caused by the weight of the equipment and the perturbed reactions from their university peers in an image-conscious age group. Given that a significant majority of British citizens carry internet-enabled smartphones with them almost at

all times (Ofcom, 2015), broad populations in the UK today are not unlike the mid-1990s MIT pioneers. Turkle (2008) referred to smartphones and laptops as 'always-on/always-on-us' communications devices, which converted their users to *tethered* selves. The term 'tethered self' refers to the manner in which the user occupies a liminal space between their immediate physical surroundings, and their lives exhibited within the glass screen. Indeed, for avid users of internet-enabled communication, these devices connect them not to a secondary or diminished 'virtual' environment, but to what they perceive as 'real' and of greatest priority; the family and friends whom they call and text, the push-activated workplace email account, and their various social media feeds.

Cooley's (1902) concept of the 'looking-glass self' could prove illuminating here, particularly regarding the identity formation of heavy social media users. According to Cooley, the looking-glass self forms through the "imagination of our appearance to the other person, the imagination of his judgement of that appearance, and some sort of self-feeling, such as pride or mortification" (1902:104). Robinson (2007) draws on Cooley's 'looking-glass self' to suggest that, in the context of text-based roleplaying, online interaction creates a 'cyberme' identity. For the purposes of roleplaying online in the text-based multi-user domains that Robinson refers to, or indeed more contemporary online game platforms such as a World of Warcraft server (Bainbridge, 2010; Bessiere, Seay and Kiesler, 2007), this is an interesting and effective label. However, I would be uncomfortable with a strict distinction between 'actual' identities of individuals and the identities that might be attributed to their online personas. For some users of social media, the touch-screen glass on their Apple or Android smartphones could be superimposed as the looking-glass medium through which they both articulate and receive the identity which to them may appear entirely real. An undergraduate raiding their current account overdraft who exclusively posts extravagant photographs of restaurant dinners and holidays onto the service *Instagram* might be offering an artificial inflation of a given reality, but to them and to their audience the webpage is nevertheless a reflection of their real selves. As Wertheim notes when she refers to online role playing, "'I' - that is, my 'self' - can play any number of different personae online and off, but that does not mean I become fragmented … I am still me, unless I become a true split personality like Sybil" (1999:250).

For the purposes of this thesis, I do not pro-actively impose a conceptualised divide between virtual and real spheres, although there is some analysis of such a divide through the interpretation of the British

discourse that constructed the threat of cyberterrorism. The securitisation of cyberterrorism in the UK is not the sole preserve of those individuals who use the internet directly or on a frequent or habitual basis; in the event of a theoretical catastrophic cyberterrorist incident, death and destruction would not discriminate between those who were connected to the internet at that time and those who were not; thereby making a distinction between 'real' and 'virtual' potentially superfluous. That being said, the 'cyber' element of cyberterrorism does present peculiarities both on a practice and a theoretical level, because entering cyberspace involves a partial transcending of physical space and bodily boundaries (Papacharissi, 2002:21; see also Donath 1999). The ability to convey and receive information over long distances without the aid of horse, boat or train did, of course, exist with the invention and installation of the telegraph, telephone and terrestrial broadcasting, but the economies of scale offered by internet-enabled services substantively democratised communicative capabilities. One understated identity alteration that internet-enabled communication forces upon users by default is that of the user-as-a-consumer; as "every instance of participation involves a transfer of data which has been economised" (Goldberg, 2010:707); ISPs and cellular carriers act as commercial gateways for connections to internet services, paywalls restrict access to content, and seemingly 'free' services such as those offered by Google are intuitive advertising platforms that convert the user base into the product to be sold and sold-to. Because internet infrastructure relies upon a physical electrical and fibre-optical network and the information it carries directly interplays with human interaction, cyberspace should not be considered a strict 'virtual' sphere. Nor should cyberspace be considered a traditional 'public' space or commons, given the commercialised nature of the infrastructure and standards upon which it resides and operates.

Identity is a recurrent theme underpinning the process of meaning-making in the discourse that is mapped and analysed in the subsequent chapters, as identity is a central component of the articulations that permit securitisation processes to exist and have meaning. Indeed, the intersubjective perception of "insecurity becomes the product of processes of identity construction in which the 'self' and the 'other', or multiple 'others' are constituted" (Shepherd and Weldes, 2007:532). The binaries of threatening or protective identities become cemented in legislation, thereby enforcing a rigid delineation between acceptable, legal activity/behaviour and unacceptable, illegal activity/behaviour. In the case of terror and counter-terror, a securitised discourse would act to delineate between permissible violence and illegitimate violence.

In principle, a change in the acceptability of a discourse is required in order for its related legislation to be debated, mediated, passed and applied. For instance, in 1986, Robert Schifreen and Stephen Gold became the first British nationals convicted for the illegal breaching of a computer system when they accessed the Duke of Edinburgh's Telecom Gold[8] account. They were convicted under the Forgery and Counterfeiting Act 1981, and the conviction was repealed on appeal because hacking was not within the legal remit of forgery. The actions committed by Schifreen and Gold, which were *normatively* illegal in official discourse were not, at the time, explicitly illegal in the written, legislated discourse of British law. To address this legislative deficit, the *Computer Misuse Act* 1990 (CMA) made any unauthorised accessing of a program or data a criminal offence, punishable with a maximum penalty of a five year incarceration term (Legislation.gov, 1990). As mentioned in the introduction, a computer program or data offence could also be prosecuted through the *Terrorism Act* 2000 under certain circumstances. Whilst the British intelligence services have wide-ranging exemption from such legislation through the Intelligence Services Act, it is nevertheless of interest that the 2015 revision of the CMA included a clause that explicitly exempted the intelligence services from prosecution through the CMA. Some cynical commentators attributed this to a panicked attempt to assuage a then-ongoing legal challenge brought by Privacy International and seven ISPs against GCHQ computer hacking operations (Connett, Barber and Griffin, 2015.

This section has outline the significance of 'discourse' and 'identity' in the social construction of the threat of cyberterrorism to the UK. In later chapters, the 'threatening' cyberterrorist identity is found to be a partially-fixed discursive nodal point that is placed in juxtaposition to a security 'guaranteeing' cyber actor, epitomised by the British state. The next section outlines tools of discursive persuasion; metaphor and descriptive language.

Metaphor and Descriptive Language as Tools of Persuasion in Securitisation

The significance of *seeing* in our material experience of human reality is embedded in the English language; the phrases, "great, I'll *see* you soon", "I *watched* Reading FC play last night", and "I *saw* a great business opportunity" are revealing precisely in this regard. To say that, as human beings we are

[8] An early email service, launched by BT in 1982.

fundamentally visual creatures is almost an indisputable assertion. As Nicholas Mirzoeff noted in his *An Introduction to Visual Culture*, there is "a growing tendency to visualise things that are not in themselves visual", a culture that "does not depend on pictures themselves but the modern tendency to picture or visualise existence (1999:5-6). The approaches to the study of social science that rely on discourse analysis have been criticised for largely ignoring the visual, and the field would benefit from ceasing to overlook this element of human communication (Wang, 2014:265). Nevertheless, David Campbell was succinct when he stated that "the existence of the world is literally inconceivable outside of language and our traditions of interpretation" (1998a:6), and there is "no way of bringing into being and comprehending non-linguistic phenomena except through discursive practices" (1998b:25). The meaning of imagery is related to a linguistic message, through an inter-relative process that Roland Barthes (1977a:39) called 'anchorage'.

Through the process of condensation and anchorage, parts of the original entity expires and ceases to exist. A perennial problem with linguistic identification and characterisation is, therefore, that no single concept could be sufficient to adequately define a phenomenon and all the intersubjective human experiences that have existed or may exist in correspondence with it (Bleiker and Chou, 2010:16). Lacan refers to a very similar concept when he suggests that crucial aspects of being (that is, human experience) are lost when such experiences are reduced to the format of linguistic words or another easily interpretable signifier (Lacan, 2007). This is not to say that such an expiration is a bad thing; indeed it is essential in order for human beings to successfully communicate inter-subjectively meaningful information. But it is a phenomenon that must be acknowledged and is useful in the context of cyberterrorism, which, for the time being, was conceived in, and exists entirely through, discourse.

El Refaie's (2003) article, "Understanding Visual Metaphor: The Example of Newspaper Cartoons" is particularly useful here. Referring to the concept of the visual metaphor, Refaie writes that "an abstract entity cannot be depicted at all without the mediation of symbols or metaphors" (2003:85). Along with their ability to engage with the emotions of a target audience, metaphors serve to provide such anchorage for discursive entities, whether they are clear and accessible, or murky and ambiguous. This anchorage is achieved through a process of 'condensation', where polysemous visual concepts are reduced to a linguistic entity that can be easily disseminated and communicated (Morris, 1993). Let us briefly take the example of the American and Israeli sanctioned Stuxnet attack against Iranian nuclear centrifuges in 2009 and 2010. In

this example, a wide plethora of images are implicated, for instance individuals using desktop computers to code a virus specifically designed to disrupt a SCADA system, the Iranian Siemans SCADA system itself, not to mention panicked nuclear scientists at the Bushehr site once they noticed the issue (the Stuxnet virus was designed to 'trick' control panels into falsely displaying the centrifuge's status as operating under normal conditions). Of course, these are just a few images of feasibly infinite examples that were implicated in this attack. Communicating such an ethereal concept is challenging, and it is for this reason that condensation is applied. When news stories on the Stuxnet attack carried images relating to the Stuxnet attack, most stories were typically accompanied by images of the infrastructure of the Bashehr site, either the outside of the building, or the inside; with personnel, or without (for instance, see Dehghan, 2011; Shubert, 2011; Williams, 2011b). These images were themselves a condensation of other images and the carriers of those images through a form of superimposition (see Bataille, 1985; Kress, 1994), but without the anchorage provided by the text, they would simply have been images of large infrastructure and men in white overalls or security fatigues. Images can be condensed into other images ad infinitum for as long as a viewer is capable of interpreting what they see and imagining further images in their own mind, but it is only with the application of linguistics that the image finds an anchor that can be distributed as a partially-fixed entity within a discourse. As Nietzsche astutely noted, "we believe that when we speak of trees, colours, snow, and flowers, we have knowledge of the things themselves, and yet we possess only metaphors of things which in no way correspond to the original entities (1999:144-145)". Nietzsche understood truth to represent "a mobile army of metaphors, metonyms and anthropomorphisms … a sum of human relations, which have been enhanced, transposed, and embellished poetically and rhetorically, and which after long use seem firm, canonical, and obligatory to a people" (1982:46-47).

This thesis does not offer an analysis of the aesthetic representation of cyberterrorism, although it does draw on the popular fictional narrations depicted in film 2012 James Bond film, *Skyfall*. A direct, concerted analysis of imagery would require a greater pool of 'cyberterrorism imagery' than currently exists. There *are* dozens of news stories concerning cyberterrorism reported by the British press (Chen, Jarvis and MacDonald, 2014), and these stories tend to be accompanied by stock imagery of hands behind a keyboard, or shady masculine figures against a background of bright binary code (for instance, see Hammond, 2015; MacAskill, 2010; McTague, 2014), but such news stories from the broadcasting and newspaper outlets do

not represent 'official' discourse, at least not in the sense of being ordained and published by the British Government.

In contrast, official security documents produced by the British Government tend *not* to be accompanied by imagery. This does not necessitate that representations of what the cyberterrorist threat looked and felt like was absent from the corpus. Indeed, it is entirely possible for securitising actors, and their intended audiences, to draw upon textual discourse that directly influences the interpretation of what a threat looks and feels like.

Particularly in cases where the visual characteristics of a phenomenon may be indistinct, the conveyance of such characteristics through text-based communication can be accomplished through the use of metaphor. The Oxford English Dictionary defines metaphor as "a figure of speech in which a word or phrase is applied to an object or action to which it is not literally applicable", or "a thing regarded as representative or symbolic of something else" (2016b). With analysis of discourse – and, in particular, discourses of securitisation – it is of fundamental significance to adequately accommodate not only the articulation of a speech/text act, but also to account for the interpretation (the listening or reading) of that item (Weldes, 1999). A plethora of metaphors, adjectives and projected narration were identified in the corpus that is mapped and analysed in the subsequent chapters. For instance, cyberterrorism has been described variously as a 'Tier One' threat (Cabinet Office, 2010b:47), a threat of potentially 'catastrophic' consequence (Osborne, 2015), an 'evil' akin to the threat posed by the Third Reich (Jarvis, 2015), 'depraved' (Hayes, 2016), and an 'unknown menace' (Soames, 2015). Whilst in several respects cyber weaponry is unique vis-a-vis pre-existing weapons systems, its characteristics have been likened to chemical and nuclear weapons (Patten, 2010; Hannay, 2010).

Spencer has written an excellent article on the role of metaphors in the social construction of terrorism (2012). Spencer notes that there are two ways of understanding metaphors. The first of these is 'rhetorical', which is where metaphors are 'convenient labels' (Chilton and Lakoff, 1999:56) that replace one word with another; in essence, these metaphors serve to make speech easier and more eloquent (Charteris-Black, 2004:25; Chilton, 1996a:359). Such metaphors 'decorate' discourse without affecting its original intended meaning (Beer and De Landtsheer, 2004b:5). The second understanding of metaphor usage is described by Lakoff and Johnson (1980:5); whereupon metaphors are used to understand and experience one

kind of thing 'in terms of another'. It is stated that metaphors "are devices for simplifying and giving meaning to complex and bewildering sets of observations that evoke concern" (Edelman, 1971:65). As Spencer notes, these metaphors "thereby make humans understand one conceptual domain of experience in terms of another by projecting knowledge about the first (familiar) domain onto the second (more abstract) domain" (2012:396).

In the context of a securitising move being heard or read by the target audience, metaphors function in this recourse-to-metaphor because they are capable of activating pre-existing knowledge in the target audience that pertains to a threatening Other. This pre-existing perception of an enemy Other can operate without the enemy Other being physically present, because this imagined entity is created by the Self (Kinvall, 2004). Irrespective of whether or not a member of a target audience has personally met an individual who could be objectively labelled a 'cyberterrorist', they nevertheless harbour a perception of what a cyberterrorist is and what cyberterrorist activities may look like, which they have gleaned from engagement with print and broadcast media, personal conversations, personal use of internet services, and a thought-process that internalises new information through these filters. As Hulsse and Spencer have suggested, the projection of metaphors onto an 'unknown' serves to 'create' a reality (2008:578). Acknowledging that metaphors possess this discursive capability raises the analytical capacity of discourse analysis with regards to the securitisation of cyberterrorism; a threat that, at the time of writing, is based on conjecture.

Importantly, metaphors do not entail a clear set of policies; they are not an agenda nor an explicit plan. Instead, they can be said to "open up space for policy possibilities", offering "a discursive construct that frames the situation in a certain way" (Spencer, 2012:399). To put it another way, metaphors are "more likely to influence policy indirectly through their impact on the decision maker's general approach to an issue; they will be part of the conceptual foundation, not a detailed policy map" (Shimko, 1994:665). Linguists have called metaphors with (potential) policy ramifications 'figures of thought', a term that can be applied to metaphors that consist not simply in representing phenomena, but in *depicting* them (De Leonardis, 2008:34). By establishing a similarity between two concepts when, previously, there was not one, such metaphors actively *create* a reality. As Schwarz (2015:67) has noted on the usage of the term 'surgical strike' to describe contemporary air-to-ground military strategy, this is a metaphor that actively serves to

make a messy, inevitably bloody attack appear cleaner than it actually is. One result of this particular metaphor could be to mitigate popular discontentment with Western air-to-ground involvement in locations such as Syria, Yemen and Pakistan.

One does, however, heed Hall's warning that one should not take a complete and uncritical acceptance of the prowess of metaphor (1993:48). Hall argued that an analysis that is over-reliant on metaphors would take for granted the social order that already exists. Accordingly, one views metaphors as part of a repertoire of tools that securitising actors may seek to apply when they develop their securitising moves. As a tool, metaphors accept and draw upon at least some degree of pre-existing 'common' or 'open-source' knowledge. Metaphors, along with all discursive practices, are inherently allowed to exist because a system of state, government and societal sovereignty imposes limitations on action within space and time (Walker, 1993:176).

Furthermore, in drawing upon metaphors and descriptive narration in the analysis throughout this thesis, it is important to clarify that this thesis does not – indeed, cannot – make assumptions regarding the *intentions* of securitising actors whenever they draw upon a metaphor for the purpose of illustrating threat or otherwise. As Paris (2002:433) has noted, when scrutinising the invocation of metaphors by political and security actors, one does not have the access to the private and unguarded communications between central figures that would provide the necessary evidence to make cogent, non-speculative assumptions regarding the actual intentions of actors. Even if one were to have access to a grand cache of emails between Cabinet Ministers and their aides through a *Wikileaks* dump, this would still only provide signals towards the intentions of securitising actors, rather than sufficient material to provide a comprehensive qualitative assessment. The mindset of a securitising actor is their own domain. Again, whilst I vicariously enjoyed Mulder and Scully's heroic, melodramatic adventures to uncover American government and extra-terrestrial conspiracies and de-securitise details of a grand plot to prepare the Earth for colonisation by aliens (Soukup, 2002), I am not seeking in this thesis to uncover collusion or malpractice behind the British Government's securitisation of cyberterrorism. Here, metaphors and descriptive narration are considered tools – irrespective of whether or not the securitising actor genuinely believes in the objective reality of that metaphor – that are used to coerce target audiences. Whilst I do not engage in research naively, there is an extent to which discourse(s) must be taken at face value.

The usefulness of metaphors, and the tenet that makes them distinct as linguistic tools, is in the power of persuasion and illustration that is entailed by their ability to engage the emotions of an audience. Paris details this succinctly when he writes that to:

> "suggest that a foreign leader is behaving 'like Hitler' … is apt to produce a more emotional response among listeners than the suggestion that the foreign leader is behaving 'like the head of an oppressive, authoritarian regime', because strong emotions are associated with the evocations of Hitler's name" (2002:428).

Referring to an entity as 'Hitler-esque' is an overt means of portraying it in a denigrating light, but a further powerful tenet of metaphors is that they need not be so explicit as to rely on actual usage of, say, the H-word. Metaphors can be 'summoned' through subtle means with 'trigger phrases' or 'oblique references' that evoke a metaphor without explicit enunciation of the metaphor itself (Paris, 2002). It is feasible, therefore, that an array of threatening notions could be ascribed to a socially-constructed 'cyberterrorist' identity through the evoking of subtle metaphors.

The following section of this chapter details how sources have been gathered for the purposes of analysing the discourse of the securitisation of cyberterrorism.

Source Acquisition

Hansen's *Security as Practice* (2006:59-64) has been instructive with respect to the approach that this thesis takes to source acquisition. Accordingly, Hansen (2006) proposes four routes to the study of securitisation: 1) the official discourse of the government, 2) political opposition and the media, 3) cultural representations and popular culture, and lastly 4) marginal political discourses emanating from non-government organisations and academia. Like Croft (2012:99-100), I believe that there are significant rewards for both one's analysis and findings by addressing all four of these pools of sources. However, due to the space constraints of a thesis, the corpus that has been mapped and analysed in the subsequent chapters includes the official discourse of the Government and the discourse exhibited by backbench MPs and Peers. The Ministerial contributions are the foremost focus of analysis, given that those speaking on behalf of the Government and the security agencies are the actors who are capable of signalling and making calls for securitisation. It is from these sources, which include resources such as Security Strategies, officially

sanctioned reports and interviews with Ministerial figures, that one may locate the language and metaphors raising the spectre of securitisation. Accordingly, official Governmental sources are the overriding occupation of in particular, Chapter Four, which traces the emergence of cyberterrorism as a significant threat by the Government. Chapter Six will also consider Hansen's third pool of sources. Paying tribute to the role of popular culture is not frivolous, particularly in the case of cyberterrorism; indeed, cyberterrorism emerged from fictional authorship in the 1980s and was nurtured by popular culture until arguably the late 1990s or even the terrorist attacks in New York and Virginia in September 2001.

Sources were selected from the time period 12th May 2010 to 24th June 2016. This time period, spanning six years, was selected because it represents the tenure of David Cameron's premiership as Prime Minister leading a Coalition Government from May 2010 to May 2015, to his premiership of a majority Conservative Government until his resignation announcement following the June 2016 European Referendum result. This is not to say that David Cameron is the chief author of the UK's cyberterrorist-as-threat narrative, nor is it to imply that considering events before May 2010 and after June 2016 would be superfluous. Rather, Cameron's six year tenure as Prime Minister of the United Kingdom provides a contemporary duration from which I was able to draw sources. Disallowing material outside of the premiership of David Cameron reduced the variable factor that would be present had one included the tenure of another Prime Minister. Indeed, a comparison of the securitisation of cyberterrorism between eras of British politics is not the overriding focus of this thesis. Whilst one recognises that a Major-Blair-Brown-Cameron-May genealogical study would be an interesting approach, such a comprehensive endeavour would necessitate a thesis of its own. Furthermore, the threat of cyberterrorism to the UK was not publicly detailed by the Government as a 'Tier One' threat until the publication of the Coalition's *National Security Strategy* (Cabinet Office, 2010a:11). Whilst the strands that are mapped in the subsequent chapters could be traced further back in time beyond May 2010, the central strand upon which the securitisation of cyberterrorism rested – that cyberterrorism represented a severe or 'Tier One' threat to the UK – was only formally established in 2010.

The years 2010 to 2016 represent a timespan during which the UK was more connected to, and reliant on, internet-mediated communications than in any six years previously in British history. This time period also saw significant developments that had at least some form of impact on the security narratives,

such as the Snowden revelations in 2013, and the UK's first mature political debates about surveillance legislation in the internet age. May 2010 to June 2016 also represents a duration during which the classification of the threat from international terrorism fluctuated between 'substantial' and 'severe' (MI5, 2015). Finally, June 2016, roughly mid-way through my tenure as a scholarship PhD student at Nottingham Trent University, felt a fitting cut-off point at which I decided I would no longer draw new sources and would concentrate on writing up the thesis.

There are some exceptions; that is, under particular circumstances, I have consciously selected some sources that were published *prior* to May 2010. In such cases, I have deemed the source to be a *living* document that is still active within British discourse, whether official, public, or legislative. For instance, the *Terrorism Act* 2000 is still a highly relevant, living document that operationalises efforts to define what terrorism and cyberterrorism are, and establishes the parameters under which these individuals identified as credibly epitomising these threats can be punished through the judicial system.

Throughout my analysis, priority was given to a select number of primary texts that I considered representative of the construction of a common roadmap for the securitisation of cyberterrorism in the UK. These sources were constituted by 110 unique items. These included official documents written and published by the British Government and their agencies, speeches by Ministers and Hansard contributions by Members and Peers, and three public polls. These discursive items provided stable 'nodal points' where officially-sanctioned partial fixings of discourse could be identified. For the purpose of interpretive analysis, this items of discourse were assumed to represent the dominant 'official' narrative, carrying agency as a series of respective 'securitising moments'. The subsequent chapters which map the 110 unique sources constitutes the first comprehensive mapping of the official British discourse of the threat of cyberterrorism.

These 110 unique sources were, mostly, acquired by running searches for 'cyber-terrorism', 'cyberterror', 'cyberterrorism', 'cyber-terrorist' and 'cyberterrorist' against the gov.uk website and the Hansard search engine within the timeframe parameters of 12th May 2010 to 24th June 2016. These searches elicited contributions within the Commons and Lords chambers, public-facing Government documents, press-releases, external Ministerial speeches and third-party documents published in co-authorship with Government departments. A limited selection of sources, for instance, David Blunkett's (2015) interview with the *Yorkshire Post*, or the polls that are referenced, were acquired by running targeted searches against

the Google search engine or emerged from pre-existing knowledge about the discourse of cyberterrorism. Results from the gov.uk and Hansard searches included those which may not have expressly stated 'cyberterror/cyberterrorism/cyberterrorist', but did make references to both 'cyber' and 'terrorism' (or a derivative of terror) within the space of a few sentences. When I encountered a relevant source in these targeted searches, I saved the excerpt (for instance, paragraph) that surrounded the relevant quote into a document, in which I also included relevant metadata. This metadata, which was applied to all collected Hansard contributions and external Ministerial speeches, included a Parliamentarian's political party, their constituency, their Governmental or shadow Governmental roles, their membership of committees at the time of the reference (and date of them leaving such posts, if this occurred before 24th June 2016), any relevant special interests and the title of the debate in which the Speaker had solicited their contribution. Running the variations of the queries against the search engines typically elicited numerous identical hits, and multiple hits of the same source were discounted after the first record of the source had been made. Furthermore, some Parliamentarians, particularly Conservative backbenchers, had a penchant for parroting lists of threats to the UK in their contributions in the Chamber, in which they would include 'cyber' and 'terror' respectively, without a concerted linkage between these two threats (for instance, see Beith, 2010; Hodgson, 2016; Burnham, 2016; Hammond, 2016). Where a sufficiently direct inference could not be made to 'cyberterrorism' (as opposed to, say, 'cyber and flooding and health epidemics and terror and climate change') from such lists of threat, these sources were saved in the corpus but excluded from the mapped discourse included in the subsequent chapters of this thesis. This is not to say that such contributions are entirely irrelevant to the analysis of the official social-construction of the threat of cyberterrorism to the UK; indeed, parroting a list from a brief that you have been given by a party whip is entirely consummate with the notion of securitising 'ritualistic chanting'. Chanting is chanting, whether or not it is coerced or scripted by a superior. However, such parroted listing of threat did not closely align with the strands that could be elicited from more substantive and novel excerpts gleaned from Hansard contributions and the other sources upon which the mapped discourse has been built.

The next section outlines the interpretive method that was applied to map and analyse the 110 unique sources.

Interpretive Method

In the opening section of this chapter, it was noted that one of the predominant criticisms that can be made of interpretive approaches to the study of social science is that interpretivism relies upon intellectual honesty. In this section, I hope to outline an approach to the study of the construction of the threat of cyberterrorism in the UK that meets the requirement – indeed, duty – of ensuring transparency in one's research approach. Some approaches are better suited for this task than others. For instance, Ashley's (1988) 'double reading' approach to interpretivism was tempting; when 'double reading' sources, a researcher first reads a source 'as is', in its literal and unadulterated form, and will follow this with a second reading that incorporates a holistic perspective (for example, the manner in which a source may be interpreted by varying audiences, via which distortion and evolution of the original meaning may occur). Ashley's case for double reading is convincing, however, it is my preference to make the treatment of the sources more explicit. As much as feasibly possible, I have sought to reduce the extent to which readers of this thesis need to place their trust in my research integrity, and instead rely on the transparency of the research methods.

My approach to the analysis of these resources is inspired by, and similar to, that which is applied by Baker-Beall (2016) in his *The European Union's Fight Against Terrorism*. I have approached the sources in a two-step process, which I will detail here.

The first of these steps is to map the discourse, by identifying the components of each of the sources that serve to make them *work*. Each source was held under the scrutinising lamp of three analytical questions. Firstly, in order to ascertain the most prominent language in the 'cyberterrorism-as-threat' discourse, I asked the question: "What are the key words, terms, phrases, labels, metaphors and beliefs in each source?". Once the language characterising the sources was identified, I asked the question "What are the main strands of the discourse?". 'Strands' was the term that I applied to themes located in the sources. These strands concurrently served to construct the 'cyberterrorism-as-threat' discourse. In asking this question of the sources, I directly acknowledged the intertextual nature of discourse; that is, sources are not observed to be operating in their own vacuum, but instead they are in a flux of agreement, competition and negation.

The final element of this discourse 'mapping' was implemented to extract the identity construction from the sources. I asked the question: "How does the discourse construct a threatening cyberterrorist Other that warrants combating?".

The next stage of analysis sought a detailed understanding of the functioning of the discourse. In order to achieve this, I funnelled sources through a further three questions. As described previously in this chapter, in discourse analysis, discourse is considered to be *performative*, and it gains this performative traction when there is a partial fixation of meaning; both of the concepts and of the identities of the actors. In order to explicitly draw out sites of partial fixation, I asked the question: "How does the discourse partially fix the meaning of the identities and events that it implicates"?

The second question that I used to orchestrate my understanding of the functioning of the discourse was: "What knowledge and/or practices does the discourse legitimise, and what knowledge and/or practices does it serve to exclude?". The endeavour to assess what is legitimised and excluded by discourse(s) is a means through which one determines the very essence of discursive power. As Foucault (1977; 1980; 2003) convincingly suggested, discourse operates by rules of exclusion; delineating between what can and cannot be said, who can and cannot speak, who is correct and who is not. Of course, such power is not simply symbolic; distinguishing these binaries serves to permit or even encourage some actions whilst constraining others, determining which actors can or cannot act in a certain way.

The third and final question to illuminate the functioning of the discourse was: "To what extent can the construction of the threat of 'cyberterrorism' be considered novel?". Asking this question sought to draw out the aspects of the discursive construction of the threat of cyberterrorism that drew inferences from existing discourse – such as the generic post-9/11 discourse of counter-terrorism in the UK – and those aspects which could be said to be new.

Discursive Strands

Having asked these questions of the 110 unique sources, I arrived at a set of 'strands' and 'sub-strands' to which, in aggregate, all items in the corpus (exempting parroted lists) related to at least one. These strands were 'Cyberterrorism as a Tier One Threat to the UK', 'Cyberterrorism as Unique Temporally',

‘Cyberterrorism as Unique Spatially’, and ‘From Fiction to Reality’. The temporal and spatial strands were more meaningful when divided into distinct sub-strands that could be identified from the corpus. Accordingly, the sub-strands for the ‘temporal’ uniqueness of cyberterrorism were ‘New Terrorism’ and ‘Escalation of Threat’. The sub-strands for the ‘spatial’ uniqueness of cyberterrorism were ‘Physical versus Cyber’ and ‘Safe Havens’. The following chapters detail the mapping and analysis of these strands. Chapter Four concerns the notion of cyberterrorism as a ‘Tier One’ threat; the most threatening category in the taxonomy of threat offered by the Coalition Government in 2010. This is the strand that is regarded as having operated as the central pillar for the securitisation of cyberterrorism in the UK. Chapter Five details the ‘temporally’ unique strand, which is the notion that cyberterrorism is a threat that has escalated over time and will continue to do so for the foreseeable future. Lastly, Chapter Six details the ‘spatially’ unique strand, which, at its core, is the idea that cyberterrorism operates in two spatial environments; one that is based on human identity, and the other which is purely technical. Chapter Six also includes the ‘fiction’ strand, which is the proposition that due to the void in the epistemology of cyberterrorism that results from the absence of a cyberterrorist incident to-date, select fictional narratives have, in part, filled this dearth in the narration of the experiencing of cyberterrorism.

Conclusion

This chapter has introduced the ‘interpretive’ approach to Security Studies, and has elucidated on the roles of ‘discourse’ and ‘identity’ in this field. This chapter has also noted the utility of particular forms of discursive articulation, which can appear in the form of descriptive narration and in metaphors. From the outset, cyberterrorism is a novel case study because it is an event that is securitised before it has ever occurred. Consequently, in order for the securitising actors and members of the audience to meaningfully communicate with one another about cyberterrorism, they must resort to linguistic tools that allow them to express their views on cyberterrorism in relation to other phenomena that are more fixed in meaning. This chapter has detailed the means by which sources have been acquired and handled, in order to undertake the mapping and analysis that forms the basis of the next chapter. This chapter has also outlined the three question that I asked the sources in order to map them, the three questions that directed the analysis, and the

strands and sub-strands that were identified from the corpus. Lastly, this chapter has introduced the four strands and four sub-strands that the mapping discerned from the 110 unique sources that have been handled from the corpus.

The next chapter details the central pillar of the construction of the threat of cyberterrorism to the UK via the 'official' political British discourse. In this fourth chapter, I map and analyse the first of the four 'strands' that I have found through my mapping and analysis of the sources. This strand is the notion, seminally introduced by the Coalition Government of 2010, that cyberterrorism represented a 'Tier One' threat to the UK. Chapter Four also applies the novel 'Pantomime' framework to the British securitisation of the threat of cyberterrorism, a framework that could be used to substantiate the relationship between (and within) the securitising actors and the audience.

Chapter Four: The Discursive Construction of the Threat of Cyberterrorism to the United Kingdom

This chapter serves three functions. Firstly, this chapter maps the discourse of Whitehall that established cyberterrorism as a 'Tier One' threat to the UK. The effect of this mapped discourse was that the threat of cyberterrorism was removed from a 'politicised' status, in which it was largely not discussed and had not been categorised as a national security risk, and was instead 'securitised'. Using the approach outlined in the preceding chapter, this fourth chapter applies an interpretive discourse analysis against the mapped discourse to unpack *how* the threat of cyberterrorism came to be regarded as a 'Tier One' level risk, the highest threat category presently used by the British Government. Lastly, this chapter proposes that one core consequence of the securitisation of cyberterrorism was that cyber weaponry was not implicated in this securitisation; the nefarious identities who may wish to use such weapons were. As a result, the securitisation of cyberterrorism did not exempt the possibility of positive applications for cyber weapons. On the basis of a socially-constructed representation of a cyberterrorist identity, the securitisation articulated a particular illegitimate form of cyber violence. Given that this socially-constructed representation tacitly not did exclude the possibility of legitimate forms of cyber violence, it is suggested that the securitisation of cyberterrorism did not merely serve to justify extraordinary measures against perceived cyberterrorists, but it also tacitly endorsed the UK's cyber weaponry program. Whilst the subsequent chapters diverge from the traditional Copenhagen School framework of securitisation and unpack the process-driven production of meaning in the securitisation of cyberterrorism, this chapter scrutinises the speech acts through the lens of the traditional framework. Before unpicking the nuance of the securitisation of cyberterrorism, it is first important to establish what this securitisation *is*, and what it has served to *do*.

This chapter therefore serves as an analytical foundation for the subsequent two analysis chapters. Each chapter is divided into two core sections: a mapping of the pertinent discourse from the corpus, and a critical analysis of this discourse. The critical analyses will address the impact of the discourse on the security practice(s) of the threat of cyberterrorism and the novel contributions that are offered by the cyberterrorist case study for the framework of securitisation theory. Having fleshed-out the process through which cyberterrorism came to be articulated as a 'Tier One' threat to the UK, Chapters Five and Six will map

and analyse additional elements of the discourse that served to emphasise cyberterrorism's uniqueness in temporal and spatial terms respectively.

Cyberterrorism as a 'Tier One' Threat to the UK: The National Security Documents

In 2010, the newly-formed Coalition Government published two policy documents that would underpin the prioritisation and categorisation of security concerns for the subsequent five-year period. The first of these was the *Strategic Defence and Security Review* (Cabinet Office, 2010b), an overarching review of the funding and structure of the British armed forces. This was the second version of the review; the first having been introduced by the then-Labour Government in 1998 (House of Commons Library, 1998). The impetus for the publication of the 2010 version of this document was twofold (Mulholland, 2010). Firstly, the joint Conservative-Liberal Democrat Government was keen to invigorate its own brand of security policy. Secondly, the Government wished to stem the then-£38 billion overspend in the Ministry of Defence's procurement budget. By explicitly listing the most notable threats facing the UK, and ranking these according to their likelihood and their scale of harm, this document, in conjunction with the *National Security Strategy 2010* (Cabinet Office, 2010a) sought to be the public-face of UK security priorities for the duration of the Coalition Government. The 2010 *National Security Strategy*, entitled *A Strong Britain in an Age of Uncertainty* was the third version of this document. The first, entitled *Security in an Interdependent World* (Cabinet Office, 2008), had been published by the then-Labour Government in 2008, and revised with a 2009 Paper entitled *Security for the Next Generation* (Cabinet Office, 2009). Whilst the publication of a national security strategy is a relatively new phenomenon in the UK, the practice has a longer precedent in the USA, where administrations have regularly developed strategies after the Reagan administration introduced the seminal edition in 1987 (White House). The British documents published in 2010 established – on a formal basis – the stature of cyberterrorism as a Tier One threat to the UK. 'Tier One' is the classification that the British Government used to distinguish the threats to British national security that – taking account of both likelihood and impact – were the highest priority (Cabinet Office, 2010a:27).

The *National Security Strategy* of 2010 was the first British security strategy to specifically cite cyberterrorism as a serious threat to the UK. It detailed "cyber attack, including by other states, and by

organised crime and terrorists" (Cabinet Office, 2010a:11), alongside 'international terrorism', 'international military crises', and 'major accidents or natural disasters' as a Tier One threat to British national security. The strategy warned that:

> "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. 'Stuxnet' … was seemingly designed to target industrial control equipment. Although no damage to the UK has been done as a result, it is an example of the realities of the danger of our inter-connected world" (Cabinet Office, 2010a:30).

Regarding the severity of the threat posed to the UK by cyberterrorism, the *Strategic Defence and Security Review* was unambiguous in its emphasis that this threat was operating on an unprecedented scale. The document stated that "over the last decade the threat to national security and prosperity from cyber attacks has increased exponentially. Over the decades this trend is likely to continue to increase in scale and sophistication, with enormous implications for the nature of modern conflict" (Cabinet Office, 2010b:4). According to this document, there were four central responses to the highest priority risks over the subsequent five years, including the development of "a transformative programme for cyber security, which addresses threats from states, criminals and terrorists" (Cabinet Office, 2010b:11). In order to counter "physical and electronic threats from state and non-state sources", the *Review* called for "investment in new and flexible capabilities such as cyber to meet emerging risks and threats" (Cabinet Office, 2010b:13). The *Review* implored that "the risks emanating from cyber space (including the internet, wider telecommunications and computer systems) are one of the four Tier One risks to national security. These risks include … the actions of cyberterrorists" (Cabinet Office, 2010b:47). This key document surmised that "these threats … are likely to increase significantly over the next five to ten years, as our dependence on cyber space deepens" (Cabinet Office, 2010b:47). This notion, that cyberterrorism was articulated as a threat that would increase over time, is scrutinised in detail in the fifth chapter.

The *Cyber Security Strategy* of 2011 was similarly clear in its construction of cyberterrorism in a particular way; as a Tier One threat to British national security. Under the subheading of *Changing Threats*, this document recognised that "the Government's 2010 *National Security Strategy* identified cyber attacks on the UK as a 'Tier One' threat – that is, one of our highest priorities for action" (Cabinet Office, 2011:15). The document further noted that:

> "cyberspace is already used by terrorists to spread propaganda, radicalise potential supporters, raise funds, communicate and plan. While terrorists can be expected to continue to favour high-profile attacks, the threat that they might also use cyberspace to facilitate or to mount attacks against the UK is growing. We judge that it will continue to do so, especially if terrorists believe that our national infrastructure may be vulnerable" (Cabinet Office, 2011:15).

The concern that terrorists might elect to use cyberspace to conduct an attack against British critical infrastructure and computing systems did not recede across the period under scrutiny. A policy paper published in May 2015, entitled *2010 to 2015 Government Policy: Cyber Security*, noted in its opening sentences that "with greater openness, interconnection and dependency comes greater vulnerability. The *National Security Strategy* categorised cyber attacks as a Tier One threat to our national security, alongside international terrorism", continuing by imploring that "the threat to our national security is real and growing. Terrorists, hostile states and cyber criminals are among those targeting computer systems in the UK" (Cabinet Office, 2015b).

The 2015 version of the *National Security Strategy* maintained the status of 'cyber' as a realm of Tier One threat to the UK. This document noted that "the range of cyber actors threatening the UK has grown. The threat is increasingly asymmetric and global … non-state actors, including terrorists and cyber criminals can use easily available cyber tools and technology for destructive purposes" (Cabinet Office, 2015a:19). The cyber threats to the UK were upheld as 'significant and varied', including "cyberterrorism … and disruption of CNI as it becomes more networked and dependent on technology, including networks and data held overseas" (Cabinet Office, 2015a:85).

This term, 'Tier One', established a formal classification of cyberterrorism as one of the most significant threats facing the UK. The term also provided a theme that could be repeated, and its repetition, whether consciously or unconsciously, engaged in the (re)securitisation of the threat of cyberterrorism. In effect, the 'Tier One' label emerged as a politically-charged theme that Ministers and MPs 'ritualistically chanted' (Oren and Solomon, 2015) in the Chamber, in on-record interviews and at external events. On record, no Ministers, MPs or Lords sought to detract from the Tier One classification, thereby leaving the label entirely uncontested and establishing – on a political elite level – an unchallenged securitisation. The next section maps and analyses the ritualistic chanting that endorsed the Tier One threat classification.

Beyond the National Security Documents: The Construction of Cyberterrorism as Tier One Threat

This chapter will now detail the instances in which the 'Tier One' and 'severe threat' themes entered the discourse of Ministers, MPs and Lords. In November 2011, the UK Prime Minister David Cameron delivered a *Cyberspace* speech at Downing Street in which he stated that "Britain has prioritised cyber attacks as a Tier One threat … we cannot leave cyberspace wide open to the criminals and terrorists that threaten our security and prosperity" (2011).

Francis Maude, the then-Minister for the Cabinet Office and Paymaster General, spoke relatively frequently on cyber security and cyberterrorism. In a speech at the *International Centre for Defence Studies* in Estonia in May 2012, Maude noted that "we need to protect the internet from hostile actors – the criminals, the hackers, the terrorists – who want to exploit it for less positive ends … in the UK we have rated cyber attacks as a Tier One threat to our national security" (2012a). Maude repeated the 'Tier One' theme in a speech at an *Information Assurance Conference* seven months later, stressing that the Tier One cyber threats were taken 'extremely seriously' by the Government (2012b). The same sentiment was repeated at a *Govnet Cyber Security Summit* in 2014 (2014a).

In 2016, Matt Hancock, then serving his 13-month role as Minister for the Cabinet Office and Paymaster General, reporting to the Chamber on the final annual report of the *Cyber Security Strategy*, paraphrased both the 2010 and 2015 versions of the *National Security Strategy*, to note that both had classified 'cyber' as a Tier One threat to the UK, although he did not express any particular cyber actors as representing this threat (2016).

James Brokenshire, at the time a Parliamentary under-Secretary at the Home Office also publicly invoked the idea of cyberterrorism as a Tier One threat. At a *Securing Asia* conference in June 2012, Brokenshire noted that "cybersecurity has been identified as a 'Tier One' risk in our national security strategy", and warned his audience that "terrorist groups use technology to progress attack planning, communicate and spread their ideology, evade protective security measures and increase the effectiveness of attacks" (2012). These particular comments, from Brokenshire, would appear to align with the concern that the utility of the internet for terrorists is the role that it can play in making conventional – as opposed to cyber – attacks more efficient and accessible. As previously discussed, this thesis does not consider general

terrorist usage of the internet for the purposes of administration or planning to represent an instance of cyberterrorism per se. However, it is worth including Brokenshire's comments here because it highlights a divergence, even amongst Cabinet Ministers, about whether the securitisation of cyberterrorism, when articulated, explicitly does or does not include a threat of terrorists using the internet as a direct means of conducting attacks. Further clarity on Brokenshire's position was highlighted when he delivered a keynote speech at the *Internet Service Providers' Association* annual conference in November 2013, where he restated that "the *National Security Strategy* published in 2010 identifies the risk of hostile attacks on UK cyberspace by *other states* and *large scale cyber crime* as a 'Tier One' priority for UK national security" (2013, emphasis added). Of course, terrorist application of cyber offense is explicitly included in the 2010 version of the *National Security Strategy*, and terrorism is a crime. But 'terrorism' as a discursive entity is generally invoked through use of the word itself; individuals convicted of terrorism offences are typically referred to as *terrorists* rather than *criminals* (for instance, see Chulov and Grierson, 2017 and Parveen, 2017). Whilst Brokenshire did not use his speeches to publicly dismiss the cyber threat from terrorist entities, it is of note that he explicitly referenced states as the predominant actors threatening British cyberspace.

Conservative Ministers were not alone in engaging with the Tier One theme. For instance, some opposition MPs also raised the Tier One theme in the Commons Chamber. Ian McKenzie, Labour Member for Inverclyde, noted in a *Defence and Cyber Security* debate that:

> "cyber attacks have been categorised as a Tier One threat to the UK's national security … terrorists, rogue states and cyber criminals are among those who are targeting computer systems in the UK … performing an attack need not be expensive. With minimal equipment in the right hands, a lot of damage can be done" (2014).

Martin Horwood (2014), Liberal Democrat MP for Cheltenham – notable as the locale of GCHQ's headquarters – also highlighted the Tier One classification in the same debate, and expressed his view that the Government was right to prioritise cyber security funding.

There were no instances in which the securitisation of cyberterrorism was challenged by a Member of Parliament. More explicitly, throughout all of the sources that I have identified, mapped and analysed, there were *no* dissenting voices to be found, wherein an actor could be said to be critiquing, dismissing or challenging the securitisation of cyberterrorism. This tenet is quite remarkable, especially given that a

cyberterrorist – or indeed, any major cyber attack – had not occurred in the UK during the period under analysis or indeed at the time of writing[9].

Interestingly, however, there were two instances – both of which occurred in the same debate – where MPs drew on the securitisation of cyberterrorism to juxtapose its perceived prioritisation against the securitisation of flood-risk. Kerry McCarthy, the Labour MP for Bristol East and the shadow Secretary of State for Environment, Food and Rural Affairs argued that, in reference to a then-recent Cabinet Office Briefing Room A (COBRA) meeting on flooding, Ministers had not prioritised "flood prevention, despite the national security risk assessment citing flood risk as a Tier One priority", further adding that "we would not ignore experts' warnings on terrorism and cyber attacks, so why have the Government repeatedly disregarded expert advice on flooding?" (2016). More tentatively, Mary Creagh, the Labour MP for Wakefield and member of the Select Committee for Environmental Audit raised a similar point, noting that "the 2015 national security risk assessment says that flood risk is a Tier One priority risk alongside terrorism and cyber attacks, so I want to look at the Government's record on flood defence spending" (2016). Luciana Berger, the Labour Co-op MP for Liverpool Wavertree, had made a similar argument in 2013 in a *Climate Change* debate, arguing that "I think we need to deal with some of the risks … the Foreign Secretary's climate adviser has described the security threat alone as being as grave as the threat from terrorism and cyber attacks" (2013).

By not challenging the securitisation of cyberterrorism and cyber and (or) terrorism, and yet invoking it in relation to flood-risk and climate change, these MPs were implicitly endorsing the securitised status (and its implicated extraordinary measures) as a legitimate partially-fixed discursive nodal point. Certainly, three MPs cannot be said to represent the House. But the absolute absence of a recorded challenge to the securitisation of cyberterrorism, and the invocation of it as an example of a legitimate securitisation in debates on flood-risk and climate change highlights the entrenched nature of this particular securitisation.

---

[9] Claims that cyberterrorism has already occurred in or against the UK do exist, although these claims prompt a debate as to what does and does not constitute cyberterrorism. For example, in May 2017, Samata Ullah, an autistic man from Cardiff, was sentenced to an eight year term for distributing sensitive materials in USB cufflinks and advising suspected terrorist figures interested in deploying anthrax in Kenya about online anonymity. *The Times* (Simpson and Gardham, 2017) and the *Evening Standard* (Mitchell, 2017) labelled him a 'new and dangerous breed of terrorist', a 'cyberterrorist'; the *Sun* (Lake, 2017) labelled him a 'James Bond Jihadi'. However, Ullah did not conduct any cyber-attacks per se, and therefore this thesis does not consider him to be a bona fide cyberterrorist.

Were the securitisation subject to concerted contestation, it is unlikely that the MPs would have elected to invoke it in the respective debates.

A similar point was raised during a *Trident* debate in the Commons Chamber in November 2015. Critiquing the necessity of the Trident submarine programme, Brendan O'Hara, SNP Member for Argyll and Bute, noted that "we are increasingly engaged in an ideological war with terrorism … cyber attacks will be among our enemies' main weapons. Indeed, the Prime Minister himself said that Daesh was an existential threat to the UK" (2015). Steven Paterson, SNP Member for Stirling expressed a similar outlook when he stated that "the replacement of Trident fails to address the threats outlined in the *SDSR* and the *National Security Strategy*. Instead, we should invest in … combating cyberterrorism, as well as actual terrorism on our streets" (2015). Here, the two SNP Members were actively drawing on the securitisation of cyberterrorism to critique the exceptional measures that result from the securitisation of nuclear conflict; Britain's continually operative, independent nuclear deterrent. Again, commandeering a securitisation for the purposes of critiquing another securitisation re-affirms the legitimacy of one securitisation in order to seek to destabilise the other as part of a counter-securitising move. Here, it is cyberterrorism that is being invoked as the legitimate securitisation.

David Blunkett, the then-MP for Sheffield, Brightside and Hillsborough added an alternative addition to the cyberterrorism-as-threat discourse when he spoke in the Chamber during a *UK Extradition Arrangement* debate in December 2011. Here, Blunkett appeared to converge rogue state and non-state actors as potentially wishing to engage in cyberterrorism. Accordingly, Blunkett stated that:

> "there are rogue and emerging states in terms of cyber attack and cyberterrorism … and as such attacks are trans-border and affect installations throughout the world, we need to sit down and work out how we deal with that entirely new eventuality, which affects people across the globe. If we do not, we will rue the day" (2011).

This perspective – that states could, at least in principle, engage in explicitly termed acts of cyberterrorism – did not appear elsewhere in the corpus; however, it is of note that a former Home Secretary found this connection worthy of parliamentary record. David Blunkett also stands apart from other Members because he was the only non-Ministerial parliamentary figure to have discussed cyberterrorism with the press. Having been asked by the *Yorkshire Post's* political editor, Adrian Pearson, about the 2015 threat

landscape vis-a-vis the threat landscape in the aftermath of 9/11, Blunkett replied that the UK was situated in a 'technology arms race' with terrorists, malicious actors and criminals in cyberspace, and that:

> "I think there has been a transformation in terms of the nature of the threat. The physical threat is much less … now the threat is cyber, I strongly believe that the attack from cyber, and the dislocation that that could cause to all kinds of essential parts of our well-being, our utilities, our infrastructure, our economy, this is greater than the physical threat, and we really need to take this more seriously in the future" (2015).

Refraining from openly criticising Government policy, Blunkett signalled his perception of the priority risks facing the UK, and drew on his Ministerial experience in the aftermath of 9/11 as an experience of crisis whilst in senior office to legitimise his concerns. Whilst Ministerial figures had spoken openly about the seriousness of the cyber threat from actors such as terrorists, they did not appear to overtly share Blunkett's stance that these threats actually exceeded those of non-cyber threats. It is notable that Blunkett, speaking in the final years of his tenure as an MP and as a former Home Secretary, elected not to critique the securitisation of cyberterrorism, but instead chose to endorse it in separate instances both inside and outside of the Chamber.

Peers also adopted the 'Tier One' terminology to describe the threat of cyberterrorism. In the Lords' Chamber, Baroness Neville-Jones, Conservative Peer, member of the National Security Strategy Joint Committee and serving as the Special Representative to Business on Cyber Security, stated that "we identified terrorism, cyberattack … as major threats to the stability and security of this country. Terrorism and cyberattack were classed as Tier One risks … those risks are not going away; they are remaining" (2014). Three times in the space of four sentences during a debate on the *Strategic Defence and Security Review*, the Liberal Democrat Peer Baroness Smith of Newham invoked the Tier One theme in relation to the threats of "cyber, terrorism and international conflict" (2015). Lord Alderdice, a Liberal Democrat Peer who at the time was a member of the Lords' House Committee, the Liaison Committee and the Intelligence and Security annual report Committee stated that he was "gratified to note the recognition of cybersecurity as a Tier One risk", adding, for emphasis, that:

> "it is important to understand that this is not simply a question of traditional terrorists, whether domestic or international … using the modality of cyber to arrange traditional-style terrorism … there are new ways of engaging in attacks that are mediated entirely through the internet – for example, the damaging of Government infrastructure and the necessary national utilities" (2011).

Lord Taylor of Holbeach, at the time a Parliamentary under-Secretary to the Home Office, also raised the Tier One theme – although in the form of cyber *and* terrorism – warning that "it is now possible that a major cyberattack on essential systems – for example those controlling power supply, communications or food distribution – could result in loss of life, serious illness or injury, serious damage to the economy … national security or severe social disruption" (2014).

Lord Reid, the Labour Peer, phrasing a question to Baroness Neville-Jones in the chamber in November 2010, stated that the Minister and the Government were "correct in identifying cyber as a major new priority in the strategic security review", but asked whether she accepted:

> "that if we are to counter the use of malware, industrial espionage, or, God forbid, cyberattacks from terrorists, possibly in our emergency systems or in the financial sector, we will require above all a new cadre of well-developed, trained and selected young people who are at the very frontiers of thinking in this direction?" (2010).

Baroness Neville-Jones replied that the noble Lord had put "his finger on a very important issue" (2010).

Whilst he did not expressly use the term 'Tier One', Lord Jopling, the Conservative Peer and member of EU-related committees, spoke in reference to "terrorists, criminals and hostile states", stating in a debate on his committee's report on cyberattacks that "anyone who doubts the havoc that successful cyberattacks can cause, and so the importance of protection against these attacks, needs to look no further than the opening pages of our report to see how in May 2007 Estonia virtually ground to a halt" (2010).

Speaking with regards to a different security-policy document, Baroness Jolly, then the Liberal Democrat's defence spokesperson welcomed the *SDSR*'s 'realisation' "that cyber is a real and daily threat", noting that cyber threats "could come from someone's bedroom – that of a terrorist or a bored student. Cyber is real and poses a serious threat to the workings of our machinery and to civil society" (2015).

Lord Touhig, in a debate on the *Queen's Speech*, referenced the 2015 *SDSR*'s classification of cybersecurity to ask the Ministry of Defence Minister, Earl Howe, for updates on the progress of the UK's offensive cyber program for the purposes of countering "the work of people such as ISIL and other terrorist organisations around the world" (2016).

From my review and mapping of the sources, I have determined that the 'Tier One' threat strand is the central underpinning theme that provided the continuity of the cyberterrorism-as-threat construct. Articulated explicitly in three national security strategies published across 2010 to 2015, this theme was repeated or re-chanted (Oren and Solomon, 2015) by Ministers, MPs and Lords. Whilst some limited ambiguity was exhibited with regards to 'cyberterrorism as threat' or 'generic use of the internet by terrorists', most notably with Matt Hancock's (2016) public speech, overall the re-chanting and lack of contestation of this strand indicates that cyberterrorism was successfully securitised and thus removed from the 'political' realm. The securitised status of the threat of cyberterrorism was further substantiated by the references that were made to cyberterrorism as a bona fide threatening entity in unrelated debates on climate change, flood-risk (McCarthy, 2016; Creagh, 2016; Berger, 2013) and nuclear weapons (O'Hara, 2015; Paterson, 2015).

Whilst the 'Tier One' strand provided the official voice of continuity that underpinned the securitisation of cyberterrorism, other strands also existed – strands which provided key nuance that would discursively assemble cyberterrorism into an entity both sharing characteristics with other threats and also possessing unique distinctions. Chapters Five and Six will detail these respective strands; 'Cyberterrorism as Unique' (temporarily and spatially) and 'From Fiction to Reality'.

Public Perception of the Threat of Cyberterrorism

As noted earlier in this chapter, this thesis is primarily concerned with the 'official' construction of the threat of cyberterrorism in the UK. Accordingly, great weight and attention has been paid to the relevant 'moments' offered by Ministers, MPs and Lords. Neither this chapter, nor the thesis at large, offers a discourse analysis of the 'third tier' of the audience implicated in the securitisation of cyberterrorism; the public at large. However, this section will briefly detail the findings of publicly-available polls in relation to the prioritisation of threats offered by the British public when consulted. During the period under scrutiny – May 2010 to June 2016 – there were no publicly-available polls explicitly seeking the views of the general public on cyberterrorism. Nevertheless, there are two polls that could be instructive. This section will also

note a third poll that was targeted at researchers internationally, who were interested in the matter of cyberterrorism.

In a Yougov poll conducted in September 2014, in which respondents were offered a 'tick all that apply' question on serious threats to national security, 69% listed "terror attacks from current or former UK citizens", 68% listed "terror attacks from foreign citizens", and 43% listed "online/cyber attacks that disrupt life in the UK" (Rogers, 2014). This placed cyber attacks below immigration, at 55%, yet above alternative responses such as "resource competition" and "climate change or extreme weather", which were at 30% and 28% respectively. The nature of the options offered in response to the poll effectively means that they are open to interpretation, and, realistically, a perceived threat of cyberterrorism could align with both the categories of domestic/foreign terrorism, *and* cyber attacks. In the same poll, when respondents were urged to select just one response, 30% of respondents listed "terror attacks from current or former UK citizens", 15% listed "terror attacks from foreign citizens", and 3% listed "online/cyber attacks that disrupt life in the UK" (Rogers, 2014). The limited response to the latter option is interesting, and one would suggest that this is perhaps symptomatic of the lack of a case study of a cyberattack significantly disrupting critical national infrastructure – at least in the UK – at the time of the poll being conducted.

In a 'tick all that apply' poll conducted in July 2015, 66% of British respondents were very concerned about the threat of Islamic State, and 34% were very concerned about cyber attacks on governments, banks, or corporations (Pew Research Center, 2015). Whereas the previous poll offered a forward suggestion regarding the severity of the hypothetical cyber attack in question, this poll did not do so; which could perhaps account for some of the percentage disparity between the Pew and Yougov polls.

In 2012, the Cyberterrorism Project, based at Swansea University, conducted a survey by distributing a questionnaire to over 600 researchers, authors and experts who were involved in research linked to cyberterrorism. Respondents were identified by conducting targeted literature reviews, standing in relevant academic communities and the application of two mailing lists, eliciting 118 responses from 24 states and six continents (MacDonald et al, 2013). There were 32 respondents who reported themselves as employed in the UK, representing 27% of total respondents. The greatest proportion of the response was from those employed in the USA, with 41 people, or 35% of the total response. Consequently, the Cyberterrorism Project's survey cannot be said to be representative of a 'British' perspective on the securitisation of

cyberterrorism. However, I note the survey here because it is the largest poll that has been conducted *explicitly* on the matter of cyberterrorism[10]. Some elements of this poll are of particular note. Of 110 respondents who replied to the question "In your view, does cyberterrorism constitute a significant threat?", 58% responded 'yes', 20% 'no', 12% 'possibly/potentially', and 6% were unsure (MacDonald et al, 2013:14). When asked "do you consider that a cyberterrorist attack has ever taken place?", 49% responded 'yes' and 49% responded 'no' (MacDonald et al, 2013:15). In concluding remarks on this survey, Jarvis and MacDonald noted that "it is highly significant, then, that several national legislatures (including the UK) have adopted … [the view that] treats cyberterrorism as a subset of the broader category of terrorism, but simultaneously recognises that there are qualitative differences between the two" (2015:675). They claim that part of this significance was the scope for the conceptual debate surrounding cyberterrorism to infiltrate and influence that which is implicated by terrorism more broadly.

From the polls, it is apparent that members of the public are concerned about both the threat of terrorism and the threat of cyber attacks. Whilst this cannot by default be read as 'the public fear cyberterrorism', it is not a great leap to suggest that the public may consider terrorists as actors potentially interested in conducting a cyber attack against critical national infrastructure. However, given that these polls only offer insight into two of the six years under scrutiny, and they did not explicitly invite respondents to include 'cyberterrorism' as part of the box-ticking exercise, the inferences that can be made are limited. Some of the respondents ticking the respective 'cyber attack' options may have done so on the basis of the perceived threat of inter-state cyberwarfare, rather than attacks launched by non-state actors. Whilst I do not wish to under-represent the voices of the public – or the 'third tier' of the audience in my 'Pantomime' model of securitisation – I would reiterate that this thesis is concerned with the 'official' securitisation of cyberterrorism as articulated at Whitehall. Perhaps the greatest insight that can be gleaned from this section is that there is a pressing need for more research to be conducted on public knowledge and awareness of the threat posed by terrorist application of the internet to conduct attacks against critical national infrastructure. Survey research that offers comparisons of awareness and prioritisation of this threat amongst the populace in the UK, with that expressed in other states, would be of particular value.

---

[10] A 'five years later' poll is currently being conducted by the Cyberterrorism Project team, to which this author has responded.

The penultimate sections of this chapter draw on the discourse that has been mapped here. These sections will further the analysis by detailing the inter-relationship between the strategic documents, the Cabinet Office and MPs and Lords. The purpose of this analysis is twofold. Firstly, this analysis builds on our understanding of how the 'Tier One' securitising speech act performed security and made certain actions possible. Secondly, this analysis illustrates one utility of the audience framework of securitisation theory through the case study of the threat of cyberterrorism to the UK.

Lessons from the Construction of Cyberterrorism as a Tier One Threat: Anticipatory Security

This section and the subsequent section detail some of the key lessons that can be ascertained from the official British securitisation of cyberterrorism, pertaining to our knowledge of what this securitisation has made possible. In this endeavour, these sections will also demonstrate part of the novelty of the case study of the British construction of the threat of cyberterrorism for 'securitisation theory'. In this section, it is suggested that by securitising the threat of cyberterrorism in 2010, the Government's speech act was a performance of 'anticipatory' security.

The decision to identify a corpus of 110 unique sources from the period 12th May 2010 to 24th June 2016 was a conscious one, and the rationale of this choice has been detailed in Chapter Three. It is worth noting, however, that the 12th May 2010 date from which sources were collected missed some elements of the discourse that would have helped to inform the discursive construction of the threat of cyberterrorism and the logic behind the Cabinet Office's decision to declare it a Tier One threat in 2010.

Of particular note is an excerpt from the 2009-2010 *Annual Report of the Intelligence and Security Committee*, which stated that:

> "GCHQ informed the Committee that it is not known whether terrorist groups intend, or have the capacity, to launch significant attacks over the internet but this, along with extremist use of the internet, remains an area of considerable concern. Nevertheless, we have been told by GCHQ that the greatest threat of electronic attack to the UK comes from State Actors, with Russia and China continuing to pose the greatest threat" (Intelligence and Security Committee, 2010:22).

It is interesting that the securitisation of cyberterrorism was established by the Cabinet Office – for the first time in official British discourse – after GCHQ had informed the Intelligence and Security

Committee that as far as the intelligence service was concerned, there was no substantive evidence that terrorists were particularly eager to develop, or were capable of developing, cyber weapons which could endanger British national security. This logic of securitisation befits the 'anticipatory' model of security provision, which will be scrutinised in greater detail in the next chapter.

The establishment of the securitisation of cyberterrorism in the security strategies (Cabinet Office, 2010a; 2011; 2015a) indicates two possibilities. The first possibility is that the Government possessed classified, credible information on the capacity of contemporary terrorist organisations to develop and orchestrate substantial cyber attacks against British critical national infrastructure. The second possibility is that the Government wanted to pre-empt the possibility of terrorists conducting cyber attacks against British critical national infrastructure. These possibilities are not exclusionary; the Government may have both possessed classified information pertaining to the eagerness of terrorist groups to conduct cyber attacks against the UK, and been simultaneously concerned that this was a precedent that would increase in frequency or intensity over time. This latter point – that cyberterrorism was a threat deemed to be increasing over time – is analysed in greater detail with further mapping and analysis in the next chapter.

Whether one, or both, of these possibilities motivated the Government to classify cyberterrorism as a Tier One threat to the UK (Cabinet Office, 2010a:11), it is of note that the Government sought fit to even speak of 'cyberterrorism'. The alternative would have been to incorporate terrorist application of cyberattacks within the pre-existing terrorism-as-threat discourse, rather than develop a new subset of this discourse. To speak of 'cyberterrorism' rather than 'terrorism' is to suggest that this is a form of terror that can be distinguished from a monolithic category of 'terror'. This notion befits the 'New Terrorism' thesis, which is explored in greater detail in the following chapter.

There is a growing field of literature in Security Studies that discusses the notion of 'anticipatory' or 'precautionary' security, governance and justice (for instance, see Anderson, 2007a; 2007b; Adey, 2009; Lackoff, 2007; Massumi, 2005; Goede and Graaf, 2013; Chesney, 2005; 2007; Sarat, Douglas and Umphrey, 2007; Woude, 2010; Zedner, 2007; McCulloch and Pickering, 2009; Kessler, 2008; Opitz, 2011). Marieke de Goede is instructive in distinguishing the difference between 'preventative' and 'precautionary' measures of managing risk. Accordingly, prevention "addresses itself to risks that are … statistically knowable and

calculable according to cycles of regularity … precaution, on the other hand, addresses threats and dangers that are irregular, incalculable, and, in important ways, unpredictable" (Goede, 2011:9).

An example of a preventative management of risk in the UK is the way in which the risk of HIV proliferation amongst intravenous consumers of drugs (IDUs) is handled by British authorities. Reflecting on drugs-policy discourse in the UK, Eva Bertram et al suggested that, following the 1980s HIV epidemic, the British authorities operated within a 'public-health paradigm', with a focus on "strategies for harm minimisation for the individual and society" (1996:215-216). This paradigm essentially works to empower IDUs "to change their behaviour by providing them with information, promoting motivation to change, and providing the means to make those changes" (Bertram et al, 1996:216). Others have described this is as a "consumer-oriented style of service delivery", as the direction of provision is dictated by the requirements of IDUs themselves (Stimson and Lart, 1991). Peter McDermott, one of the pioneers of harm-reduction efforts in Liverpool stated retrospectively that "giving clean needles to strangers didn't automatically mean they wouldn't share, but if you didn't do it they had no access to the right choices … people understood the risks they were running. They actively wanted to minimise their risk". This British health initiative, Bertram et al argued, acted to significantly reduce the proliferation of HIV by the early 1990s, particularly in the urban centres of Scotland (Bertram et al, 1996:216). Philip Bean has suggested that whilst the British model is "a jumble of inconsistencies", it is beneficial to the addict and broader society, because "the drug world is too complicated for one approach to dominate" (2010:133-134). It is notable that the prevalence of HIV in the UK remains relatively high, with 6,095 new diagnoses in 2015, reflecting an infection rate of 11.3 per 100,000 people, compared to the Western European average of 6.3 per 100,000 people; however, only 2% of these new diagnoses were from the IDU population (Chau et al, 2016:4; Avert, 2017). Notwithstanding localised spikes, the HIV risk to the British IDU population is calculable, relatively predictable, and is monitored through the Needle Exchange Monitoring System, established in 2007.

This preventative public health policy does not fit the model of securitisation. This is not to say that health risks cannot be securitised, but one would expect the policies and strategies implicated in a securitisation to be state-focused, whereas clean needle programs are operated by pharmacies and charities and monitored by local authorities and the NHS. However, the securitisation of cyberterrorism, a threat which has not yet become tragedy to-date, and for which there exists little or no publicly-available details

pertaining to the objective likelihood of a terrorist organisation engaging in this kind of activity, fits the 'anticipatory' or 'precautionary' frame of risk management. The threats of terrorism, cyberterrorism and piracy – amongst myriad others – "exceed rational calculation and statistical risk assessment", because the threats "are by their nature dispersed, infrequent, and insufficiently historically documented to enable meaningful predictions" (Goede, 2011:9). It is possible that the securitising agents and members of the audience included in the above mapped discourse who were members of the Privy Council or were senior members of Government departments may have had access to sensitive confidential data tracking the propensity for cyberterrorism to strike the UK. However, until such data reaches the National Archives, agency should not be given to speculation, and taking the securitisation as a whole, the knowledge of the threat that was available across the audience spectrum was limited to the notion espoused in the strategy and review documents (Cabinet Office, 2010a:11; Cabinet Office, 2011:15; Cabinet Office, 2015a:19). This was the notion that cyberterrorism was a possibility and that it could cause significant harm to the interests of British society and economy. Adopting an anticipatory response to a securitisation – as opposed to reactionary – alters the proscriptive logic; operating in a state of 'not knowing' is not cause for inaction. One of the key components to the anticipatory or precautionary logics of risk management is that a dearth of knowledge cannot be "regarded as an excuse for inaction in the face of a potentially catastrophic threat" (Goede, 2011:9). US Secretrary of Defence Donald Rumsfeld captured this logic succinctly during the same infamous June 2002 NATO press conference in which he noted the existence of 'known unknowns' and 'unknown unknowns', when he stated that "the absence of evidence is not evidence of absence" (2002). The notion that one can (or should) imagine threats in order to act upon them before they actualise themselves will be explored in greater detail in Chapter Six.

It is reasonable to suggest that cyberterrorism fits within the remit of anticipatory risk governance. The fear of an anticipated but ill-known future event is a central function of terrorism itself. As Michael Frank has suggested, fear is future-facing and "terrorism systematically exploits this anticipatory nature of fear" (2015:92). Ultimately, to "achieve its defining effect – collective fear of more violence to come – terrorism relies on the belief that the next attack is impending, and that it could happen anywhere, anytime" (Frank, 2015:92). Whilst the UK's experience of the securitisation of cyberterrorism aligns with anticipatory risk governance, there is another significant function of the 'cyberterrorism as a Tier One threat' discourse.

This function, which is analysed in the following section, has served to delineate between legitimate and illegitimate forms of violence in cyberspace. By establishing in 2010 that cyberterrorism exists as a bona fide threat to British national security, the Government simultaneously created a conceptual space in which 'legitimate' forms of cyber violence could exist.

Lessons from the Construction of Cyberterrorism as a Tier One Threat: Legitimising the UK's Cyber Weaponry Program

In this section, it is argued that from the perspective of the British Government, the core utility of securitising the threat of cyberterrorism is that it has tacitly endorsed the UK's own cyber weapons program. By categorising cyberterrorism as a Tier One threat, the Government – acting as a securitising agent – created a partially-fixed nodal point that labelled cyber mediated violence by non-state actors as illegitimate. By default, the creation and maintenance of this partially-fixed nodal point endorsed a socially-constructed reality in which legitimate cyber mediated violence could exist.

A consistent theme in the mapped discourse included in this chapter is the infrequency of technical discussion of the threat of cyberterrorism. If cyberterrorism is indeed novel, it may have been reasonable to expect that one symptom would have been for the discourse to cogently express *why* this novelty can be said to exist. However, during the period of May 2010 to June 2016, instances where an MP, Minister or Lord expressly spoke in explicit detail about the nature of a hypothetical terrorist incident and the objective impact it could have on a given computer system were infrequent. Instead, where MPs, Ministers and Lords elected to discuss cyberterrorism, they typically did so in superficial, even glancing ways. For instance, as noted in this chapter, during a *Trident* debate, Steven Paterson, the SNP Member for Stirling noted that the UK should invest in "combating cyberterrorism, as well as actual terrorism on our streets" (2015). Here, the distinction between cyberterrorism and 'actual' terrorism was not articulated but assumed. Other Members present in the debate, and post-event readers of Hansard, are left to infer what this distinction is. Similarly, in the next chapter, it is noted that during a debate on *Cyber Bullying*, Margaret Ritchie (2013) of the SDLP described cyber bullying as an insidious form of cyberterrorism. Here, Ritchie was not suggesting that cyber bullying is the *only* form of cyberterrorism, but rather, that it was *a* form of cyberterrorism. This thesis does not regard

cyber bullying to be a form of cyberterrorism, and Margaret Ritchie's sentiment was not voiced elsewhere in the corpus. However, Ritchie's comment, which was not admonished by the Speaker nor contested by other Members present in the chamber, is evidence of the multi-vocality of the ambiguous chanted phrase of 'cyberterrorism'. The role of multi-vocality in sustaining an ambivalent securitisation is considered in this section.

Irrespective of how each Minister, MP or Lord chose to interpret the definition of cyberterrorism, there were no instances throughout the corpus where a member of the second tier elected to express a counter-securitising claim. The securitisation of cyberterrorism was not questioned, but instead accepted. It is useful to substantiate the utility of vocalised acceptances of the threat of cyberterrorism.

Security is an inherently intersubjective phenomenon. Furthermore, 'terrorism' as a field, practice and discursive entity has not been categorically defined. There is an inherent 'know it when you see it' element to common comprehensions of what does and does not constitute terrorism (Gentry and Sjoberg, 2014; Richards, 2014). However, whilst a database exists in which thousands of international incidents are categorised annually as 'terrorist' attacks (Global Terrorism Database, 2017), this database barely includes cogent cyber attacks, nor does an equivalent 'cyberterrorist' database exist[11]. The Ministers, MPs and Lords who constructed the discourse that has been mapped in this chapter could not refer to a bona fide historical account of a cyberterrorist incident. Instead, there is some evidence that their views on what a cyberterrorist would *do* has been informed by existing accounts in popular fiction. The role of fictional accounts in informing the British discourse of the threat of cyberterrorism is explored in greater detail in the sixth chapter.

In the absence of a bona fide historical case study of cyberterrorism, there was some evidence that those who referenced cyberterrorism in the corpus did so in a way that nurtured rather than arrested the ambiguity. For example, as noted in this chapter, Ian McKenzie, the Labour MP for Inverclyde, reported that "terrorists, rogue states and cyber criminals are among those who are targeting computer systems in the UK … with minimal equipment in the right hands, a lot of damage can be done" (2014). This excerpt exhibited three ambiguities. Firstly, 'terrorists' are included amongst other actors who may wish to use the internet to

[11] Searching the Global Terrorism Database for 'cyber' returns six hits, ranging between the years 2001 and 2013. Two of these incidents involved firearms, and three involved explosives. One incident, against an oil pipeline in 2008 in Refahiye, Turkey, involved remote electronic interference that caused an explosion. No casualties were reported.

cause harm. Secondly, ‘minimal equipment’ is not defined. Thirdly, ‘a lot of damage’ is not clarified. From McKenzie’s assertion, we can infer that cyberterrorists exist, a cyberterrorist attack is possible, and that the scale of potential damage could be high. When the 2015 version of the *National Security Strategy* warned of ‘significant and varied’ cyber threats to the UK, including ‘terrorists’ who could “use easily available cyber tools and technology for destructive purposes” (2015a:19,85), these tools are not detailed.

In a similar fashion, when David Cameron, the Prime Minister, warned that “we cannot leave cyberspace wide open to the criminals and terrorists that threaten our security and prosperity” (2011), this articulated point of vulnerability – the openness and interoperability of internet communications – is not substantiated. The assumed inference might be that British cyberspace is an ‘open door’ that can be exploited. Likewise, when Francis Maude stated: “return to a paper world? Of course not. We’re not trying to protect ourselves from the internet … we need to protect the internet from hostile actors – the criminals, the hackers, the terrorists – who want to exploit it for less positive ends” (2012a), the scale, nature and potential of these ‘less positive’ ends were not elaborated. Maude’s statement shares a similarity with Ian McKenzie’s (2014; see also Blunkett, 2011,2015; Jopling, 2010; Jolly, 2015), detailed above, with ‘terrorists’ ‘packaged’ with criminals and other nefarious cyberspace-based actors. This is an important point, which indicates that the cyberterrorism-as-threat discourse is not standalone, but instead exists as part of a broader discourse of threatening actors in cyberspace. Packaging the identity of threatening cyberterrorists with rogue states, criminals and unspecified hackers highlights the potential pervasiveness of illegitimate violent cyber actors and bolsters the case for the British state to act as the guarantor of the UK’s cyber security (Mott, 2016).

The ambiguous discourse of a category of terrorist threat that has not occurred and may not occur perhaps indicates that it was important for both the securitising actor and the audience to advocate the *possibility* of cyberterrorism taking place, without entering into in-depth narratives of the means by which a cyberterrorist incident could be accomplished. This is ‘ambiguous chanting’ in action. Without having access to any classified materials on the likelihood of contemporary terrorist organisations conduct major cyber attacks against UK infrastructure, one would suggest that the securitisation of cyberterrorism operated on a speculative rather than definitive basis. To return to the *Cyber Security Strategy* of 2011, this document warned that terrorists “*might* also use cyberspace to facilitate or to mount attacks against the UK … especially if terrorists *believe* that our national infrastructure may be vulnerable” (2011:15, emphasis added).

The inference from this excerpt is that because cyberterrorism is a genuine possibility, one of the means to pre-empt the threat is to ensure that the UK's national infrastructure cannot be perceived as being vulnerable to cyber attack.

It is argued here that the emergence of cyberterrorism as a Tier One threat broadly befits the Copenhagen School's securitisation theory. Cyberterrorism shifted from a largely non-articulated national security threat to a securitised threat with immediate effect with the publication of the UK 2010 *National Security Strategy* (Cabinet Office, 2010a:11). Here, the collective Government was the securitising actor, which had proclaimed cyberterrorism to be a Tier One threat to British national security. Whilst few members of the public at large may feel motivated to pro-actively read the *National Security Strategy*, or access Government press releases surrounding the publication of such documents, 'cyberterrorism as Tier One threat' was established as a theme that could be re-articulated by members of the first and second audience 'tiers'. With the securitising act accomplished, credibility and legitimacy was ascribed to the perception that cyberterrorism was possible and warranted serious concern. Members of the audience could speak of this fixed nodal point, with the credible backing of the Cabinet Office, and feel less at risk of being accused of conspiracy or hyperbole. Ministers, MPs and Lords who vocalised their agreement with the securitisation of cyberterrorism – expressed by using the term 'cyberterrorism' and uncritically highlighting its threatening nature – were active rather than passive actors. Repeated 'chanting' of a threatening cyberterrorist threat without articulating its definition, parameters or the means by which it could occur, does little to develop the discourse. However, there is a core utility to ambiguously chanting about the threat of cyberterrorism. 'Terrorism', when used as a label, is an ill-defined yet powerful discursive delineation between legitimate and illegitimate violent actors (Stampnitzky, 2013). The mere existence and reaffirming of the term cyber*terrorism*, therefore, serves to construct a discursive delineation between legitimate and illegitimate violent actors in cyberspace.

Creating and maintaining this delineation – irrespective of whether cyberterrorism occurs – has a cogent policy significance. The development, possession and application of cyber weapons at the state level is not regulated. A policy vacuum exists, and the norms governing signalling and deterrence in cyberspace have yet to be developed (Dipert, 2010). If the experience of state-level adaptation in the years following the emergence of the atomic weapon in the 1940s is informative, standards and norms of cyber weaponry may

yet take decades to develop (Liff, 2012; Manson, 2011). The 2007 cyber attack against Estonia, the 2008 attack against Georgia and the 2009-2010 attack against nuclear centrifuges in Iran all indicate that states are willing to cause disruption or damage against other state targets (Deibert, 2011). The articulation of cyberterrorism as a Tier One threat *performs* a tacit legitimisation of an unregulated and unspecified British cyber weapon arsenal. If the development of *illegitimate* cyber weapons operates in the domain of terrorists, criminals and rogue states, *legitimate* cyber weapons, or at least the concept of legitimate cyber weapons, must exist. The UK, which was an early state to publicly recognise its own cyber weapon program (Harvey, 2011) has not had any substantive public-facing debates on the necessity for, or nature of, its cyber arsenal. Creating and maintaining the distinction between legitimate and illegitimate forms of violence in cyberspace is a powerful element of the narrative that justifies the acquisition – and potentially use – of a novel weapon platform by a contemporary liberal democratic society.

The securitising acts entailed in the national security documents (Cabinet Office, 2010a,2011,2015a) did not implicate cyber weapons as de facto threatening tools by their own right. Instead, the threatening identities who may be interested in using these novel weapons systems were implicated. This corpus-wide focus on identities – as opposed to technologies – is analysed in greater detail in the sixth chapter. Had the discourse focused more heavily on the threatening properties of the cyber weapons themselves rather than the malicious intentions of groups or individuals who may wish to use them, this could have been said to have a potentially deteriorating effect on the tacit endorsement of the British state's cyber weapon program. According to the mapped discourse, cyber weapons were not inherently problematic; the nefarious actors who might use such weapons were. The discourse therefore does not by default exclude the possibility of positive applications for cyber weapons. Indeed, Lord Touhig (2016) and George Osborne (2015) – the then-Chancellor, whose GCHQ speech is mapped in the next chapter – expressly linked the existence of cyberterrorists to the need for a British cyber offensive program. Osborne warned his audience that "we need not just to defend ourselves against attacks, but rather to dissuade people and states from targeting us in the first place … we reserve the right to respond to a cyber attack in any way that we choose" (2015). This linkage is an overt manifestation of this tacit delineation between violent identities in cyberspace. Illegitimate actors wish to use cyberspace against Britain's national security; therefore it is not only reasonable but also necessary for the UK to develop and maintain an adequate cyber offensive strategy.

The distinction between legitimate and illegitimate forms of cyber violence would have been less cogent had the securitising act and associated discourse not been so categorical in classifying cyberterrorism as a Tier One threat. If the discourse had been reassuring – for instance, stating that whilst terrorists may wish to conduct significant cyber attacks, it is unlikely that they would be able to do so – the implied threat perception would have been less alarming. Whilst much of the discourse that has been mapped in this chapter, and indeed subsequent chapters, appears to exhibit ambiguity, the core notion that cyberterrorism is a 'Tier One' threat is a categorical speech act and a fixed discursive nodal point. According to this securitisation, cyberterrorists *do* possibly exist and they *are* trying to develop advanced cyber weapons. Whilst an array of policies are potentially legitimised as a result of this threat construction, such as surveillance of online communications, forcible seizure of encryption keys, state-to-individual hacking, and forced cooperation between large technology firms and the Government; the core function of creating a common knowledge that cyberterrorists exist is the tacit legitimisation of the British state's own interests in offensive cyber technologies.

Having mapped and analysed the British discourse that formed the 'cyberterrorism as a Tier One threat' theme, this chapter finishes with a concluding section that summarises its key content.

Conclusion

This chapter sought to map the 'official' discourse in the UK that could be regarded as having established cyberterrorism as a threat to British critical national infrastructure warranting extraordinary responses. This chapter articulated this discourse broadly within the framework of the 'traditional' approach to securitisation theory (Buzan, Waever and Wilde, 1998). It was found that the securitisation of cyberterrorism was a case of 'anticipatory security'. However, this chapter has also emphasised that the utility of the securitisation framework is bolstered if the 'audience' is framed as having agency.

Given that cyberterrorism was regarded as a 'Tier One' threat in the 2010 *National Security Strategy* (Cabinet Office, 2010a), the 2011 *Cyber Security Strategy* (Cabinet Office, 2011) and the 2015 version of the *National Security Strategy* (Cabinet Office, 2015a), the threat of 'cyberterrorism' could, reasonably, be considered 'securitised', even if the matter had not been discussed in either Chamber, nor at any external

events. However, from the mapped corpus of official discourse outlined above, it is apparent that this securitisation was entrenched by Ministers, MPs and Lords who chose, by their own volition, to repeat the 'Tier One' and 'severe threat' (or similar) themes. Throughout May 2010 to June 2016, there were no debates held in either Chamber specifically regarding the threat posed by cyberterrorism, nor did Ministers attend events expressly concerning cyberterrorism. Each instance in which the threat of cyberterrorism was raised was an instance where a member of the either the first or second audience-tier implicated in this securitisation had elected to voice their views on the issue. Throughout the mapped discourse, there were no cases in which a member of either tier of the audience expressly sought to indicate their dissent against the core drive of this securitisation; that cyberterrorism represents a 'Tier One' threat to the critical national infrastructure of the UK.

The mapped references to cyberterrorism in the national security documents and from Ministers, MPs and Lords did not include specific technical details. In the analysis, this was deemed to be notable, given that the perceived existence cyberterrorism – and indeed any cyber threat – relies entirely upon a relatively recent man-made technology. The core theme in the mapped discourse included in this chapter was that the existence of a cyberterrorist identity was deemed to be credible and that this threatening identity represented a high-level risk to British national security. By ambiguously-chanting their tacit agreement with this theme, the audience members gave further credence to this partially-fixed discursive node. The existence of this partially-fixed node is evidence of a socially-constructed illegitimate form of violence in cyberspace. One consequence of the existence of this node is that by default, there must be a concept of legitimate violence in cyberspace. The securitising act exhibited in the national security documents had not sought to securitise *all* cyber weapons; instead, the securitisation was targeted against the identities of hypothesised actors potentially interested in using such weapons.

The next chapter will outline further aspects of the official securitisation of cyberterrorism beyond this core 'Tier One' theme. Specifically, this fifth chapter will detail how this particular securitisation is *unique* vis-a-vis other securitisations, such as that implicated by 'traditional' or 'analogue' terrorism. Outlining this uniqueness in spatial and temporal terms, with reference to further mapped discourse, this chapter draws on Post-Structural interpretations of securitisation theory to argue that cyberterrorism presents a novel case study. Whilst the fourth chapter of this thesis regarded the 'Tier One' strand as a relatively

singular and distinct thread, the ‘spatial’ and ‘temporal’ strands which form the basis of the next chapter are divided into sub-strands to account for the greater diversity of description about the nature of the threat of cyberterrorism that had been articulated by members of the first and second audience-tiers.

Chapter Five: Cyberterrorism as Temporally Unique

The previous chapter mapped and analysed the official discourse surrounding the threat of cyberterrorism between 12th May 2010 and 24th June 2016 and established that this was a discourse exhibiting concerted and consistent characteristics of securitisation. However, whilst the securitisation framework exists precisely because there are some broad generalisations that can be gleaned from any given 'securitised' phenomenon, not all securitised threats are the same. This fifth chapter seeks to further the mapping and analysis of the securitisation of the threat of cyberterrorism in the UK, to highlight how this threat is discursively constructed as unique. The mapped discursive content that is considered in this chapter is material from the corpus that has not yet been raised in the thesis. The distinctiveness of the threat of cyberterrorism is articulated in two key strands: 'Cyberterrorism as a temporally unique threat', and 'Cyberterrorism as a spatially unique threat'. These strands are further divided into distinct sub-strands. There are two sub-strands for the 'temporal' element, which are 'New Terrorism' and 'Escalation of Threat'. Similarly, there are two sub-strands for the 'spatial' element. These are 'Physical versus Cyber', and 'Safe Havens'.

I could have identified more strands from the corpus, such as 'cyberterrorism as a hitherto ignored threat', or 'cyberterrorism as a financially costly threat'. However, due to the space constraints of the thesis, I have selected the most prevalent strands and sub-strands to articulate the unique nature of the threat of cyberterrorism, versus other threats to British security. The four strands and four sub-strands that I have used to structure the mapping and analysis of the corpus are comprised, in sum, of *all* of the corpus. Widening the strands further would have risked thinning the scope of the analysis and could have rendered the thesis susceptible to 'straw man' strands. Some of the mapped content included in this chapter will not rigidly adhere to a single strand or sub-strand, but will instead crossover to two or more. Where this clash has occurred, I have placed the discursive item in the 'best fit' strand and sub-strand, and must stress that this is an exercise in coherence of structure, rather than an intention to rigidly compartmentalise the discourse. This chapter maps and analyses the aspects of the discourse relating to the 'temporal' strand, beginning with the sub-strand of 'New Terrorism'. The sixth chapter of this thesis details and analyses the 'Spatial' sub-strands and introduces the final strand, 'From Fiction to Reality'.

Cyberterrorism as a Temporally Unique Threat: 'New Terrorism' - Mapping

In the previous chapter, the key themes underpinning the strand were 'Tier One' and 'severe/extreme threat'. The 'New Terrorism' sub-strand possesses key themes of its own. I have identified these themes because they are broadly in alignment with the characteristics of 'New Terrorism' that are advocated by academics endorsing the dichotomy between old and new forms of terror (Laqueur, 2000). Accordingly, these themes are: 'evil', 'unknown/uncertain/complex' and 'WMDs/unconventional weapons'. This section maps the elements of the corpus which adhere to these themes. The 'New Terrorism' narrative and field is examined more closely in the subsequent section, which offers an analysis of this mapped discourse.

The demonisation of proscribed groups through language such as 'evil', or 'barbaric' is a component of the language surrounding contemporary counter-terror efforts. There was some evidence of the use of this language in the corpus. For instance, Dan Jarvis, the Labour MP for Barnsley Central and the shadow Justice Minister, discussed the 'new threats' that the UK faced, during a debate on *Britain and International Security* in July 2015. Jarvis, heralded by colleagues for his career in the Parachute Regiment of the British army, reported to the Chamber that the UK suffered more cyber attacks than any other European state, and that "terror and extremism are as formidable an enemy as any that our country has ever faced … it is every bit as *fierce* as the *evil* this country waged war on more than 70 years ago" (2015; emphasis added). Suggesting that there are similarities between today's threat from terrorism and the devastation caused by the Wehrmacht, Luftwaffe, Kriegsmarine and Waffen-SS during the Second World War is perhaps an over-statement; an estimated 27-28 million Soviet citizens lost their lives during the conflict, as did 350,000 British citizens, representing 0.75% of the pre-war British population (Reynolds, 2002:223-224).

In 2015, leading a Commons debate on *National Security and Defence*, David Cameron informed the Chamber that "of course, the threats we face today go beyond that evil death cult [ISIL]. From the crisis in Ukraine to the risk of cyber attacks and pandemics, the world is more dangerous and uncertain today than even five years ago" (2015a). In a February 2016 speech, John Hayes, who was then serving as Minister for Security at the Home Office, expressed concern that "the essential change in terrorism is the increasing adaptability of terrorists, and of Daesh in particular. It uses new technology, new methods. It is adaptable. And it *revels* in its *own depravity*" (2016; emphasis added). This use of language suggests that terrorism,

particularly that epitomised by international Islamic extremism, terrorises not simply on the basis of a rational cost-benefit analysis of projected material gains from conducting political violence, but kills for the exercising of an ideology that is considered depraved by the British securitising agents and audiences. Similar sentiment to Hayes was expressed by George Osborne during a November 2015 speech delivered to GCHQ, in which he warned that "ISIL's murderous brutality has a strong digital element … they are using [the internet] for evil … they have not been able to use it to kill people yet by attacking our infrastructure through cyber attack. They do not yet have that capability. But we know they want it, and are doing their best to build it" (2015).

For Sir Nicholas Soames, Conservative MP for Mid Sussex, contemporary terrorists were a 'menace'. Accordingly, during a *NATO* debate in the Chamber, Soames expressed concern that:

> "the emerging challenges of the 21st century that threaten us, our way of life and our prosperity are not so much Médecins sans Frontiéres, but Menace sans Frontiéres … the operating environment has shifted from one of near certainty, in the Cold War, to a period of uncertainty, in the war on terror, and it will move further left towards the unknown" (2015).

It is apparent from these excerpts that both Osborne and Soames highlighted that the terrorist threat environment was not static, but instead in flux, with both figures warning that the threat was likely to become increasingly intractable. Furthermore, it is of note that Soames elected to use the term 'unknown', and indeed, he was not the only figure in the corpus to have chosen this particular term. During a speech on CONTEST to the Cityforum in February 2011, at which Pauline Neville-Jones, at the time a Minister of State for the Home Office and Security, implored that the UK must "address any technical shortfalls in our ability to tackle cyberterrorism", she also explained to her audience:

> "that the threat we face is changing. Al-Qaida is under pressure from the international community. But let us not be in any doubt that this group still aspires to launch attacks against the West. We now see new alliances between previously unconnected and indeed, *unknown* terrorist groups. We face an inherently unpredictable threat from self-starting individuals motivated by Al Qaida's rhetoric of global jihad (2011a; emphasis added).

The notion that cyberterrorism – and the actors behind this threat – represented a distinctly 'complex' phenomenon was also apparent from the corpus. 'Complexity' shares similarities with 'unknowability', but these terms are not directly interchangeable. The Oxford English Dictionary defines 'unknown' as "not known or familiar" (2017a), and defines 'complex' as "consisting of many different and connected parts", or

"not easy to analyse or understand" (2017b). To describe something as 'complex' would infer a greater extent of knowledge of it vis-a-vis describing it as 'unknown'.

In a September 2011 speech to the *Council on Foreign Relations*, Theresa May appeared to draw inspiration from the 'New Terrorism' thesis. May informed her audience that "the new terrorist threats are no less complex and difficult than the old. In some ways they are harder to deal with. They challenge our systems and structures. Terrorism now is more diverse, decentralised and perhaps also more agile than the landscape of 9/11" (2011a). May continued that: "we continue to see little evidence of systematic cyberterrorism. But this is now part of the language of Al-Qaida. As a tactic, and as a weapon, cyberterrorism is perfectly suited to the world of the lone terrorist, operating outside a hierarchy and without traditional command and control" (2011a).

Theresa May was not alone in espousing this concern. For instance, in October 2015, Lord Ahmad – then a Parliamentary under-Secretary for Countering Extremism under the Home Office whilst concurrently serving as under-Secretary for the Department of Transport, gave a speech on *Aviation Security in an Increasingly Complex Environment*. In this speech, Ahmad told the audience that whilst the three-day conference was debating many of the issues facing the aviation industry, none were more important than security "in an increasingly complex environment" and in particular, the need to protect "air passengers from the ever-evolving threat of terrorism" (2015). To Ahmad, it was clear "that as terrorists continue to innovate, our protective measures have to stay on their coat tails, and where possible get ahead" (2015).

An issue characterisable as being 'complex' is not, by necessity, intractable. To some figures in the corpus, the complexity of the threat of cyberterrorism – along with other cyber threats – represented an opportunity for the UK and British industry. For instance, Pauline Neville Jones spoke in October 2010 to inform the Lords Chamber that:

> "we will not succeed in defeating a cyber enabled terrorist enemy if our own communications are vulnerable. We need to be able to disrupt them, not them to disrupt us. This is the new national frontier. It offers very exciting, interesting and intellectually challenging opportunities for younger people and it is of great import to the nation" (2010).

In a similar vein, raising a question the following month, Julian Brazier, the Conservative MP for Canterbury and at the time a member of the Defence Committee, asked the Prime Minister whether he agreed that the UK was "very well placed to lead the transition in Europe towards the era of the information-

age terrorism, especially as we have GCHQ, and as his new National Security Council has made such a strong commitment to more spending against cyber warfare?" (2010). The Prime Minister responded that his honourable Friend made "a very good point", and that there was an "opportunity to combat this new threat of cyberterror and cyber attacks" (2010).

As noted in the opening section of this chapter, part of the 'New Terrorism' thesis argues that the means of attack of 'newer' terrorism are more diverse than that of the 'old'. For instance, whereas 'old' means of terror may have included the placement of a bomb in a public space, or the taking of hostages, 'newer' terrorists were more interested in acquiring the means to kill greater numbers of people with techniques or devices one would normally associate with state-based entities. There was some evidence in the corpus that members of the second tier of the audience engaged with this notion on public record. For instance, Lord Alderdice, the Liberal Democrat Peer noted that there was now a "need to move beyond the conventional in terms of the issues we have to address – notably cyber and terrorism" (2015).

Wendy Morton, the Conservative MP for Aldridge-Brownhills, juxtaposed cyberterrorism with 'bullets and bombs' when she raised a question with David Cameron, when he reported to the Chamber in November 2015 on the matter of the G20 and the then-recent attacks in Paris. Accordingly, she asked the Prime Minister whether he agreed "that the threat we face from terrorists today is not just about bullets and bombs, but about cyber attacks?" (2015). David Cameron responded that she was "absolutely right", emphasising that "we face cyber attacks not just from states, but from radical groups and individuals" (2015b).

Lord Patten, a Conservative Peer, who lamented that "when in opposition, Members of this side of the House again and again pressed noble Lords … to tackle issues such as … the threat of cyberterrorism … to scant avail" (2010), warned his colleagues in a debate on the *Terrorist Asset-Freezing Bill* that "fast coming down the track … are various forms of cyberterrorism … cyber weapons are so much easier to procure – they are more like chemical weapons by comparison to other more general military hardware, let alone nuclear materials" (2010). Lord Hannay, the crossbench Peer, used his time in a debate on *Cyberattacks* in October 2010 to draw a conceptual linkage between nuclear weapons and cyber weapons. Accordingly, Hannay stated that "the target against which that threat is directed – our society's increasing dependence on sophisticated forms of electronic communications – is continuing to grow at a frantic pace

which shows no sign of slacking … the target, as it grows, is likely to become softer unless effective countermeasures and increased resilience can be devised" (2010). Whilst he recognised that the analogy was not exact, if the cyber threat resembled any other threat, it was "perhaps closer to the one that we faced from nuclear weapons in the early years after their discovery, when we did not have a clear idea of what responses would work best and whether deterrence would be effective (2010). Hannay continued that, "the asymmetry of threats from nuclear weapons in the hands of terrorists, which makes nonsense of earlier deterrence doctrines, is matched in some ways by the inherent asymmetry of threats from cyberattacks (2010). Not only is Hannay directly engaging with the notion that terrorists are seeking to diversify their means of attack, but his comments are an apt example of how speakers engaging with a securitisation are able to draw upon pre-existing analogies and case studies to elucidate a point regarding a threat that is complex; or indeed, in the case of cyberterrorism, has not occurred. Furthermore, the securitisation of nuclear armaments is a largely fixed, entrenched securitisation in British discourse; by likening this securitisation to that of cyberterrorism, Hannay is expressly emphasising the significant scale of threat posed by terrorist use of cyberspace for the purpose of conducting attacks.

Another Lord, the crossbench Peer Viscount Waverley, also used analogy when speaking on the matter of cyberterrorism, suggesting that terrorists may elect to transition from suicide bombing to cyber enabled attacks, given the disruption that could be wrecked from the failure of a bank. Accordingly, in an *EU Report* debate in October 2010, he stated that:

> "a simple analogy to reinforce the case for global endeavours is to compare the threat of cyberterrorism to the threat of the banking sector. We know that one bank failing can have a catastrophic global impact. The same can apply to the world of cyberterrorism. I do not wish to appear alarmist, but I fear that, whereas suicide bombings have been the weapon of choice in certain quarters, carefully targeted cyberattacks will be the weapon in tomorrow's world" (Andersen, 2010).

Responding to a question during a *Strategic Defence and Security Review* debate that same month, Lord Strathclyde, the Conservative Peer who at the time was the Leader of the House of Lords, said that he was "delighted that the noble Lord [Lord Reid of Cardowan] welcomes the announcement on dealing with cyberterrorism. It is an important new threat that we take seriously" (Galbraith, 2010).

Lastly, whilst he did not explicitly discuss cyberterrorism, Kevan Jones, the Labour MP for North Durham, speaking in January 2013 as the shadow Minister for Defence, stated that "the security landscape

today is both uncertain and unpredictable. New threats such as cyber warfare and biological terrorism exist alongside conventional threats" (2013).

The next section draws on the academic 'New Terrorism' literature to critically analyse this aspect of the temporal distinctiveness of the securitised threat of cyberterrorism. It is argued that the linguistics of the 'New Terrorism' thesis had been inserted into the securitisation of cyberterrorism. This served two functions. Firstly, 'cyberterrorism' was contextualised within a framework of new and novel forms of terrorist threat. Secondly, this aligning of the 'cyberterrorism' discourse with pre-existing narratives of terrorist threats served to entrench the securitisation.

Cyberterrorism as a Temporally Unique Threat: 'New Terrorism' - Analysis

The phrase 'New Terrorism' is reflected in an approach to the study of terrorism and political violence that articulates a dichotomy between 'old' and 'new' forms of terror. The 'New Terrorism' lens is generally regarded as having originated from the writings of Laqueur (for instance, see Laqueur, 2000). Academics and policymakers who advocated the viability of this dichotomy argued that the terrorist threat espoused by Al-Qaida and its affiliates was extraordinary and without precedent. The distinctive characteristics of 'New Terrorism' have been described as "increasingly networked, more diverse in terms of motivations, sponsorship and security consequences; more global in reach; and more lethal" (Lesser, 1999:87). Unlike 'old terrorism', which might, for instance, have involved the taking of hostages or a telephone call that warns of a bomb placement before it detonates, 'New Terrorism' was deemed to represent "a very different and potentially far more lethal threat than the more familiar 'traditional' terrorist groups" (Hoffman, 1998:2000; see also Laqueur, 2000 and Neumann, 2009). 'New Terrorism', was typically associated with 'Radical Islamism' and deemed to be driven by religious conviction or ethnic identification, as opposed to the 'political' interests exhibited by 'old' terror entities such as the ETA or IRA (Howard and Sawyer, 2004). 'New Terrorists' were regarded as seeking to solicit extensive civilian casualties (Lesser et al, 2002). Of particular interest in relation to this thesis, fears were articulated regarding the new terrorists' willingness to acquire weapons of mass destruction (Gurr and Cole, 2000). In an interview with the *Time* magazine in 1998, Osama bin Laden had stated that acquiring chemical and nuclear weapons was "a

religious duty", and that it "would be a sin for Muslims not to try to possess the weapons that would prevent the infidels from inflicting harm on Muslims" (see PBS, 2014); however, there is scant evidence to suggest that any non-state terrorist entity has acquired weapons of mass destruction. Opportunities for a well-prepared non-state actor to surreptitiously acquire nuclear materials have existed, and, given the absence of publicly-available data on attempted dirty-bombing by terrorist organisations, not been taken advantage of. For instance, for a period of several weeks during 2011, at least 10,000 barrels of yellowcake uranium were left unsecured in warehouses in Libya (Spencer, 2011). A terrorist organisation with the wherewithal to safely remove and relocate the barrels – or organised criminals who could have sold them on the black market – could have taken advantage of this security lapse.

It is not the place of this thesis to directly engage with and critique the misplaced nature of the 'New Terrorism' hypothesis – indeed, other academics have produced excellent work demonstrating this already (for instance, see Croft, 2012; Duyvesteyn, 2004; Crenshaw, 2011). Christina Pantazis and Simon Pemberton have linked the pushing of what they term the 'ideology' of 'New Terrorism' on policymakers to the positioning of think tanks such as the RAND Corporation within the American 'military-industrial complex' (2009:376-380; see also Burnett and Whyte, 2005). Other notable literature has ascribed the 'New Terrorism' thesis as a form of 'neo-Orientalism', in which a 'radical Muslim' Other was positioned in the War on Terrorism in a binary opposition to the liberal United States and its allies (for instance, see Gentry, 2015; Tuastad, 2003:592; Nayak, 2006:44; Nayak and Malone, 2009:257; Puar and Rai, 2002; Hellmich, 2008; Solomon, 2012:910). 'Islamic' terrorists, through this Orientalist lens, were said to have been articulated as 'shadowy figures', and, amidst a preventative rather than reactive security culture, their – potentially – threatening behaviour was anticipated as an 'unspecifiable may-come-to-pass' (Ahmed, 2004:79; see also Gentry, 2015:139). This befits the notion of 'anticipatory' security, which was explored in the preceding chapter.

However, even if the 'New Terrorism' lens could be said to inherit misguided premises, this does not negate its potential impact on official discourse and policy-making. Indeed, the 'New Terrorism' concept was assimilated by the American government in its review of the 11th September 2001 attack against the World Trade Centre and the Pentagon – notably, the second chapter of the 9/11 Report was entitled *The Foundations of New Terrorism* (National Commission on Terrorist Attacks on the United States, 2004:47) –

and, inevitably, the ‘New Terrorism’ discursive construct also shaped the official counter-terrorism discourse in the UK. That ‘New Terrorism’ is an objectively dubious premise does not negate its powerful stature in popular and official discourse and its continued legacy in British security practices (Mythen, Walklate and Khan, 2012; Jackson, 2005; Spencer, 2010). Furthermore, as Weimann (2005) recognised, ‘cyberterrorism’ could be linked with the ‘New Terrorism’ lens (see also, Ronfeldt and Arquilla; 2001; Arquilla and Ronfeldt, 2001). Whilst a cyberterrorist incident has not occurred at the time of writing, the notion that terrorists may wish to use the internet as a means of wrecking death and destruction meshes with the anticipatory and anxiety-driven ‘what if?’ theme of the ‘New Terrorism’ field.

As discussed earlier in this section, the ‘New Terrorism’ thesis should be regarded as problematic. However, from my mapping of the discourse surrounding cyberterrorism, it is apparent that some members of the first and second tiers of the audience described the threat posed by cyberterrorists through means that befitted characteristics of ‘New Terrorism’. Excerpts from the corpus made judgements about the motivations and logic of cyberterrorism; cyberterrorists were deemed to be evil (Jarvis, 2015; Osborne, 2015), depraved (Hayes, 2016), unknown (Neville-Jones, 2011a; Soames, 2015), and radical (Cameron, 2015b). According to Theresa May (2011a), cyberterrorism was “perfectly suited” to a new era of terrorism in which terrorist behaviour had become “more diverse, decentralised … and agile”, in a shift towards non-hierarchical lone-terrorism. In a rare case in the corpus, Lord Patten focused on the nature of cyber weapons – as opposed to the identities of those who may wish to use them – warning that cyber weapons were easily procured unconventional weapons sharing characteristics with chemical weapons (2010). For Lord Hannay (2010; see also Jones, 2013), however, the issue of a distinctively threatening cyber identity and weapons-system were twinned; terrorists in possession of cyber weapons presented an asymmetrical threat not unlike that of terrorists armed with nuclear weapons.

That there was some evidence of usage of the linguistics of ‘New Terrorism’ in the corpus is perhaps not surprising. The capacity to use computer technology to directly cause damage or disruption only emerged in seminal form in the 1980s, making cyberterrorism a contemporary means of causing harm when compared to, say, the use of arms or bombs relying on incendiary technology originating from Ancient China (Lin, 2010:316). Furthermore, a terrorist with the capability and the willingness to use computers and internet-enabled means of delivery to cause harm will, by default, have access to the means of communication and

administration that facilitate the non-hierarchical, or 'lone wolf' forms of terror which could befit the 'New Terrorism' thesis. Consequently, there are grounds on which – as the corpus would suggest – *cyberterrorists* as agents, and *cyberterrorism*, as a means of attack, could both be considered 'new'. It is revealing that, when pressed for analogies, Lord Patten (2010) and Lord Hannay (2010) chose to draw on chemical weapons and nuclear weapons. That they chose these analogies is indicative of a) cyber weaponry's status as an unconventional weapon and b) the lack of a historical precedent for a significant and recorded attack involving terrorist application of a cyber arsenal.

The prominence of the 'New Terrorism' linguistics in the corpus is indicative of an entrenchment of the discursive social-construction of an illegitimate violent identity in cyberspace. By highlighting the 'evil', 'depraved', and 'menacing' nature of this identity, the members of the first and second tiers of the audience were using their 'ritualistic chants' to add nuance to the securitisation. The securitisation could therefore be said to have *evolved*, as a result of this mediation through ritualistic chanting. By emphasising the evil and depraved identity of cyberterrorists – in alignment with a broad 'New Terrorism' thesis – the narratives of cyberterrorists, whether they exist or not, are silenced. This would suggest that the discursive treatment of hypothetical, spoken-into-existence cyberterrorists by MPs, Ministers and Lords befits the historical precedent in which existing, non-cyber, terrorist groups have had their narratives of retaliation against perceived injustice silenced through the use of 'New Terrorist' linguistics by British policymakers. For example, Tony Blair, responding to the bombing of the transport system in London in July 2005, sought to pacify the narrative of the perpetrators by describing both the actions and the identities as evil. In a speech delivered to the Labour Party conference, Blair stated, "senseless though any such horrible murder is, it was not without sense for its organisers. It had a purpose. It was done according to a plan. It was meant. What we are confronting here is an evil ideology" (2005). Silencing the narratives of the terrorists, whether cyber or conventional, real or hypothetical, serves to mitigate the window in which empathy towards the terrorist entity could form. According to the 'New Terrorist' element of the socially-constructed threat of cyberterrorism, understanding the narrative of the cyberterrorist is not necessary nor useful; it is sufficient to regard them as evil. Whilst this may not make the 'illegitimate' violence of cyberterrorism intractable, it serves to make the division between legitimate and illegitimate forms of cyber violence harder to critique. The 'New Terrorism' theme has made counter-terrorism policies and narratives less amenable to meaningful

debate. Those who have campaigned for the rights of suspected terrorists, critiqued counter-terrorism policy, or sympathised with some elements of the narratives of terrorists, have been labelled 'terrorist sympathisers' by British policymakers (Watt, 2015), and, in some cases, have been charged with terrorism offenses (MacAskill, 2017). The appearance of the 'New Terrorism' linguistics in the securitisation of cyberterrorism was not necessary to the survival of this discursive construct, but it may have served to extend its longevity in the absence of a bona fide cyberterrorist attack.

'New Terrorism' was not the only aspect of the temporal uniqueness of the socially-constructed threat of cyberterrorism. My mapping of the corpus identified two distinct components of this temporal uniqueness. The next section of this chapter maps the discourse that relates to the second sub-strand of the 'temporal' uniqueness of cyberterrorism; the notion that cyberterrorism is a threat that increased between May 2010 and June 2016, and was set to further escalate for the foreseeable future.

Cyberterrorism as a Temporally Unique Threat: Escalation of Threat – Mapping

The key theme of this sub-strand that could be identified from the corpus was the notion that cyberterrorism was an accelerating threat over time. This acceleration was articulated in two forms; that the severity of a potential cyberterrorist attack was increasing, and that the windows of opportunity to conduct such attacks were also escalating. This was a common sub-strand in the discourse; securitising agents, as well as members of the first and second tiers of the audience engaged with this sub-strand both inside and outside of the Chamber. Excerpts from the corpus that relate to the notion of an escalating threat of cyberterrorism are mapped in this section.

David Cameron, speaking during a January 2015 press conference with US President Barack Obama at the White House, used the opportunity to emphasise that both states would have to:

> "keep pace with new threats, such as cyber attacks … if our forebears could join us here in the White House today, they might find the challenges that we're facing from ISIL to ebola, from cyberterrorism to banking crises, they might find those hard to comprehend, but they would surely recognise the ties that bind us across the Atlantic and the values that our peoples hold so dear" (2015c).

Here, Cameron was juxtaposing shared 'values' of the UK and USA – which are based on a rich historical context – with the 'new threats', including cyberterrorism, which lacked the historical context that would render them immediately comprehendible to former leaders of both states.

David Cameron was not the only leading Cabinet figure to discuss the urgency of the new threat of cyberterrorism outside of the Chamber. A speech that George Osborne, then the Chancellor of the Exchequer, delivered to GCHQ in November 2015 bears particular interest. Accordingly, Osborne told his assembled audience that:

> "earlier this year the Prime Minister asked me to chair the Government's committee on cyber, and through that I see the huge collective effort required to keep our country safe from cyber attack; the great range of threats we face; and how this will be one of the great challenges of our lifetimes … the stakes could hardly be higher – if our electricity supply, or our air traffic control, or our hospitals were successfully attacked online, the impact could be measured not just in terms of economic damage but of lives lost … so when we talk about tackling ISIL, that means tackling their cyber threat as well as the threat of their guns, bombs and knives. It is one of the many cyber threats we are working to defeat … the truth is that we have to run simply to stand still. The pace of innovation of cyber attack is breathtakingly fast" (2015).

This extract, delivered to a select and specialist audience, but disseminated publicly through the gov.uk website, is an example of a securitising actor (re)publicising a securitising call. The extract exhibits common and comprehendible language and phrasing, as opposed to the more specialist language that Osborne's immediate audience would have been accustomed to. Osborne used this speech to indicate spending priorities in the *Spending Review*, which was to be published the following week. In the above extract, Osborne is explicitly articulating a referent object, (British critical national infrastructure) and suggests that an attack against this object, which could be conducted by ISIL, could lead to the loss of life. Furthermore, this was not a static threat, but one that was escalating at a 'breathtakingly fast' pace (Osborne, 2015). This warranted a policy environment in which the British Government and the state authorities (for instance, GCHQ, MI5 and the NCA) would need to develop their knowledge of the threat and their capabilities to deal with it.

Osborne continued his speech by highlighting that the asymmetry of threat was escalating, because:

> "in the past few years, an online marketplace has developed, which means all the elements of an attack can now be bought and assembled from the computer of anyone with the money to pay for it. The barriers to entry are coming right down, and so the task of the defenders is becoming harder … imagine the cumulative impact of repeated catastrophic breaches, eroding that basic faith in the internet that we need for our online economy and social life to function … if the lights go out, the banks stop working, the hospitals stop functioning or Government itself can no longer operate, the impact on society could be catastrophic" (2015).

Here, Osborne was emphasising that the increasing ease of conducting cyber attacks was effectively making the role of GCHQ – and, presumably, IT security specialists more broadly – more difficult. Osborne asks his audience to *imagine* the impact of successive cyber breaches; activating the emotive responses required for a securitisation to function. Furthermore, Osborne uses the term 'catastrophic' twice. 'Catastrophic', a word denoting something that entails "sudden great damage or suffering" or "sudden and large-scale alteration in state" (OED, 2017c) is not a term that pulls punches when describing the nature of a threat. These extracts from Osborne's November 2015 GCHQ speech are perhaps, defensibly, the most emphatic securitising calls exhibited in the corpus. The term 'catastrophic' was used elsewhere in the corpus, for instance, by Viscount Waverley (Andersen, 2010) and by Lord Harris of Haringey, who noted that the UK was becoming more reliant on ICT systems, that "foreign states and others" had been identified as 'probing' British critical national infrastructure and that fellow Peers should "be quite clear that there would be catastrophic consequences in the event of something significant happening" (2015).

The 2010 *Strategic Defence and Security Review* – suitably entitled *Securing Britain in an Age of Uncertainty*, detailed that "over the last decade the threat to national security and prosperity from cyber attacks has increased exponentially. Over the decades ahead this trend is likely to continue to increase in scale and sophistication, with enormous implications for the nature of modern conflict" (Cabinet Office, 2010b:4). The escalating threat of cyberterrorism was also articulated elsewhere in official documentation. For instance, *Contest: The United Kingdom's Strategy for Countering Terrorism*, published in July 2011, noted that:

> "we continue to see no evidence of systematic cyberterrorism. But the first recorded incident of a terrorist 'cyber attack' on corporate computer systems took place in 2010. The so-called 'here you have virus' (the responsibility for which was claimed by the Tariq bin Ziyad Brigades for Electronic Jihad) was relatively unsophisticated but a likely indicator of a future trend. Since the death of Osama bin Laden, Al-Qaida has explicitly called not only for acts of lone or individual terrorism but also for 'cyber jihad' (Home Office, 2011:34).

Terrorist groups that rally behind an ideology inspired by the Islamic faith do not have a monopoly on political violence. However, it is of note that the authors of the CONTEST document believed 'cyber jihad' to be a credible future threat. This document presented a relatively dour outlook on the future threat landscape, warning that:

> "terrorist groups will use a range of attack techniques, both established and new. There will be more cyberterrorism … at present we believe the threat of a terrorist cyber attack is low but as the tools and technologies needed for cyber - attack become more widely available and the success of criminal cyber operations becomes more widely known" (Home Office, 2011:41,74).

From these excerpts, one can infer that the CONTEST document was unambiguous in its message on cyberterrorism; this was a threat that had not existed before, but would become an increasingly pressing reality. Terrorists were willing and eager to deploy cyber weapons against the British state as part of an electronic 'jihad', and when the barriers to entry to conduct cyber attack were sufficiently lowered, the UK would begin to experience these attacks.

An insightful report on *UK Cyber Security: the Role of Insurance in Managing and Mitigating the Risk*, co-published by the British Government and the insurance firm Marsh, listed terrorists in its taxonomy of malicious actors interested in damaging British firms, and warned that the threat picture "is likely to get starker as technology and internal processes get better at eliminating accidental failures, while malicious attacks grow in ambition and impact" (Cabinet Office and Marsh, 2015:8,9). The report made reference to the 2014 German steel mill failure that resulted from a malicious cyber attack, and informed its readers that:

> "physical losses are a growing concern – both in terms of severity and frequency – given the interconnectedness of cyberspace and the physical world. One example of this new category of risk can be seen in the way that industrial control systems operate in the energy sector. Today, these new generation control systems are built on the concept of openness and interoperability, and this has exposed the sector to a host of cyber security risks that are only just beginning to be understood (2015:13).

This document appeared to make a conscious effort to avoid hyperbole. Whilst recognising that it is feasible for a cyber attack to cause human mortality, it noted that "for the time being, the probability of death and bodily injury resulting from a cyber attack is considered to be negligible. We should note, however, that in future, as more devices go online, cyber hacks and system malfunctions could pose a more material threat to human life" (2015:13).

Theresa May, speaking as the Home Secretary in 2015, similarly eluded to a shifting and escalating threat. In an oral statement to Parliament, on the publication of the draft of the *Investigatory Powers Bill*, May stated that:

> "we live in a digital age. Technology is having a profound effect on society. Computers are central to our everyday lives … but a digital society also presents us with challenges. The same benefits enjoyed by us all are being exploited by … terrorists. The threat is clear. In the past twelve months alone six significant plots have been disrupted in the UK, as well as a number of further plots overseas. The frequency and cost of cyber attacks is increasing, with 90% of large organisations suffering an information security breach last year" (2015).

Here, May does not explicitly state whether the six significant thwarted plots in 2014-2015 concerned cyber attacks or involved analogue methods. In November 2015, David Cameron spoke at the G20 summit in Turkey and noted that "over the past year alone our outstanding police and security services have already foiled no fewer than seven terrorist plots right here in Britain" (2015d), so one would presume that the plots were 'analogue'. When Britain's security agencies, or leading political figures, choose to publicly disclose the number of recently foiled plots, details of the attacks are typically scant, given that the agencies do not wish to risk disclosing the means by which they acquired the information leading to the successful containment of the threat. However, given the novelty of a cyberterrorist plot, had one been thwarted, it is reasonable to suggest that the security agencies might disclose the fact that they had successfully prevented a new form of terror strategy. A publicly-cited example of a thwarted cyberterrorist plot could substantially bolster the raison d'etre of the securitisation of cyberterrorism. Notwithstanding this, it is of note that Theresa May linked these six thwarted plots with the expanding role of technology in British society and the escalating frequency and costs of cyber attacks.

May's Ministerial colleagues, when speaking on the subject, espoused similar sentiment; that the threat of cyberterrorism was likely to be an escalating one. James Brokenshire acknowledged that the British Government was "conscious of the changing nature of potential risk" (2012) when as Parliamentary under-Secretary for the Home Office he delivered his June 2012 speech at the *Securing Asia* conference. Brokenshire elaborated further on this in his *Cyber Crime* speech in March 2013, when he informed his audience that:

> "to date, terrorists have not seen cyber attack as an important means of conducting their actions, although of course they use the internet to radicalise, spread propaganda, disseminate violent extremist material and communicate with each other. But we and other governments must be very mindful of the fact that this could change" (Home Office and Brokenshire, 2013).

Baroness Neville-Jones, speaking during a *Tackling Online Jihad* conference in her capacity as the Security Minister, reportedly told her audience that the terrorist threat to the UK was a diverse one, and that

"as terrorists diversify their techniques and shift geographically, the range of tools available to them widens and opportunities for differing forms of terrorism, including cyber attack increase" (2011b). She substantiated this line of thought by noting that there was also a risk:

> "likely to grow over time and which we monitor closely, that terrorists will develop serious cyber attack capabilities: by this I mean the ability to commit acts of terror by hacking into critical infrastructure and online systems. In some form, a cyber attack attempted by terrorists, if not inevitable, is of so great a likelihood that we bear it in mind in developing operational capabilities" (2011b).

Brokenshire and Neville-Jones were not alone in their Ministerial re-chanting of the securitisation of cyberterrorism, underpinned by the notion that it was an escalating rather than receding or static threat. In his May 2012 speech delivered in Estonia, Francis Maude, speaking as the Paymaster General and Minister for the Cabinet Office, implored that:

> "we need to protect the internet from hostile actors … the terrorists who want to exploit it for less positive ends … and we know the threat is accelerating. High end cyber security solutions that were used 18 months ago by a limited number of organisations to protect their networks may already be out in the open marketplace" (2012a).

Maude had expressed similar sentiment in the previous year. In a written statement on the release day of the *Cyber Security Strategy* in November 2011, Maude stated that "the threat to our national security from cyber attacks is real and growing. Organised criminals, terrorists, hostile states, and 'hacktivists' are all seeking to exploit cyberspace to their own ends" (2011).

These were not the only instances of Francis Maude making this argument. In a written statement to Parliament in December that same year, Maude stated that "there exists a real and growing threat to our interests in cyberspace; these threats have increased concurrently with the growth of the 'internet economy'", but he sought to reassure his colleagues by adding that "the Security Service has developed and enhanced its cyber structures, focusing on investigating cyber threats from hostile foreign intelligence agencies and terrorists" (2012d). The next day, giving a speech at *IA12*, Maude told his audience that the internet had to be protected from terrorists, and that "the nature of the threat means we cannot afford to drop our focus *even for an instant* … the threats won't disappear and they are *ever-changing*" (2012b, emphasis added). In 2014, Maude still espoused that "because of the relentless and ever-changing nature of cyber threats, we also need to be on the front foot to develop new skills and capabilities in the future" (2014e).

In a speech in February 2016, then-serving in Maude's former role as the Paymaster General and Minister for the Cabinet Office, Matt Hancock informed his audience that "cybercrime, espionage, or attacks on critical infrastructure, from both state and non-state actors are increasing. The average cost of the most severe online security breaches now starts at almost £1.5 million. The number of significant attacks has doubled in the UK in the last year alone" (2016b). Hancock expressed a similar view in a press release the following month in which he wrote that "the UK faces a growing threat of cyber attacks from states, serious crime gangs, hacking groups as well as terrorists" (2016c).

John Hayes, at the time the Minister of State for Security at the Home Office, delivered a speech the following month entitled *What is Real is Reasonable*, in which he raised the issue of Islamic State's use of technology, articulating that:

> "it is all too tempting to view the threat we face as abstract, as theoretical. To believe that we have always faced threats. That the threats we face now are essentially the same as those in the past … the threat we face now is changing, ferocious and flexible. The threat is evolving rapidly. Responding to it is a testing challenge" (2016).

For Hayes, the threat level was "unprecedented and growing", and he quoted Andrew Parker, the Director General of MI5, who had claimed that "the threat we are facing today is on a scale and tempo that I have never seen before in my career" (2016).

Ed Vaizey, the then-Minister of State for Culture and the Digital Economy, wrote in the introduction to the *Cyber Governance Health Check 2015/16* that "the UK faces a growing threat of cyber attacks from states, serious crime gangs, hacking groups as well as terrorists" (2016:2).

Lastly – for Ministerial contributions to this sub-strand – William Hague, at the time the Foreign Secretary and First Secretary of State, stated that "we do all face sophisticated and persistent threats in cyberspace from terrorists or organised criminals" (2013b). Hague also warned during his visit to GCHQ in August 2013 that terrorists and other adversaries' approaches "and techniques are constantly changing and our intelligence agencies are faced with a tremendous challenge to keep pace" (2013c).

The contributions from Ministerial figures noted here do not constitute a majority of the Cabinet. However, the Prime Minister, the Chancellor, and the Home Secretary all advocated the notion that cyberterrorism was an escalating threat. With this notion endorsed by official Government publications (Cabinet Office, 2010b; Cabinet Office and Marsh, 2015), as well as Brokenshire (2013), Neville-Jones

(2011b), Maude (2011, 2012a), Hancock (2016b, 2016c), Hayes (2016), Vaizey (2016) and Hague (2013c), it is not unfair to state that this was, broadly, a cross-Cabinet sentiment. I would therefore suggest that the notion that cyberterrorism was an escalating threat was an entrenched sub-strand of the securitisation of cyberterrorism for the 12th May 2010 to 24th June 2016 period under scrutiny.

Similarly to the 'Cyberterrorism as a Tier One Threat' strand, there was no evidence from the corpus that this sub-strand was contested by the wider body of Parliamentarians and Peers. This section will now detail the wider official discourse endorsing the notion that cyberterrorism was an escalating threat to the UK.

The opposing front bench did not appear to dispute this sub-strand. Jim Murphy, the Labour MP for East Renfrewshire, speaking in November 2010 in his capacity as shadow Secretary of State for Defence, stated that "I sense that the unprecedented scale and pace of global change will, if anything, increase ever more sharply in the future", elaborating by adding that "today's threats are far more complex and difficult to map, and they are harder to repel. Terrorism, cyber attack, natural resource shortages, large-scale natural disaster or unconventional attacks from chemical or biological weapons all threaten our shores, our interests and our values" (2010). Kevan Jones, Labour MP for North Durham, speaking in January 2013 as a shadow Minister for Defence, stated that "the security landscape today is both uncertain and unpredictable. New threats such as cyber warfare and biological terrorism exist alongside conventional threats" (2013). Yvette Cooper, the Labour MP for Normanton, Pontefract and Castleford, and at the time the shadow Home Secretary, stated in an *Investigatory Powers* debate in June 2015 that she had observed "growing problems with organised cyber attacks for major companies, infrastructure and the Government" (2015). In a *Britain and International Security* debate, Vernon Coaker, Labour Member for Gedling and the then-shadow Secretary of State for Defence, noted that the security landscape was "far more uncertain" than had been envisaged in 2010, and he warned his colleagues that there were "new emerging threats such as those involving cyber", which appeared "to grow at an exponential pace" (2015).

As noted in the 'Tier One' strand analysis, some Members sought to co-opt the securitisation of cyberterrorism and wield it to legitimate their views on other political or security issues. There was one similar instance here. Russell Brown, who at the time was the Labour MP for Dumfries and Galloway, argued in November 2012 that:

> "there is a positive case for Scotland to remain part of the United Kingdom. No one doubts that our country is capable of being independent, but why should we want to lose all those advantages? At a time of immense and fast-evolving challenges throughout the world, with a plethora of security threats on the horizon, why on earth should we want to devote time and money to dividing our resources north and south of the border? We should be working together, throughout Britain, to remain vigilant against the constant threat of cyberterrorism" (2012).

Here, Brown is soliciting the evolving threat of cyberterrorism as a discursive tool to argue in favour of a constitutional status quo. In alignment with Lynton Crosby's 'project fear'-style of political campaigning (Coates, 2016), this perspective placed the requirement to address the securitised threat of cyberterrorism – along with other threats – as a priori with respect to the aspirations of Scottish nationalists. Such co-opting of a securitisation for political expedience serves to solidify the securitisation, because such a re-chanting of the securitised motion is voiced by the speaking actor as unproblematic or without contention around its central rationale.

As with the 'New Terrorism' sub-strand detailed earlier in this chapter, there was also mention of nuclear weapons in relation to cyber weapons within this sub-strand. Whereas in the previous sub-strand this engagement drew similarities between cyber and nuclear weapons – in that both are unconventional – this sub-strand noted the ineffectiveness of nuclear weapons as a deterrent against cyber weapons. Whilst he did not reference a specific actor, Lord Browne, a Labour Peer, noted that "cyber attacks are more commonplace today and they will grow both in number and intensity", adding that due to the potential diluting of the capacity to ascribe attribution to a cyber attack, nuclear weapons would provide "less of an insurance policy" against future challenges (2013).

Elsewhere in the corpus, Parliamentarians and Peers re-chanted similar calls made by the Ministerial figures cited above. For instance, Nigel Dodds, the Democratic Unionist MP for North Belfast and the then-spokesperson on justice and foreign affairs for the DUP, advocated during a *NATO Summit* debate in May 2012 the necessity to "spend more on the technology of tomorrow", because "cyberterrorism poses an ever-greater threat". Referencing this threat of cyberterrorism, Dodds urged the Prime Minister to lobby for NATO to devote resources to "that big and growing problem across the world" (2012). Nick Harvey, at the time the Liberal Democrat MP for North Devon, iterated in a *Defence Spending* debate in March 2015 that one of the most significant threats to the UK was "the ever-growing threat of global terrorism and cyber attack" (2015). Sir Hugh Bayley, then the Labour MP for York Central and president of the NATO

parliamentary assembly, echoed a similar note in the same debate, emphasising that NATO needed to counter the new and emerging threat of cyber attack (2013). Mims Davies, the Conservative MP for Eastleigh, speaking during an *Investigatory Powers* debate in June 2015, noted that "the modern world presents new challenges for our security – challenges from terrorism at home and overseas, from cyber attacks" (2015). Lastly, The Earl of Courtown, speaking during a *Global Challenges* debate in the Lords chamber, told his fellow Peers that "in the past five years the threat levels from violent extremism and terrorism, Russian aggression, cyber attacks and global conflict have grown" (2015).

The next section of this chapter offers a critical analysis of the mapped discourse relating to the notion that cyberterrorism was likely to be a threat that would escalate over time.

Cyberterrorism as a Temporally Unique Threat: Escalation of Threat – Analysis

As noted above, this sub-strand of the 'Cyberterrorism as a Temporally Unique Threat' strand revolves around the notion that, from May 2010 to June 2016, and indeed, beyond this period, the threat to the UK posed by cyberterrorism increased. That this may be represented within the official discourse may not be exceptional; between this period, the integration of the internet into British society and economy increased. According to the Office for National Statistics, in 2010, 30.1 million adults in the UK used the internet every day or nearly every day, which was almost double the estimated figure for 2006 (ONS, 2010:1). Including less frequent British users of the internet increased this figure for 2010. 38.3 million people, or 77% of the British population, were regarded as 'internet users'; those who had used the internet in the three months prior to being surveyed (ONS, 2010:2). By 2016, this figure had reached 45.9 million people, or 87.9% of the British population (ONS, 2016:2). By 2010, the internet represented a significant asset for the British economy. For instance, in 2009, the internet contributed roughly £100 billion, or 7.2% of British GDP, according to a report commissioned by Google and undertaken by Boston Consulting Group (Kalapesi, Willersdorf and Zwillenberg, 2010:5). This report noted that the UK was a net exporter of e-commerce goods and services, exporting £2.80 for every £1 imported (Kalapesi, Willersdorf and Zwillenberg, 2010:5). A 2012 report produced for Vodafone valued the size of the 2008 British internet ecosystem at £82 billion, of which 16% was cellular, and estimated that between 2010 and 2015, British

internet traffic would increase by 37% per annum (Vodafone, 2012:3). The Boston Consulting Group estimated that in 2016, the internet economy would account for 12.4% of British GDP; a figure that would have characterised the UK as more reliant on internet-mediated commerce than all of its G20 counterparts, with South Korea at 8% and the USA at 5.4% (Dean et al, 2012:9). CISCO projected that between 2015 and 2020, British internet traffic would increase three-fold, with a compound annual growth rate of 21% (2016:1). To place this against analogue traffic, the Department for Transport (2016:1) noted that road traffic had increased by 2.2% in 2015, surpassing a pre-financial crisis peak to reach a total mileage of 317.8 billion. This is not to negate the core function of the road network in the UK's economic and societal security, but it highlights that the internet – as an industry and as an infrastructure – grew rapidly over the time period under scrutiny in this thesis and was set to increase at rapid pace for the foreseeable future. With increased reliance on the internet in the fields of commerce, research and development, education and national infrastructure over the period under scrutiny, it is perhaps reasonable to envisage there being an overall elevated insecurity surrounding this aspect of the British state and economy.

From the official engagement with this sub-strand of the securitisation of cyberterrorism, it is apparent that not only was cyberterrorism characterised as a Tier One threat that was in alignment with the 'New Terrorism' thesis, this threat was deemed to be an escalating one. As noted in the beginning of this section, this is not necessarily surprising; the UK's increasing reliance on IT systems for the effective functioning of its economic and societal structures necessarily entails a heightened vulnerability. It is nevertheless intriguing that 'cyberterrorism' was explicitly referenced by Ministerial and other figures in this sub-strand; cyberterrorism was deemed to be an escalating threat irrespective of the lack of a bona fide cyberterrorist incident having occurred prior to, or during, the May 2010 to June 2016 period under scrutiny. As can be observed from the above mapped discourse, Al-Qaida was referenced as a concerted threat in relation to cyberterrorism in 2011 (May, 2011a; Neville-Jones, 2011a; Home Office, 2011:34), but by 2015 this had shifted to the threat epitomised by ISIL (Cameron, 2015a, 2015e; Osborne, 2015; Hayes, 2016). However, juxtaposing the cyberterrorist threat against that posed by state actors, the US and Israeli state-sanctioned Stuxnet attack against Iranian nuclear centrifuges across 2009 and 2010 demonstrated that, internationally, states were both willing and capable of engaging in aggressive and destructive cyber operations. In 2011, David Cameron had sought a reset of Russian relations (Stratton, 2011), but by 2014 and

the international furore over the shooting down of the airborne flight MH17, the UK was one of the keenest states advocating harsh sanctions on Russian trade in oil, gas, arms and financial transfers (Mason, Wintour; 2014; Mason, 2014; Borger, Luhn and Norton-Taylor, 2014). Whilst Russian aggression in cyberspace against other states was predominantly associated with 'information warfare' (see Giles, 2016:2) - for instance, the hacking of Estonian state websites in 2007, the hacking of Mikheil Saakashvili's website in 2008, and the switching off of channels on the TV5Monde network in 2015 (Soshnikov, 2016; Jones, 2017) – it remains that Russia had both the motivation and the capability to conduct aggressive cyber maneuvers against the UK. That Ministers and non-ministerial figures publicly 'chanted' notions of an unsubstantiated, unproven cyber threat from terrorist organisations across May 2010 to June 2016, speaks to the serious concerns of the securitising actors and the vested audience(s) about non-state application of cyber weapons, including that epitomised by terrorists.

The official discourse surrounding cyberterrorism that has been mapped in this chapter – incorporating the statements of Ministers, MPs and Lords – demonstrates that the threat of cyberterrorism was regarded as increasing across time. This notion was not merely promoted in 'ritualistic chants' by members of the first and second tiers of the audience, but was also encapsulated in the securitising acts of the national security documents. The *Strategic Defence and Security Review* of 2010 noted that "the actions of cyberterrorists … are likely to increase significantly over the next five to ten years, as our dependence on cyber space deepens" (Cabinet Office, 2010b:47). This notion was re-affirmed by the 2011 *Cyber Security Strategy*, which suggested that "the threat that [terrorists] might also use cyberspace to facilitate or to mount attacks against the UK is growing. We judge that it will continue to do so" (Cabinet Office, 2011:15). What is distinct about the threat of cyberterrorism is that it is a threat that has not occurred. Whilst this thesis has focused on the official British discourse of cyberterrorism, it is of express interest that, at least from the open-source and recorded discourses of cyberterrorism, statements from proscribed terrorist groups themselves are absent. Missing here, in essence, is the equivalent of Osama bin Laden's 'weapons of mass destruction' comment in his 1998 *Time* magazine interview (PBS, 2014), wherein a significant figurehead from a proscribed terrorist group openly signals their intent to develop cyber weapons of a capacity beyond those which only 'disrupt'. Website defacement, and the use of DDoS attacks by terrorist groups or entities empathetic to the political causes of terrorists, are not terrifying. In 2014, a *MailOnline* article reported that:

> "Islamic State militants are planning the creation of a 'cyber caliphate' … from behind which they will launch massive hacking attacks on the US and the West … both Islamic State and Al Qaeda claim to be actively recruiting skilled hackers in a bid to create a team of jihadist computer experts capable of causing devastating cyber disruptions to Western institutions" (Charlton, 2014).

However, the source for this news item was a speculative comment provided to *Fox News* by Steve Stalinsky, an executive director of the Middle East Media Research Institute. In April 2015, an *Observer* article pondered: "could ISIS's 'cyber caliphate' unleash a deadly attack on key targets?"; but again, this was a speculative piece by the author (Graham-Harrison, 2015), including comments from the respective authors of *ISIS: The State of Terror* and *The Future of Violence: Robots and Germs, Hackers and Drones*. Lastly, a *Mail on Sunday* article, published November 2015, reported that "a group called Cyber Caliphate, set up by Junaid Hussain from Birmingham, urged its followers to take control of the [Twitter] accounts to spread IS propaganda" (Gallagher, 2015). Junaid Hussain – who was also notable as the husband of Sally Jones – had by this point been killed in an American drone strike, but his digital caliphate had conducted successful defacement attacks. These attacks have included that against Tasmania's Hobart International Airport website in 2015, when it was defaced with a statement endorsing ISIS (Telegraph, 2015) and the hacking of the *Facebook* page of TV5Monde (France24, 2015). However, these hacks were more 'nuisance' or 'information warfare' than cyberterrorism per se.

As a consequence, the auditorium in which the discourse mapped in this chapter has occurred – including the securitising actors and the primary and secondary tiers of the audience – has been denied statements that one might expect from cyberterrorists, which, in effect, could have reasonably been expected to *agree* with the agents and audiences in the form of "yes, we intend to attack you in cyberspace". Granted, the dearth of such statements could be because they may be self-defeating; disseminating a message about an intention to conduct a serious and prolonged hack against British critical national infrastructure could provide the Security Services with sensitive information that would make an attack less likely. Smeets (2018) has suggested that cyber weapons are uniquely 'transitory'; the utility of a particular cyber weapon declines over time as security patches are released, old software becomes obsolete and is replaced, and new hardware systems replace legacy versions. Furthermore, according to Smeets (2018; see also Libicki, 2007; Krepinevich, 2012; Axelrod and Iliev, 2014), the 'transitory' nature of cyber weapons is particularly acute for

the offensive actor in cyberspace. Launching a weapon, or signalling an intention to launch a weapon, could mean that the weapon becomes ineffective against its intended target within months, days, or hours. However, the dearth of signalling statements from terrorist organsations, in combination with the absence of a bona fide cyberterrorist attack during the period under scrutiny, means that the official discourse operated in what is essentially a speculative echo chamber. Repeatedly warning of the existence of a serious threat to the UK, without unclassified evidence to support this claim, risks, in layman's terms, 'crying wolf'. In effect, the persistence of the temporal claims that are mapped in this chapter – the notion that cyberterrorism is an increasing threat over time and for the foreseeable future – could indicate a collective attempt by the agents and audiences who engaged in the official discourse of cyberterrorism in the UK to overcome the temporal conditioning of 'crying wolf'. By arguing that the threat was not only here right now in an immediate present, but that it would continue to exist, become more likely over time and potentially more 'catastrophic' in its impact, the securitising calls and the ritualised chanting endorsing these calls sought to increase, or even remove, the shelf-life of the securitising moments.

Consequently, it is suggested here that the British experience of the securitisation of cyberterrorism may be most effectively conceptualised as a 'process' rather than a 'single bombshell event' (Guzzini, 2011:335; see also Stritzel, 2011). The Government's (Cabinet Office, 2010a) classification of cyberterrorism as a 'Tier One' threat in 2010 was, and is, a public-facing securitising act that shifted the perceived threat of cyberterrorism to a 'securitised status'. However, this was simply a procedural labelling of the cyberterrorist threat as the most significant category of national security threat to the UK. The most emphatic endorsements of the securitisation of cyberterrorism are to be found in the discourse exhibited by the first and second tiers of the audience, in their 'ritualistic chants' (Osborne, 2015; Nevill-Jones, 2011b; Hayes, 2016; Brown, 2012). Given that cyberterrorism has not occurred, the maintenance of the securitisation of cyberterrorism was not necessarily guaranteed. The members of the first and second tiers of the audience rallied behind the securitisation, expressing their belief that this was a threat that was likely to increase over time. As was noted in the analysis of the role of the 'New Terrorism' thesis in the securitisation of cyberterrorism, the process through which the audience(s) mediated this securitisation could be said to have *evolved* it. Granted, unlike the 'New Terrorism' thesis, the notion that cyberterrorism was an escalating threat was explicitly detailed within two of the strategic document securitising acts (Cabinet Office, 2010b,2011). As a result, 'ritualistic

chanting' about the escalating threat of cyberterrorism was not adding an entirely novel concept to the partially-fixed nodal point of the securitisation. Nevertheless, members of the audience expanded on this sub-strand by using more expressive language than that encapsulated in the strategy documents. For George Osborne, the pace of innovation in cyber weaponry was "breathtakingly fast" (2015). For Francis Maude, because the threat was "ever-changing", the focus on countering cyberterrorism could not be dropped "even for an instant" (2012b,2014e). For John Hayes, the threat was not only "evolving rapidly", but was also "changing, ferocious and flexible" (2016). Lastly, for William Hague, the threat was "constantly changing" and the task of responding to this threat was "a tremendous challenge to keep pace" (2013c).

The 'anticipatory'-style of securitisation that has been applied to the threat of cyberterrorism befits a 'pre-crime' format (see Zedner, 2007). The securitisation of cyberterrorism befits the future-orientedness of counter-terrorism narratives more generally (Frank, 2015; see also Schott, 2013; Coaffee and Fussey, 2015; Zulaika, 2012), but this is perhaps more acute in the case of cyberterrorism because it lacks a historical precedent. Temporalities are both implicated and produced in security politics (Cavelty, Kaufmann and Kristensen, 2015), and the British securitisation of cyberterrorism is not an exception to this. Whilst it has been argued in this thesis that one of the core functions of the securitisation of cyberterrorism is the tacit delineation between legitimate and illegitimate forms of violence in cyberspace, this conceptual distinction relies upon the longevity of the securitisation itself. Cyberterrorism has been 'spoken into existence' (Conway, 2005). As a result, a process in which the audience(s) are upheld as active participants in reinvigorating life into the securitisation offers a framework through which the apparent longevity of this securitisation – the overcoming of 'crying wolf – can be explained. Like the British experience with counter-terrorism more broadly (Fisher, 2013), in the absence of objective measurements of the risk of cyberterrorism, power is ascribed to ambiguous speculation in an 'atemporal normality'. The discourse that has been mapped in the preceding section demonstrates that audience members were in agreement with the securitising act; cyberterrorism was a threat that was due to escalate over the years under scrutiny, and indeed for the foreseeable future.

The next section offers a brief concluding summary of the arguments that can be drawn from the mapping and analysis contained in this chapter.

Conclusion

This chapter has mapped and analysed two sub-strands of the British securitisation of cyberterrorism, both of which relate to the 'temporal uniqueness' of this threat. These sub-strands were 'New Terrorism' and 'Escalation of Threat' respectively. Regarding the 'New Terrorism' sub-strand, it was argued that whilst the securitising acts epitomised by the public-facing strategic documents had not overtly incorporated notions of 'New Terrorism' in their articulation of cyberterrorism, this was something *added* by the first and second tiers of the audience. It was found that the articulated threat of cyberterrorism had inherited aspects of the 'New Terrorism' thesis that has infiltrated British counter-terrorism narratives more broadly.

Concerning the second sub-strand, 'Escalation of Threat', it was found that the audience tiers had agreed with the warnings encapsulated in the securitising acts in the strategic documents. Without citing objective data, members of the first and second tiers of the audience included warnings about an increasing threat of cyberterrorism in some of their 'ambiguous chants'. In some cases, the language used by members of the audience was found to be more expressive than that of the original securitising acts. This, it was suggested, was a symptom of a process-driven securitisation, particularly in the case of a threat that has not occurred and can be said to exist on the basis of speculation. Repeated 'chants' about the increasing threat of cyberterrorism, without reference to specific dates or events, was said to be a rhetorical means of increasing the intersubjective 'shelf-life' of the securitisation. By suggesting that the threat of cyberterrorism was set to increase for the foreseeable future – as opposed to stating that a cyberterrorist attack is expected by X date – the members of the audience were seeking to avoid the risk of 'crying wolf'.

In academic terms, over the passage of time it will be fascinating to see whether these forward-viewing securitising calls are proven accurate by instances of cyberterrorism in or against the UK. This line of thinking also beckons a call for further research; in an environment in which anticipatory security is given credence, to what extent do forward-viewing securitising moves – concerning a threat that has not occurred and for which there is little substantive publicly-available information regarding its scale or likelihood – shut down or limit the scope for counter-securitising moves? Without oneself possessing a comprehensive knowledge of the nature of a threat, is it possible to successfully counter-securitise against a discourse that has been (re)constructed through dire, but unsubstantiated, warnings and calls for action?

The next chapter maps and analyses elements of from the official discourse that concern the second unique aspect of cyberterrorism; its spatial exceptionality. This spatial strand is divided into two sub-strands, which are ‘Physical versus Cyber’ and ‘Safe Havens’. The next chapter will also map and analyse the final strand this thesis has identified from the official discourse of cyberterrorism in the UK; ‘From Fiction to Reality’. This is the notion that to some extent, the lack of substance pertaining to the nature of cyberterrorism can be ‘filled in’ by fictional representations of threat that are depicted in popular films and novels.

Chapter Six: Cyberterrorism as Spatially Unique, and 'From Fiction to Reality'

The previous chapter analysed elements of the official British construction of the threat of cyberterrorism between 12th May 2010 and 24th June 2016 that served to inform the 'temporal uniqueness' of this threat. It was established that securitising agents and members of the audience(s) had espoused their view that cyberterrorism was an escalating threat over time. This was notwithstanding a lack of a cyberterrorist incident during this period and the absence of public statements from cyberterrorists endorsing this notion of an increasing probability of imminent attack. This sixth chapter, which is the last instalment of the analytical sections of this thesis, continues the mapping and analysis of the official securitisation of the threat of cyberterrorism in the UK, specifically to highlight the remaining prominent strands that were identified from the corpus. The first of these strands is the notion that cyberterrorism is spatially unique. This strand is divided into two sub-strands, which are: 'Safe Havens' and 'Physical versus Cyber'. The second strand is 'From Fiction to Reality', which is the notion that the lack of substance pertaining to the nature of cyberterrorism has been partially 'filled in' by fictional representations of threat that are depicted in popular media. Cyberterrorism fiction is perhaps a niche market; however, the popular James Bond film, *Skyfall*, made notable appearances in the corpus, as did William Forstchen's novel, *One Second After*.

The analytical contribution of this chapter is therefore threefold. Firstly, it is argued that the linguistics of terrorist use of 'safe havens' – spaces where terrorists can plot without interference from state bodies – had been transferred from a generic UK post-9/11 terrorism discourse to the discourse constructing the threat of cyberterrorism. Secondly, it is found that whilst cyberterrorism as a perceived threat exists because it has been enabled by computing and internet technologies, the securitisation of cyberterrorism did not draw on these technological spaces. Building on the arguments made in the preceding analysis chapters – that a conceptual cyberterrorist *identity* is the threatening construct – it is argued that this is a pre-emptive securitisation. By avoiding tying the securitisation of cyberterrorism to a particular software, hardware, terrorist group, region or conflict, the audience's 'chanting' sought to pre-empt an existing terrorist group developing a capacity to conduct cyber attacks against the UK, or a new cyberterrorist organisation emerging. Lastly, it is argued that there was an epistemic void in the UK's social-construction of the threat of cyberterrorism. One means in which members of the audience sought to partially fill-in this epistemic void

was by drawing on popular fictional narratives in which cyberterrorist attacks were either described or visualised.

This chapter begins by mapping the excerpts from the discourse that related to the first sub-strand of the strand, 'Cyberterrorism as a Spatially Unique Threat'. This sub-strand is the notion that cyberterrorists, in a similar fashion to conventional terrorists – would seek 'safe havens' from which they could plot or evade the UK's counter-terrorism efforts.

Cyberterrorism as a Spatially Unique Threat: 'Safe Havens' – Mapping

This section maps excerpts from the corpus that relate to the 'Safe Havens' sub-strand of the 'Cyberterrorism as a Spatially Unique Threat' strand. It is worth noting here that the use of the term 'safe haven' in relation to the threat of terrorism pre-dates the securitisation of cyberterrorism. The notion that terrorists were interested in communicating, training and plotting within 'safe havens' gained traction rapidly after the attacks against the World Trade Center and the Pentagon on 11th September 2001. Ten days after the attacks, the then-US President George Bush delivered a State of the Union address in which he declared, "we will starve terrorists of funding, turn them one against another, drive them from place to place, until there is no refuge or no rest. And we will pursue nations that provide aid or safe haven to terrorism" (2001). Tony Blair, at the time the British Prime Minister, incorporated this phrase into speeches delivered at the Labour Party conference on 2nd October and to Parliament on 4th October (2001a; 2001b). The 'save haven' phrase was not retired in 2001; Gordon Brown continued to use the term during his premiership (2009), as did David Cameron, who notably spoke about the potential 'safe haven' of the internet-mediated spaces of Facebook and WhatsApp (Chorley, 2015). Nevertheless, British Government usage of the phrase was not uniformly concerned with terrorists seeking extra-judicial spaces. Similarly to the argument made in Chapter Four – that there is a discursive distinction between legitimate and illegitimate forms of cyber mediated violence – there has also been inferences of legitimate and illegitimate safe havens. For example, in February 2002, the Government published a White Paper entitled *Secure Borders, Safe Haven* (Home Office, 2002; see also Walters, 2004; Sales, 2005), which sought to assuage public concerns about misuse of the UK's

asylum-seeking process. In this use of the term, the ‘safe haven’ was a spatial environment in need of protection.

If adversaries are able to operate in ‘safe havens’, whether analogue or virtual, attribution becomes more difficult. It is this notion of attribution that was prominent in the corpus, in instances where the securitising act and members of the first and second tiers of the audience alluded to the characteristics of ‘safe havens’.

For instance, in the case of the securitising act entailed by a strategic document, the 2011 *Cyber Security Strategy* highlighted that terrorists were “active today against the UK’s interest in cyberspace”, but that “with the borderless and anonymous nature of the internet, precise attribution is often difficult and the distinction between adversaries is increasingly blurred” (Cabinet Office, 2011:16). Those who engage in cyber attack typically – whether unconsciously or consciously – leave information in the code of the virus that will identify themselves as the attackers. IT security experts who are well-versed in common habits of hacking groups can also gleam insights on an attacker’s identity by drawing inferences from the ‘structure’ of the code, much like one might run analysis on sentence structure or calligraphy. Alternatively, it is also possible that attackers might deliberately attempt to misdirect investigators to an actor other than themselves.

In a June 2014 speech, the then-Home Secretary Theresa May noted that the internet “has become essential not just to the likes of you and me but to organised criminals and terrorists … we are in danger of making the internet an ungoverned, ungovernable space, a safe haven for terrorism” (2014). A similar view was expressed by Francis Maude, who, at the time was the Paymaster General and Minister for the Cabinet Office, stated in a press release that “cyber criminals and terrorists should have no refuge online, just as they should have no sanctuary offline” (2012).

Nick Clegg, the Deputy Prime Minister, gave a speech in March 2014 entitled *Security and Privacy in the Internet Age*, in which he warned his audience that the internet had “opened up new possibilities for criminals, terrorists and hostile states to plot, recruit and carry out attacks, while concealing their identities” (2014). William Hague, at the time the Secretary of State for Foreign and Commonwealth Affairs, expressed similar sentiment when he noted that “we should never forget that threats are launched against us secretly, new weapons systems and tactics are developed secretly … terrorist groups that plan attacks or operations against us do so in secrecy” (2013a).

One means through which an internet user can attempt to circumvent widely used means of online surveillance – and thereby increase the challenge of attribution – is to use free software known as The Onion Router (Tor). The utility of Tor, and terrorist interest in using this service, is examined further in the analysis section. However, it is worth noting here that references in the corpus to 'Tor', 'dark web' and 'darknet'[12] were sparse. Only one reference had been made to this software. As a lone voice in the corpus explicitly discussing the darknet, James Morris, Conservative MP for Halesowen and Rowley Regis, stated during an *Investigatory Powers* debate in June 2015 that:

> "[technology] represents a profound threat to our future national security. It provides opportunities to our enemies – for countries operating and wanting to develop cyber attacks against our infrastructure; it enables terror groups to communicate below the radar in encrypted chatrooms on the dark web; and it allows networks to develop which are difficult to detect and to analyse" (2015).

When David Cameron made his remarks on the potential for Facebook and Whatsapp to be 'safe havens' for terrorists (Chorley, 2015), he was discussing end-to-end encrypted communication, but this is not the same as Tor-enabled internet communication. A user can connect to end-to-end encrypted means of communication – for instance, by connecting to WhatsApp on their smartphone using their home router – but do so through a bona fide IP address. However, if a user tunnels all of their internet traffic through the Tor network, as far as their ISP will be aware, their communications will, by default, be encrypted. If the Tor-connected user sends and receives end-to-end encrypted communications through this tunnel, they will be sending encrypted data packets within several layers of encryption. End-to-end encryption makes snooping more challenging for those who do not have the requisite private keys, but it is darknet services that offer the greatest mainstream capacity to exponentially increase the difficulty of attribution.

Francis Maude made repeated remarks in public in which he expressed his view that the internet was 'dark' and 'menacing' (2012; 2013a; 2014a; 2014b; 2014c). However, in these five instances Maude did not expressly link this 'darkness' with the darknet; instead, he linked the dark nature of the internet to the potential darkness of human nature (2012). A socially introduced or inferred 'darkness' is not the same as the technical capacity to 'darken' online connections and communication through encryption. This is explored in greater detail in the analysis section.

---

[12] 'Dark web' and 'Darknet' are interchangeable terms used to describe websites and web services that are hosted via Tor. These services can only be accessed by internet users who are connecting to the internet via the Tor network.

It is apparent from the analyses there was some evidence from the corpus that members of the audience – most notably, former Home Secretary Theresa May (2014) and former Prime Minister David Cameron (Chorley, 2015) – were concerned about the possibility that internet-mediated communication offered a new, virtual landscape and safe haven in which terrorists, with or without the cyber prefix, could communicate and evade authorities. This sub-strand is comparatively smaller than the previous sub-strands that have been mapped in this thesis. However, it is closely linked to the next sub-strand of the spatial uniqueness of cyberterrorism, 'Physical versus Cyber'. This is the notion that there are distinct differences between analogue and virtual spaces, which have consequences for the nature of the threat of cyberterrorism. The next section offers an analysis of the 'Save Haven' sub-strand.

Cyberterrorism as a Spatially Unique Threat: 'Safe Havens' – Analysis

This section offers an analysis of the preceding mapped discourse. It is suggested here that the 'Safe Havens' sub-strand serves a similar function to that of the 'Tier One' strand identified in Chapter Four. Whilst in Chapter Four it was proposed that the 'Tier One' strand sought to create a delineation between legitimate and illegitimate forms of cyber enabled violence, it is argued in this section that the 'Safe Havens' spatial sub-strand created a conceptual distinction between legitimate and illegitimate forms of *being* in cyberspace.

The spatiality of the internet can be defined in differing ways. One way to conceptualise the spatiality of the internet is to consider the storage and movement of data. Given the vast quantities of internet traffic generated by services such as Youtube, Google, Netflix and Facebook, it is perhaps easy to overlook the gargantuan expanse of internet data beyond these public-facing and accessible services. Research conducted by Sandvine in 2013 found that in North America, Netflix consumed 28.18% of data packets transferred across the internet, and Youtube consumed 16.78% (see Solsman, 2013). If one were to imagine that the world-wide-web is depicted as an iceberg, the sphere of the web in which publicly-accessible services operate can be classed as the 'surface' web, however, the vast majority of the data held on servers connected to the web exists in what could be termed the 'deep web', a phrase coined by Michael Bergman (2001). This deep web incorporates web content that cannot be accessed by running queries against

conventional search engines or is protected by security features such as passwords. Restricted content on a user's Facebook page, or data held on a university's intranet, would be examples of deep-web data. As Weimann (2016) has noted, due to the difficulty of accessing this content en-masse through systematic means[13] it is near-impossible to meaningfully quantify the size of this 'deep' web, although some estimates have suggested that the deep web is 400-500 times larger than the 'surface' (Barker and Barker, 2013:4).

Within this 'deep' web – perhaps depictable on our iceberg as its deepest layer – is the 'darknet'. This term was popularised in a paper authored in 2002 by Microsoft researchers (Biddle et al, 2002), in which they detailed peer-to-peer networks as future avenues for content dissemination. Today, the term 'darknet' refers to servers and clients that use specific software to host and access web content. Several such services exist, but the most renowned is The Onion Router (Tor). When a host or client connects via the Tor network, their connections are tunnelled through Tor relays (proxies) around the world, essentially obfuscating their true IP address. Data packets are encrypted in several layers by the user's computer, and each 'relay' unpacks one layer of this encryption, until the data packet reaches the exit node, which unpacks the final layer of this encryption and delivers the packet to its intended addressee. Darknet content is that which is hosted by a server using the Tor network; these are web domains that a suffixed with '.onion', as opposed to say, '.co.uk'. The Tor network became increasingly popular globally over the May 2010 to June 2016 period under scrutiny, with the estimated user base increasing from roughly one million in October 2011 to approximately two million by 2016 (TorProject, 2017a). Between May 2010 and June 2016, the bandwidth usage of the Tor network increased from an estimate of just a few Gbit/s to an estimated 75 Gbit/s (TorProject, 2017b). The majority of this usage and demand on the Tor network's bandwidth is by users who use the network to connect to 'surface' or 'deep', as opposed to 'darknet' content; the Tor Project has estimated that roughly 96.6% of Tor traffic is used for this purpose (2015). By connecting via the Tor network, for example, a Chinese political dissident might be able to access an unfiltered version of Google's search engine and other sanctioned content hosted on the web.

However, it is the remaining 3.4% of Tor data usage that attracts alarmist media attention, given that Tor hidden services provide an environment in which proscribed content can be accessed and disseminated

[13] 'Surface' web sites can be 'trawled'. Trawling involves the use of a web crawler, which is a bot that systematically browses the web, saving pages as it works, which it can later use for the purposes of indexing. It is through this trawling and indexes that services such as Google and DuckDuckGo are able to compile large and useful search engines.

with relative impunity[14]. Drawing an incomplete list of 5,615 .onion addresses from the .onion search engines 'onion.city' and 'ahmia.fi', Daniel Moore and Thomas Rid (2016) ran a text-content crawler against these websites over a two month period between January and March 2015. This crawler yielded 300,000 addresses, or 205,000 unique pages from the original 5,615 urls, and Moore and Rid (2016:21) were able to conclude that, at least from their corpus, the most common uses for Tor hidden services were narcotics sales, illicit finance and violent pornography involving children and animals. However, intriguingly, they found a relative near-absence of Islamic extremism on the hidden services, with just a small number of active Jihadist websites. Commenting on this finding, Moore and Rid noted that "the darknet's propaganda reach is starkly limited … hidden services, secondly, are often not stable or accessible enough for efficient communication; other platforms seem to meet communication needs more elegantly. Islamic militants do commonly use the Tor browser on the open internet, however, for added anonymity" (2016:21-22; for instance, see an ISIS Tor guide at Archive.org, 2015). There is some evidence that terrorists have been encouraged to adopt internet safety measures such as the indiscriminate use of Tor for any online activity related to their political cause. For example, a blog post authored by presumed ISIS sympathisers, entitled *Remaining Anonymous Online*, included a section on Tor, which stated that "Tor is a world ahead of [virtual private networks] in terms of security and is the fundamental basic I recommend everyone to have" (see the full blog post cited in Bartlett and Krasodomski-Jones, 2015:10).

Curiously, given the disruptive potential of this technology, especially for the purposes of counter-terror oriented intelligence gathering, 'Tor' and 'darknet' were barely mentioned in the corpus of the official construction of the threat of cyberterrorism in the UK. No strategic document, and just one member of the audience, elected to raise the matter of Tor or darknet with reference to cyberterrorism. However, I have discussed these technologies here to emphasise that not only does the internet offer transparent spheres of communication and content dissemination, but it has also created novel man-made digital 'safe havens'.

It is not the place of this thesis to contrast the British cyberterror discourse with those exhibited in other countries; however, it is worth noting that the official American and EU discourses have both been

[14] News coverage is typically printed when there has been a failure in darknet obfuscation due to analogue investigations or the successful hacking of a Tor-connected sever (for instance, see Gibbs and Beckett, 2017; Evans, 2015; Spillett, 2017).

more explicit in highlighting concern about Tor-encrypted traffic from Islamic State (for instance, see FBI Director Comey's comments in Dunsmuir, 2015 and an Institute for Security Studies report by Berton, 2015).

Academic literature has suggested that the desire to make use of 'safe havens' is a characteristic that terrorism and international crime networks share, where the success of their operations demand secrecy and untracked movements of goods and people (Shelley and Picarelli, 2002:307). This terrorism and organised crime 'nexus' or 'continuum' is said to flourish in localities where state functions have been usurped by entities sympathetic to, or even directly aligned with, terrorist and organised crime groups (Makarenko, 2004:138; Cilliers, 2003). Kittner considered the role of safe havens explicitly for Islamic Terrorism, and defined safe havens as "geographical spaces where Islamist terrorists are able to successfully establish an organisation and operational base" (2007:308). These spaces could offer a useful environment for fundraising, communicating, training and movement. Whilst this thesis does not explicitly isolate a particular political ideology of terror – instead focusing on a *type* of terror (cyberterror) – these themes are instructive. In order to conduct a successful cyberattack against critical national infrastructure, a cyberterrorist organisation or cell would require funding, spaces to communicate, training programs and perhaps also the ability to move people or goods. The latter might seem counter-intuitive for a threat that could simply require an internet connection and the requisite knowledge about one's cyber weapon and desired target, which is theoretically possible anywhere on the planet using a satellite connection. However, as was the case with the nuclear centrifuges at the Bushehr site, not all sensitive targets are connected to the internet. Where this is the case, the movement of infected hard discs or removable storage devices is paramount, and a cyberterrorist organisation may be forced to bribe or indoctrinate empathetic employees who have access to the target computer systems.

The excerpts that have been mapped in the preceding chapter align with a broader fear that has been articulated by the British Government, concerning the ability to anonymise activity on the internet. David Cameron (Ball, 2015), as the then-Prime Minister, Theresa May (Lee, 2017), as the current Prime Minister, and Amber Rudd (Wheeler, 2017), as the Home Secretary at the time of writing, have all spoken of a desire to disrupt encryption services. Banning encryption – or placing restrictions on its usage – has some historical precedent. Prior to the widespread availability of consumer-oriented computer technology, the USA and UK had imposed restrictions on the movement of encryption technologies (Kahn, 1997). However, with the

advent of zero-cost, consumer-friendly encryption computer software such as the 'GNU Privacy Guard' (GPG), the enforcement of such restrictions is rendered impossible because the computer code can be disseminated via the internet instantaneously. End-to-end encryption serves a central component of internet-mediated commerce. The UK's unique positioning in global internet commerce, which was discussed in the preceding chapter, would be irrevocably disrupted were the Government to meaningfully attempt to implement restrictions on encryption software. An exodus of the City of London's financial service industry would be unavoidable, and an economic recession would be likely.

This is not, however, to suggest that the mapped discourse is vacuous or that those who spoke in relation to the identified 'Safe Havens' sub-strand were foolhardy. The discourse is still *doing* something. It is argued here that the 'Save Havens' sub-strand serves a similar function to that of the 'Tier One' strand analysed in Chapter Four. Whilst in Chapter Four it was proposed that the 'Tier One' strand sought to create a delineation between legitimate and illegitimate forms of cyber enabled violence, it is argued here that the 'Safe Havens' spatial sub-strand created – or re-affirmed – a conceptual distinction between legitimate and illegitimate forms of *being* in cyberspace.

Similarly to the analysis in Chapter Four, it can be identified in the excerpts that cyberterrorism was not the singular illegitimate form of being in cyberspace. In the securitising act of the 2011 *Cyber Security Strategy* mapped in this chapter, 'terrorists' were again 'packaged' with 'criminals' and 'foreign intelligence services and militaries' (2011:16). 'Othering' was another discursive tool that could be identified in this sub-strand. For example, during Theresa May's speech in which she made reference to the 'safe haven' of the internet, she suggested that the internet was essential "not just to the likes of you and me but to organised criminals and terrorists" (2014). Whereas the 'Tier One' strand served to distinguish between legitimate British state-based cyber arsenals and the illegitimate cyber weapons of terrorists, criminals and rogue states, this 'Safe Haven' sub-strand legitimises legal uses of the internet by the British population at large.

Again, this is an *identity*-based conceptual delineation by the discourse, rather than a distinction based on technical details. The relative absence of references to the technical means by which cyberterrorists could implement their online 'safe havens' or general secrecy speaks to two possibilities. Firstly, it is possible that the members of the first and second tiers of the audience were unaware of software such as Tor. The average age of Members of Parliament elected in the 2015 election was 50 (Parliament.uk, 2017),

meaning that most MPs are likely to be members of an age group that Prensky (2001) would term 'digital migrants'. 'Digital migrants', as opposed to younger 'digital natives', can, in generalised terms, be less aware of the existence and utility of novel computer software. Even if a Minister or Parliamentarian were aware of anonymising software, it is possible that they may have felt that their knowledge was insufficient to speak about the matter confidently on parliamentary record. The second possibility is that references to the technical means of implementing online 'safe havens' were deemed not necessary. The software, which exists and is widely disseminated, cannot be meaningfully curtailed, certainly not without a full-scale international consensus in which ISPs around the world agreed to shut down Tor exit nodes. Furthermore, like encryption software more broadly, anonymising software has bona fide utility by non-'Othered' citizens. An individual experiencing the appearance of an embarrassing ailment could use the Tor network to prevent their ISP or third parties from connecting their IP-address with the particular health issue. A Chinese dissident could use the Tor network to access a non-filtered version of the Google search engine. Indeed, this is one of the raison d'etras of the Tor network, and is one of the reasons that the US government has previously given funding to the Tor project. In 2013 alone, the US government provided $1,822,907 to the Tor Project (Hern, 2014).

What *can* be cajoled, regulated and punished by law is human behaviour. As a result, the 'Safe Havens' sub-strand created the delineation between legitimate and illegitimate forms of being in cyberspace on the basis of the identities of internet users, rather than on the basis of internet technologies. This is a theme that is continued in the analysis of the second sub-strand of the 'Cyberterrorism as a Spatially Unique Threat' strand, 'Physical versus Cyber'. The excerpts from the corpus that related to this sub-strand are mapped in the next section.

Cyberterrorism as a Spatially Unique Threat: 'Physical versus Cyber' – Mapping

As has been detailed in Chapter Four, the constructed threat of cyberterrorism in the UK befits the 'anticipatory' frame of security. 'Anticipating' future terrorist incidents creates spatial realities (Anderson, 2010; Bialasiewicz et al, 2007; see also Aradau and Munster, 2012), not simply through the creation of new architectures in the effort to prevent such an attack occurring (Coaffee, Hare and Hawkesworth, 2009; Collier

and Lakoff, 2008; Galison, 2001; Graham, 2004), but also through the formation of *imagined* spaces. Former Chancellor of the Exchequer George Osborne's GCHQ speech (2015) that was mapped in Chapter Five, in which he urged his audience to *imagine* the cumulative impact of catastrophic breaches against the national grid, the banking sector, hospitals and government institutions is a case-in-point. By responding to Osborne's call and imagining cyber attacks against these entities, his audience collectively create personal landscapes in their minds. It does not matter that Osborne did not specify a bank branch or a particular hospital; indeed, the spatial imagining is more powerful without these discursive anchors because the loosely-defined breaches could be targeting *your* bank(s), or *your* local hospital. This imagined space renders specificity in the temporal construct irrelevant, as the "future is seen to function in a positivistic epistemic mode, where the solution to future threats is not to understand their origins, conditions of possibility, and emergence, but to accommodate these threats through spatial ordering and mapping" (Aradau and Munster, 2012:105). To put this more succinctly, it is expected that the discourse of the socially-constructed threat of cyberterrorism would not seek to *understand* the conceptual cyberterrorist, but would instead accommodate them as a threatening actor in the UK's future security relations. This process of discursive accommodation serves purposes that have been examined in this chapter and Chapters Four and Five. Further processes, which relate to the discourse of the 'Physical versus Cyber' sub-strand, are analysed in the next section.

The constructed threat of cyberterrorism in the UK presents a seminal case study, because it is an anticipated future reality that would be delivered via a unique man-made fibre-optic and copper environment. Unlike the physical properties underpinning 'land', 'sea' 'air' and 'space', the experienced environment of the internet is rendered meaningful because of its 'virtual' as opposed to 'physical' being. One cannot project an imagined future involving a terrorist cyber atrocity without engaging both the virtual and the physical components of this environment.

There was some evidence in the corpus that securitising agents engaged with the notion that in spatial terms, the 'cyber' realm was distinct from the 'physical' realm. In 2013, Phillip Hammond, then-Secretary of Defence, announced that the UK had been developing offensive cyber capabilities; making Britain the first state to publicly acknowledge the existence of such a programme. Noting in an interview with the *Mail on Sunday* that "you deter people by having an offensive capability", Hammond referred to a "laptop army" and noted that future conflict would be fought by "IT geeks in rooms like this rather than

soldiers marching down the streets, or tanks or fighter aircraft" (2013). Hammond also used the interview to address the benefits of cyber in its capacity to reduce collateral damage (2013). For David Cameron, ensuring the armed forces were equipped with the tools to guarantee British security in the 21st century necessitated an overt recognition that the threats "had changed utterly in 30 years", from "the clarity of the Cold War to the complex and shifting challenges of today: global terrorism … cyber attack" (2014). For Cameron, this threat was epitomised by an enemy that "may be seen or unseen" (2014). Similarly, for Francis Maude, the cyber threats facing the UK were "diffuse, unpredictable and generally anonymous" (2014b). Maude also raised the notion of spatial scale when he warned that "this is the threat we face: relentless in nature, global in reach and substantial in impact … the internet is too large – and the threat is too complex – for any single organisation to respond by itself" (2014d).

The novelty of internet-mediated terrorist threat was also highlighted by audience members outside of the Government. Jim Shannon, the DUP Member for Strangleford and the shadow DUP spokesperson for transport, health and human rights suggested in a Commons debate on *Defence and Cyber Security* that:

> "while cyberterrorism may not be physical terrorism of the sort some of us in the Chamber have faced personally, and whose effects can be seen in blood and tears, the effects of cyberterrorism can bring a nation to its knees and we must ensure we are not the ones who are brought to our knees, but are instead able to withstand any such attack" (2014).

Mike Gapes, the Labour MP for Ilford South and a member of the 'Arms Export Control' and 'Foreign Affairs' committees also distinguished between physical and digital attacks, noting that threats to British security "might come not from terrorist bombs but from somebody sabotaging a banking system or undermining the supply of electricity or water to our major cities by making a minor change to a software programme, albeit one with potentially disastrous consequences" (2015).

Whilst these excerpts from the corpus are relatively limited vis-a-vis the discourse that has been mapped in Chapters Four and Five of this thesis, it is apparent that there was some recognition by those engaging with the official British discourse of the threat of cyberterrorism that there was a tangible distinction between 'cyber' and 'physical' forms of terror and threat.

The next section is an analysis of the mapped excerpts from the corpus that relate to this 'Physical versus Cyber' sub-strand.

Cyberterrorism as a Spatially Unique Threat: 'Physical versus Cyber' – Analysis

This section is an analysis of the discourse that has been mapped in the preceding section. It is argued that the UK's securitisation of cyberterrorism has not revolved around the technology that enables cyberterrorism to exist in the first place. Instead, the threatening entities that have been implicated in this securitisation are the identities and behaviours of particular users of the internet. This finding, it is suggested, may be due to legislative pragmatism. Whilst computers are machines that simply adhere to the laws of code, the human beings that use them can, in theory, be cajoled and encouraged into behaving in a certain way through laws and legislative acts.

Writing on the 'securitisation of the information superhighway', Adam Kingsmith suggested that "the object to be secured is a borderless world of free-flowing information, a single seamless environment where ideas can be shared fluidly within a cyberspace that is not controlled by spatial and temporal conceptualisations of security" (2013:4). However, this is not entirely true. The internet is tied to physical spatial entities; for instance, the exchanges, the cables spanning the earth's sea floors and the satellites orbiting its atmosphere, amongst many other objects. Owned primarily by private enterprises, these physical entities are no different 'spaces' than, say, a bustling shopping mall. Internet firms such as Microsoft and Facebook are reserved about revealing the exact locations of their vast datacentres, however, the spatial reality of the architecture underpinning the internet is, mostly, not an unknown. Cartographers at TeleGeography acquire valuable location information from industry contacts to produce their *Global Internet Geography* annual report; interested consumers here in the UK can purchase TeleGeography's detailed map of metro-to-metro area bandwidth for $175 (TeleGeography, 2017). Blum's (2012) *Tubes: Behind the Scenes at the Internet* provides an excellent insight into the tangible sights, smells and sounds of the internet.

Furthermore, rather than being seamless, as Kingsmith (2013:4) suggests, the internet is *seamed*. These seams can, and have been, broken. Sharks have been recorded as having taken an interest in fibre-optic cabling spanning seabeds. Shark attacks on cables were reported between 1985 and 1987, leading manufacturers to introduce Kevlar-like protective sheaves on cable installations (Kravets, 2015). In March 2011, a 75-year old Georgian woman who had been scavenging for copper wiring accidentally sliced her

spade through fibre-optic cabling supplying internet connectivity to 90% of Armenian users for five hours until the service was restored (Parfitt, 2011).

The physical architecture of the internet is meaningless without the values that are applied to it by human beings; without human interaction the internet is simply a mass of silicon, plastic and metal. As an 'experienced' spatial environment, the internet is singularly unique and without a true precedent. With internet-enabled technologies, internet users can inexpensively communicate with one another at the speed of light, thousands of miles from one another. Steuer aptly distinguishes this uniqueness in his application of the term 'telepresence'; accordingly, he has stated that "'presence' refers to the *natural* perception of an environment, and 'telepresence' refers to the mediated perception of an environment. This environment can be either a temporally or spatially distant 'real' environment, or an animated but non-existent *virtual world* synthesised by a computer" (1992:6, original emphasis).

In reference to the American construction of an Islamic terrorist threat, Clara Eroukhmanoff (2015:248) has highlighted the role of euphemisms and metaphor in the articulation of securitised 'Remote Others', which she noted were distant from the securitising agent(s) in spatial, temporal, and ontological terms. In the construction of the threat of cyberterrorism against British critical national infrastructure, the anticipated cyberterrorists could be said to be remote actors operating in an environment that elevates this remoteness. Phillip Hammond was able to stand in a room amongst British operatives with invited journalists from the *Mail on Sunday* (2013), in an exclusive but defined space. In contrast, the cyberspace inhabited by the unseeable terrorist 'Other' (Cameron, 2014) was 'large', 'diffuse' and 'anonymous' (Maude, 2014b; 2014d). These examples from the corpus demonstrate the significance of the *experienced* spatiality as opposed to the objective spatiality of the internet in the official British securitisation of the threat of cyberterrorism. The spatial environment of the security-providing British operatives was bounded and known, and conversely, the environment inhabited by the threatening terrorist 'Other' was characterised by its unknowability.

The act of 'knowing' a threat serves to bound its capabilities. Threatening phenomena, such as the perceived threat of cyberterrorism, cannot be adequately 'known' because there has not been an incidence of cyberterrorism. The threat posed by cyberterrorism to the UK is a socially-constructed anticipated threat. Inadequately known threats, and those which cannot be seen, have a greater potential to incite fear because

they have a greater potential to activate the imagination of a given audience (see Mitchell, 2011; Andersen and Moller, 2013; O'Loughlin, 2011). There is evidence from psychological studies that the presence of fear elevates an individual's perception of risk (Lerner and Keltner, 2000, 2001; Mathews and MacLeod, 1986). Here, we could return to the notion of the 'shelf life' of the securitisation of cyberterrorism. The discourse promoting ambiguity about the spatial environment of cyberterrorists (Cameron, 2014; Maude, 2014b,2014d) promotes fear of the threat of cyberterrorism. This is because the audience(s) are encouraged to understand that the threat exists, but are not provided with substantive knowledge about the specific actors who are likely to conduct the attacks, the kind of software that they will use, and the countries or regions from which the attacks would be launched. 'Somebody' would be the perpetrator (Gapes, 2015). Granted, three examples from the corpus mapped in the preceding chapters did explicitly state that particular groups were interested in conducting cyberterrorism against the UK. These groups were Al-Qaeda (Home Office, 2011) and the Islamic State (Hayes, 2016; Osborne, 2015). However, this may be symptomatic of these organisations being the most prominent terrorist groups in British security discourse at the time. Furthermore, a majority of the excerpts in the corpus spoke of unspecified harmful cyberterrorists, without bounding this conceptual cyberterrorist identity to a particular spatial context. This renders the threat of cyberterrorism with a certain degree of timelessness; the threat of cyberterrorism is not bounded to any particular group or conflict. The decline of a particular terrorist organisation does not therefore implicate a corresponding fall in the perceived threat of cyberterrorism.

The social construction of a securitisation of a given threat requires the threat – and the referent object to be secured – to be contextualised both temporally and spatially. Something/someone, has to threaten something/someone at a given point in time. Philosophically, threat to human life and cherished human values is timeless, but policies are drafted in a specific time and space. By rendering cyberterrorism meaningful within defined contextual boundaries in their securitising moments, the securitising actors and the members of the audience established the parameters on which policy debate is formed. When Theresa May warned of the "danger of making the internet an ungoverned, ungovernable space, a safe haven for terrorism" (2014), she was implicitly engaging with a social construction on the spatiality of the internet. The world-wide-web depends, existentially, on the spatial network underpinning it; the cables, the exchanges, the servers, not to mention the myriad of offices and support staff working tirelessly and often unbeknown to the

vast sea of users. However, the social spatiality of the internet – for instance, the distinction between 'surface' and 'dark' webs – is not recognised by the internet itself, which simply serves its core function of pushing data packets indiscriminately around the world in a decentralised fashion. These data packets contain information, and as the adage goes, 'information wants to be free' (Stewart, 1988:202). As they are not conscious, sentient beings, computers do not care about the behaviours of a human being behind the keyboard, but other human beings do, and it is using this socially-constructed social spatiality that actors such as Theresa May (2014) were able to distinguish between spaces on the internet. Again, computers do not care about legislation, policies, or rhetoric; but human beings do. As Greg Graffin and Bad Religion wrote in their song *I Love My Computer*:

> "I love my computer, for all you give to me, predictable errors and no identity … all I need to do, is click on you, and we'll be joined in the most soul-less way … the world outside is so big, but it's safe in my domain, because to you I'm just a number and a clever screen name" (2000).

The love between a person and their computer may not be reciprocal, but this is a love that is mediated through law and conditioned by social identification. From the mapping and analysis of the 'Tier One', 'Temporally Unique' and 'Spatially Unique' strands, it is apparent that whilst the spatial architecture of the internet has made cyberterrorism a possible means of causing harm and inciting fear, this architecture is not the modus operandi on which the securitisation of cyberterrorism relies. Instead, the threatening entity that is articulated by the securitisation of cyberterrorism are the identities of particular users of the internet, even if these identities are ill-defined through much of the corpus. Whilst this ambiguity could be said to make the securitisation less objective, the potential longevity of the securitisation is increased because it is not tied to a particular type of software, hardware, group, region or conflict. Oblique references to 'cyberterrorists' entail that any existing terrorist group could potentially engage in cyber attacks upon the UK, or alternatively, entirely new cyberterrorist groups may emerge.

In many respects, as human beings constructed in flesh, blood and bone, we are still in our seminal stages of developing our capacity to speak about and convey meaning regarding the spaces where the human and technical aspects of the internet intertwine. This is particularly evident in popular shows such as *CSI Cyber*, which was replete with binary digits across the screen, or computer-generated visuals of the vicarious self, zooming through a black ether criss-crossed with bright lines. Transhumanism may, in a near or distant

future, usher in an era in which man and computer are one in symbiosis. However, until this epoch, we are reliant on our language, our art and our narratives to construct our understandings of the internet and the role that it plays in contemporary society; both in holistic terms and in the manner in which it might be utilised for terroristic purposes. For the duration that our analogue selves remain reliant on linguistics, art and popular narratives, fiction will possess a central role. Here, it is suggested that the final strand that is analysed by this thesis is informative.

The next section maps and analyses the final strand that is considered in this thesis. This is the notion that, given the lack of a precedent for cyberterrorism in or against the UK, popular fiction has, to a certain extent, informed the discursive construction of this threat.

‘From Fiction to Reality’: The Role of Fantasy, Imagination and Popular Fiction in the Construction of the Cyberterrorist Threat Against the UK

This section maps and analyses the excerpts from the corpus which were found to relate to the identified strand, ‘From Fiction to Reality’. The mapping and analysis is combined because this strand has the fewest excerpts. The mapped excerpts in this section adhere to two distinct categories. The first category is the notion that there was an epistemic void in the intersubjective knowledge of cyberterrorism. The second category includes excerpts that drew on the utility of fictional representations of the threat of cyberterrorism. It is argued that the use of popular fictional representations of cyberterrorism in the James Bond film, *Skyfall*, and Forstchen’s novel, *One Second After*, were both utilised to partially fill the epistemic void in the socially-constructed discourse of the threat of cyberterrorism to the UK.

Existing literature considers the role of ‘fantasy’, ‘imagination’, and science fiction on contemporary security politics. For example, Zulaika has written on the role of fantasy in the application of armed drones in American counterterrorism operations (2012; 2014). Drone warfare itself has been described by Sluka as a fantasy, “if not literally science fiction” (2011:72). According to Andrews, an author close to the White House and Department of Homeland Security, “if you do not read science fiction, you’re not qualified to talk about the future” (quoted in Singer, 2009:160; see also Zulaika, 2014:175). The anticipatory, as opposed to

reactive, nature of counter-terrorism implicitly gives imagination a bona fide agency. As Richard Jackson notes:

> "in a reversal of empirically-informed preventive decision-making approaches which proceed on the basis of what is known about a certain risk, such as the risks posed by disease or automobile accidents, the counterterrorist must instead act upon what is unknown as projected through imagination and fantasy. The important point is that not acting is never an option, even if it means constructing a self-fulfilling prophesy or causing unnecessary suffering" (2015:36).

The *9/11 Commission Report* included a section entitled 'institutionalising imagination', in which the Commission proposed that:

> "it is therefore crucial to find a way of routinising, even bureaucratising, the exercise of imagination. Doing so requires more than finding an expert who can imagine that aircraft could be used as weapons. Indeed, since al-Qaeda and other groups had already used suicide vehicles … the leap to the use of other vehicles such as boats or planes is not far-fetched" (2004:344).

If senior figures in the American security complex had failed to imagine the potential for commercial aircraft to be used as missiles against key political and economic landmarks, their 'failure of imagination' was not universal. A close scenario was imagined by Chris Carter and Vince Gilligan and broadcast six months before 9/11 to an audience of 13.2 million in the USA (Archive.org, 2014). *The Lone Gunmen*, a spin-off show of the *X-Files*, which aired in March 2001, included in its plot a government conspiracy in which hijackers attempted to fly a commercial aircraft into the World Trade Center. Indicating a tacit recognition by the US military establishment of the imaginative capacity of the creative industries, *USA Today* (2001) reported in October 2001 that Pentagon officials had met Hollywood film-makers, including Steven Souza, who co-wrote *Die Hard*. The reported purpose of this meeting was to draw on the imaginative thinking of the creative writers to hypothesise potential terrorist plots. If a scenario could be hypothesised, it would be possible to refine suitable counter-terror systems and policies to reduce the likelihood of such an attack occurring.

The cyberterrorist threat to the UK, as an anticipated threat and as a threat that has no precedent, perhaps lends itself to drawing inspiration from popular fiction rather than recorded history. The most prominent example of a concerted and debilitating cyber attack against critical systems – Stuxnet – is more *Pearl Harbor* than *9/11* or *7/7*, given that this was an unprovoked attack by two state entities against another state entity. The Stuxnet worm was developed and distributed by the USA's Cyber Command and Israel's

signal intelligence arm, Unit 8200. Whilst there is an existing field of literature on state-terrorism (Blakeley, 2007; Claridge, 1996; Gareau, 2004; Jackson, 2008; Jarvis and Lister, 2014), there were no instances in the corpus where a Minister, MP or Peer made an inference to state-based cyberterrorism. According to the British discourse of the securitisation of cyberterrorism, this is a threat epitomised by non-state, rather than state actors.

This strand, 'From Fiction to Reality', is the notion that the official British securitisation of the threat of cyberterrorism has, in part, been informed by fictional depictions of cyber attack in which non-state actors have caused significant disruption and casualties. A point that has been laboured previously in this thesis is the absence of an incident – either in Britain or indeed overseas – that could be articulated as a bona fide cyberterrorist attack. Furthermore, there is an absence of publicly available data on the potential likelihood and scale of a cyberterrorist incident. Terrorist organisations and national intelligence services, crime agencies and police forces have obvious reasons for avoiding public indulgence of details of potential cyberterrorist operations. Were a terrorist organisation to publicly forewarn of their intention to attack, say, the water system, the public and private furore would cause water suppliers – and other utility firms – to rapidly order internal reviews of their security procedures. Internal review processes could potentially close the vulnerability that the terrorist organisation had been intending to exploit. Similarly, were GCHQ or MI5 to break protocol and publicly announce an impending attack on a water supplier and this threat bore reality, one would assume that the vulnerability would have been closed following private correspondence between the firm and the intelligence services. Consequently, the terrorist organisation behind the preparations would abandon the operation, thereby severing a potentially significant source of intelligence for the authorities. This environment – understandably necessary for successful counter-terror and counter-espionage – has the consequence of starving the publicly-attainable official discourse of the threat of cyberterrorism of knowledge about the nature of the threat.

However, for a securitisation to be successful and pervasive, the necessity to safeguard a referent object should be accepted by audience tiers that include citizens who are not privy to sensitive data. In my proposed framework for the securitisation of cyberterrorism in the UK, detailed in Chapter Four, these are the second and third tiers of the audience. It is logical that some of this public-facing epistemic void would be filled by resort to metaphor, for instance by reference to historical instances that are *like* a cyber operation

that terrorists may wish to conduct. However, popular fiction can also present an epistemic source regarding the nature of a threat; films such as *Die Hard IV* and *Skyfall*, for instance, give their enraptured audiences a window through which they can project themselves – by empathising with John McLane and James Bond – into a fixed, fictionalised experiencing of a significant cyber event. In *Die Hard IV*, terrorists led by Thomas Gabriel, played by Timothy Olyphant, hack critical infrastructure in the US, including traffic systems and the stock market. In *Skyfall*, a hack of MI6 computer systems causes a significant explosion at the Vauxhall Bridge headquarters. These fictional representations articulate perpetrators, methods, effects and aftermaths of cyber attacks conducted for the purposes of inciting terror. Fictional representation can pioneer, rather than reflect, a public discourse; it is worthwhile remembering that the term 'cyberterrorism' was first coined by Barry Collin (2002) in the 1980s, in a science fiction capacity.

In conjunction with the dearth of a cyberterrorist incident, it should be noted that despite high levels of educational provision in the developed Western world and receding trepidation regarding the use of computers[15] (Gilbert et al, 2003; Ha et al, 2011; Hogan, 2009; Jay, 1981; Rosen et al, 1987; Rosen and Maguire, 1990), knowledge of computers and associated technologies is markedly low. An OECD study of people aged 16-65 in 33 developed states found that in aggregate, 5% of the population possessed cogent computer-related skills[16], one third could complete medium-complexity tasks with a computer[17], and 26% were unable to use a computer at all (Nielsen, 2016). Given that none of the tasks demanded of the participants in the OECD study involved sifting through system logs, non-GUI command-line interfaces or compiling source code, these statistics are likely to mask the real figures of people living in the developed world – including Britain – who possess a cogent knowledge of computers and the respective hardware and software that make the connected world function. British 'cyber' health drives, such as the *Cyber Streetwise* campaign[18] focus on basic user guidance such as the installation of firewalls, anti-virus software and password protection, but do not detail explicitly the processes involved in typical cyber attacks. Consequently, when people are encountering information on cyber threat, they may become disinterested if

---

15 Concern about computers is not entirely absent. Some figures have articulated concerns about the development of advanced artificial intelligence (for instance, see British Science Association, 2016; Future of Life Institute, 2015).

16 A 'level three' task, as defined by this survey, could involve asking participants to find what percentage of emails sent by John Smith were about 'sustainability'.

17 These 'medium-complexity', or 'level two' tasks involved, for instance, the completion of an online form.

18 A cross-government campaign funded by the National Cyber Security Programme, led by the Home Office. The campaign's aim is to measurably improve the online safety behaviour of consumers and small businesses.

they encounter too many terms such as ‘TCP’, ‘exchange’, ‘packet-sniffing’, ‘botnet’, ‘zombie network’ etc. The media – whether televisual, radio or print – can only expend so much time or space explaining what such terms mean, thereby imparting on the discourse a superficiality that is shared with, say, the reporting of research on nano-technology or cutting-edge batteries (Beckford, 2011; Markoff, 2017).

However, as noted previously, in order for a securitisation to function it must be assimilated successfully by multiple tiers of an audience. For this assimilation to occur, the attention of the audiences must be held so that the pre-requisite knowledge and the securitising agent’s arguments can be transmitted. Immediate emotional engagement – and thus the interest and empathy required – can be summoned amongst the audience(s) if the speaker can raise a work of fiction dealing with ‘cyber’ that the audience has previously encountered and remembered. *Skyfall* was reportedly the highest grossing film at the UK box office by July 2013, earning nearly £103 billion (Brown, 2013). In this instalment of the Bond franchise, ‘M’, played by Judi Dench, watches as the headquarters of MI6 is attacked with a cyber weapon that causes a significant detonation. The following film, *Spectre*, further illustrated the aftermath of this cyber attack, with the same building exhibited as a ruined derelict awaiting controlled demolition.

Two Hansard contributions and two speeches helped to construct this ‘From Fiction to Reality’ strand, making this strand the most limited of all three strands that this thesis has mapped from the corpus. However, this certainly does not necessitate that the strand is insignificant. Whilst the efforts of politicians to ‘humanise’ themselves during electoral campaigns by gingerly recalling the price of a pint of milk, brandishing a jar of Hellman’s mayonnaise to journalists invited into their family home, or professing their enjoyment of NWA’s rambunctious ‘gangsta rap’ (Abbey, 2015) can prove humorous, our elected representatives are not automatons immune to the pervasiveness of popular culture, and I would argue that their references to popular culture during policy debates can prove revealing.

As discussed previously, then-Chancellor of the Exchequer George Osborne had urged an audience to *imagine* the impact of cumulative catastrophic non-state cyber attacks (2015). Urging audience members to apply their imagination befits an anticipatory threat framework, but it also speaks to the need to fill a void of substantive knowledge about a threat. Other figures in the corpus claimed that there was insufficient attention being paid to non-state cyber attacks, were confused about what cyberterrorism was, or resigned themselves to the impossibility of forecasting the nature of cyberterrorism.

Whilst he did not reference specific actors – terrorist or otherwise – the crossbench Peer Lord Ramsbottom, a former Lieutenant General in the UK army, expressed alarm in January 2013 that:

> "insufficient attention is being paid to the ever-increasing threat of cyber warfare. Cyber weapons can not only disarm an adversary before he has even begun to fight, but render sophisticated armouries and even nuclear deterrence obsolete. Furthermore, as has been proven in Estonia and Georgia, cyber weapons threaten every aspect of a nation's existence" (2013).

In a similar vein, the Liberal Democrat Peer, Lord Alderdice, expressed his view that the 'psychology' of cyberterrorism was an under-developed field. Accordingly, he stated that:

> "I am yet to see sufficient attention being paid to research on the psychology of cyberwar and cyberterrorism. I declare an interest as someone who has given time academically and in business to this area. I hope that my noble friend will be able to tell me that additional resources will be devoted to research into understanding how people function in this fifth space" (2013).

In defence of the field of psychology, British academics are engaging in research on cyberpsychology (for instance, see McAlaney, Taylor and Faily, 2015). Furthermore, the journal of *Cyberpsychology, Behaviour and Social Networking* has been publishing since 1998, and the journal of *Psychological Research on Cyberspace* has been publishing since 2007. However, Lord Alderdice is quite correct that there has not been any substantive research on the psychology of cyberterrorism. A period under which there is a lack of research into an incipient phenomenon such as cyberterrorism will contribute to the extent to which the threat can be considered 'unknown' in stature or nature.

Earl Howe, speaking in the Lords Chamber as a Minister of State for the Ministry of Defence, expressed concern about the 'substantial' increase in the threat from terrorism, and noted that "it is impossible to predict the threats that we will face in ten or fifteen years" (Curzon, 2015b). Earl Howe was not alone in his perception of cyberterrorism as a relatively 'unknown' threat. Prefacing his critique of the 2010 *SDSR* and *National Security Strategy*, James Gray, Conservative Member for North Wiltshire, voiced his alarm that he and others present in the Commons Chamber had heard "about cyber warfare and so many other aspects of the world that are extraordinarily worrying and dangerous, but also extremely unknown. We simply do not know what is occurring in most of the world, and we do not know what we are going to do about it" (2015). Lord Patten also critiqued the epistemology of Government policy. In a debate on amendments to the *London Olympic Games and Paralympic Games Bill* in November 2011, Patten lamented

a ‘yawning gap’ in the drafting because cyber risks had not been included. Patten continued that “if anything is going to happen to disturb the games apart from random acts of terrorism, involving whatever devices or armaments, which may or may not be successful, it is going to be cyberattack – on the ticketing, on the transport infrastructure, on a whole range of other matters” (2011).

Baroness Finlay, speaking in 2011, perhaps identified one reason for the lack of consideration of cyberterrorism in Government policy outside of the Strategy and Strategic Review documents. The crossbench Peer and Vice President of Marie Curie Cancer Care, President of the Chartered Society of Physiotherapy and Chair of the Palliative Care Strategy Implementation Board for Wales commandeered a *Health and Social Care Bill* debate in December 2011, to convey to her colleagues that “we have heard today about infection, but the greatest threat to public health may well not come from infection but from issues such as cyberterrorism around our major utilities and the havoc that that could cause” (2011). Her point of contention was that personnel in local authorities might “feel that such things are remote and unlikely to happen” (2011). For such an experienced professional – who will have had some direct experience of governance of IT implementation for health services in local authorities – to use her time in the Lords Chamber to emphasise concerns about cyberterrorism rather than an explicit matter of health, is certainly of note.

Lastly, there was one instance of diversion from the overarching consensus on cyberterrorism as a terrorist attack against critical infrastructure. Margaret Ritchie, the SDLP Member for South Down advocated the perspective that cyberterrorism was already reigning havoc upon some UK citizens. Designating cyber bullying as a form of cyberterrorism in a debate on *Cyber Bullying*, Ritchie urged the Government to form an action plan with online communications firms, local communities and churches to tackle this insidious form of ‘cyberterrorism’ (2013). Whilst cyber bullying can cause immense discomfort, particularly to children – provoking suicide in the most extreme cases – the perception that this represented a form of cyberterrorism was not espoused by other figures in the corpus, and indeed, this notion runs counter to both the official discourse and cyberterrorism academia. Nevertheless, Ritchie’s comments are of note because they demonstrate the intersubjective, malleable nature of the linguistic label ‘terrorism’ and would have, in part, been fed by the lack of publicly-accessible substantive knowledge about cyberterrorism which

could be used to delineate between what cyberterrorism is and is not. Indeed, it is perhaps surprising that more Parliamentarians did not similarly co-opt the cyberterrorism label for alternative purposes and issues.

Having mapped excerpts from the corpus that related to the epistemic and policy vacuum of cyberterrorism, the ensuing discussion maps the efforts by some Ministers and Parliamentarians to draw on popular fictional representations of cyberterrorism in an effort to assuage a lack of knowledge about the nature of this constructed threat.

Jim Shannon, at the time the shadow DUP spokesperson for transport, health and human rights, expressly articulated the power of fictional representation of cyber threats during a *Defence and Cyber Security* debate in the Commons Chamber in March 2014. Accordingly, he told fellow Parliamentarians that:

> "all of us, both inside and outside of the House, will have watched films on television in which Governments are brought down by computer networks. I remember thinking that that was science fiction and that it could never actually happen, but all of a sudden, in our own lives as elected representatives dealing with constituents, we have found ourselves relating to some of the issues with which they have had to deal in connection with, for instance, banks. There is a real, definite possibility, for which we must be prepared" (2014).

Speaking during the same debate, Madeleine Moon, the Labour Member of Parliament for Bridgend and at the time a member of the Defence Committee, recalled reading William Forstchen's (2009) *One Second After*. In this novel, which includes a foreword authored by Newt Gingrich, three ballistic missiles carrying thermonuclear warheads are fired from re-purposed shopping containers into the atmosphere above the United States, causing what is known as the 'Compton Effect' to occur. Traditional application of a nuclear weapon is to detonate the warhead much closer to the target – typically a populous city or strategic locale – without actually reaching ground surface. However, by detonating a nuclear warhead higher than 25 miles above the earth's surface, high-gamma radiation is released, which reacts with air molecules to produce positive ions and recoil electrons which are known as 'Compton electrons'. The Compton electrons are rejected, leaving behind the positive ions, and the Compton electrons subsequently interact with the earth's magnetic field to produce charge acceleration. This charge acceleration radiates an electromagnetic field as an instantaneous and pervasive electromagnetic pulse. In the novel, the result of this nuclear-induced EMP is the instantaneous destruction of all electronic equipment that is not sufficiently insulated in a vacuum or lead safe located underground. All mobile phones, computers, vehicles that require electronics for ignition (almost all currently running motor vehicles), container ships relying on automated software at shipping ports, and

modern farming techniques cease to function, and the entire landmass of the 48 states is plunged into a post-electrical era. As the reader follows the story, they encounter widespread looting, homicide, the consumption of family pets and, eventually, human cannibalism. The novel's protagonist, John Matherson, a lecturer at a rural North Carolina university campus, retains the privilege of mobility via his mother's '59 Ford Edsel and, as a warmly-regarded professional member of the community, assumes a position of authority in his town, Black Mountain. The novel follows Matherson's efforts to establish order and prevent Black Mountain from being ransacked or becoming plagued by the renaissance of diseases hitherto unknown to the memories of living North Carolinians.

In her recollection of her reading of the novel, Madeleine Moon told the Chamber that:

> "the Chairman of the Defence Committee [James Arbuthnot] and I were given a book for holiday reading: *One Second After*. That delightful read, which probably wrecked my summer, was a description of the United States after an electro-magnetic attack had taken out all its computer-based systems. Everything went. No cars would go on the road and nothing would work. It was a scary prospect and I now understand why the Defence Committee's Chairman runs a car that does not have a computer in it. I am sure the book was a great influence in the decision to purchase that car" (2014).

The novel also appeared to instruct Moon's perception of the nature of the adversary that might elect to conduct a catastrophic cyber attack. Accordingly, she continued that:

> "the book also made me aware of the very narrow issue of who is the enemy. In traditional warfare, we tend to know who we are fighting, but in future we may be fighting criminals who are holding the country to ransom. We could be fighting terrorists, because a state is not needed to manufacture a cyber attack, or activists or anarchists. It has been suggested that some of the attacks in Estonia were by third-party actors. At the bottom of the list is the potential for a state to attack, because states like rules and the rest do not follow rules. That is why they must be our focus, our worry and our concern" (2014).

Moon's admission that it 'probably wrecked' her summer indicates that she found the novel both emotive and instructive. Certainly, the personal impact of the novel was sufficient for her to weaponise it in her re-chanting of the securitisation of non-state launched cyber weapons; even though the atmospheric detonation of thermonuclear warheads is not *cyber* per se.

As noted earlier in this chapter, *Skyfall* was a significant commercial success that included within its plot an incident bearing concerted similarity with cyberterrorism. *Skyfall* was referenced by James Brokenshire, at the time Parliamentary under-Secretary for the Home Office, in the opening remarks of his March 2013 speech on *Cyber Crime*. Accordingly, Brokenshire informed his audience that:

> "in the latest Bond movie *Skyfall*, technology and the ability to threaten the UK's interests through the internet are at the very heart of the drama. I'm sure you've all seen it, but Bond's latest nemesis hacks into top secret Government systems, exposes the identities of covert agents online and in one of the most memorable scenes causes an explosion at the heart of MI6 by manipulating sensitive computer systems. It's a great film and deserves the huge success it's received around the world. Of course it's fiction; Bond thwarts the villain and order is restored. But the real world threats we face as a country from the terrorists, the fraudsters, the hackers and those intent on using the internet and our ever more connected world to cause us harm are real, are significant, are enduring and our growing" (Home Office and Brokenshire, 2013).

Skyfall was also referenced three and half years after its release date in a March 2016 speech on *Expanding the Cyber First Programme* delivered by Matt Hancock, at the time the Paymaster General and Minister for the Cabinet Office. In his opening remarks to his assembled audience at the Institute of Directors, Hancock stated that:

> "I'm told Ian Fleming was a regular here while he served, and I can't help but think of a line from the new cyber savvy Q in *Skyfall*: 'I can do more damage on my laptop sitting in my pyjamas before my first cup of Earl Grey than you can in a year in the field'. I'm glad to see you all made it out of your pyjamas this morning. But Q had a point. It's not just soldiers, sailors, airmen, and policemen we need to protect our assets and livelihoods today. Today a line of code can ruin lives just as any bomb or bullet" (2016d).

From these two excerpts, it is apparent that *Skyfall* was an instructive film for both Brokenshire and Hancock. For both men, the commercially successful Bond film illustrated the capacity of cyber weaponry to cause tangible, physical damage and provided them with a go-to fictional case study to illuminate the arguments about the necessity for the British state to invest in measures to counter cyber threats from a range of actors including terrorists. The 'cyber as a means of perpetrating terror' narrative in *Skyfall* has utility in the re-chanting of the securitisation of cyberterrorism, particularly in the UK, because the Bond franchise is a widely-watched and recognised platform and the filming locations for the cyber destruction scenes were in central London. That Matt Hancock (2016d) chose to solicit a reference to *Skyfall* three and a half years after its release indicates the longevity of this utility.

According to Roland Barthes, "narration can only receive its meaning from the world which makes use of it" (1977b:115; see also Bakhtin, 1981, 1986; Kermode, 1967; Hall, 1987). When Matt Hancock (2016d), James Brokenshire (Home Office and Brokenshire, 2013) and Madeleine Moon (2014) referred to *Skyfall* and *One Second After* respectively in the securitising 'moments', they were invigorating meanings of these fictional pieces by directly relating their narratives to the 'real world' threat of cyber attacks against the

UK. For these figures, the fictional narratives were not abstract, nonsensical stories to be disregarded as irrelevant, but were instead *warnings* of the potential consequence of cyber attacks launched against the UK. Unless they are drafted by the Cabinet Office or another Government department, fictional narratives, whether represented in print media, in televisual image, in comic strips, in cartoons (Mazid, 2008; Hansen, 2011), in photographs (Griffin, 1999; Mitchell, 2011; Campbell, 2003; Shepherd, 2008; Moller, 2007; MacDougal, 1998; Coskun, 2012; Rodriguez and Dimitrova, 2011; Hansen, 2015; Heck and Schlag, 2013; Perlmutter, 1993) or in symbols (Vouri, 2010), do not themselves possess the agency to be considered speech or visual acts within the official securitisation as defined in this thesis. However, when securitising agents or members of the tiered audience make an explicit or inferred reference to popular fictional narratives, the narratives become mobilised in the 'moment' of the securitisation.

Skyfall and *One Second After* are not the only popular fiction pieces engaging with the notion of cyberterrorism. Readers are likely to be aware of a plethora of relevant fictional pieces that could be linked to narratives of cyberterrorism; for instance, *Die Hard IV* or *Wargames*. As Rathmell has noted, "the entertainment industry, in the form of films and novels has popularised the notion of an electronic doomsday scenario in which sub-state groups manage to penetrate critical nodes of the NII and DII and are able to, variously, launch nuclear weapons, crash the telephone system, cause mayhem on the railways or in the air or bring the financial sector to a catastrophic halt" (2008:42).

However, the utility of popular fiction in securitising moments is not exceptional to the threat of cyberterrorism. In his article on the construction of a global health pandemic epitomised by the H1N1 virus, Abraham (2011:805) noted that after the collapse of the USSR, popular films and books in the USA had depicted 'exotic viruses' emerging from 'wild zones' around the world. As Heather Schell recognised, in an international environment in which the perceived Russian threat to the West receded, lethal new viruses had "become a hot topic for science best-sellers, medical research, action movies and science fiction. On the big screen, virus thrillers like *Outbreak* and *Twelve Monkeys* have attracted major stars and large audiences" (1997:94-95). Again, these fictional works were not crafted in isolation of an objective reality, but instead reflected the possibilities of threat contained within the 'real world' itself. An elevated concern about the risk of global health pandemics emerged during the Clinton administration in the USA, epitomised by the publication of the National Intelligence Council report entitled *The Global Infectious Disease Threat and its*

Implications for the United States (NIC, 2000:5; see also Abraham, 1997; Fidler, 2003). Furthermore, popular fiction not only appears to have a capacity to inform notions of threat, but it can also proscribe means to counter threats. For example, Shabtai Shoval, the founder of Suspect Detection Systems, an Israeli security firm, was inspired by the film *Minority Report*, set in a dystopian 2054 in which crimes are predicted and prevented before they can occur. Instead of feeling perturbed by the notion of pre-crime prevention, Shoval mulled "how great it would be to be able to prophesise a crime before it happens" (Brinn, 2005). His firm developed the SDS-VR-1000, a machine that ascertains a person's emotions by measuring their facial and physiological responses to questioning (see Adey, 2009:282).

The mediums through which popular fiction is conveyed to its audiences is not static, but instead in a process of development and refinement. The changing technology alters the mediums of human interaction, and some mediums may possess a greater capacity to influence a securitisation than others. In his *What is Cinema?* essays, Bazin suggested that "one may think of the film as a supernovel of which the written form is a feeble and provisional version" (1972:59). As Bleed has noted, "visuals created with new technologies are changing what it means to be literate. Literacy of the 21st century will increasingly rely not only on text and words but also on digital images and sounds" (2005:1; see also Holland, 2016). As Mirzoeff has stated, "modern life takes place onscreen" (1999:1). In the future, the increasing extent to which these mediums can impart immersive virtual experiencing of a narrative, as opposed to vicarious enjoyment of it, may serve to intensify the scope of epistemic construction and emotive engagement that could be utilised in securitisations. As had been noted of an experience with 3D cinema:

> "you feel the experience, you don't just see it. I felt if I had stepped through that window and was riding the roller coaster myself instead of watching somebody else. I felt vertigo … and was convinced on the spot … that the future of cinema would mean the creation of films that create the total illusion of reality (Heilig, quoted in Taylor, 1998:279; see also Bos and Kaulingfreks, 2002:16-17).

If a 'virtual reality' release were feasible, rather than vicariously observe the cyber enabled destruction of the MI6 building in *Skyfall*, one could instead feel the intense reverberations, the deafening noise, smell the incendiary material, gasp as dust clogs the throat and stagger in a disoriented fashion. Future research could investigate how such fictional narration potentially influences securitising motions. On the one hand, the experiencing of a cyber enabled detonation could be a terrifying experience, shocking

audiences and re-affirming the prerogative to elect representatives who pledge to prevent such an incident from occurring in everyday life. As Julie Matthews has suggested, even with current and former technologies, "instant access to visual images and emotional accounts of terrorism have secured them a vivid place in our memory and reinforced the idea that 'we' have been targeted and are under immediate threat" (2005:203; see also Jackson, 2005; Croft, 2006; Altheide, 2010; Nilges, 2010; Holland, 2011,2013,2016). The concepts of 'risk' and 'fear' are inherently linked; a presence of fear is understood to elevate an individual's perception of risk (Lerner and Keltner, 2000,2001; Matthews and Macleod, 1986). Research has found that exposure to graphic imagery of victims of violent incidents could lead to minor shifts in perceptions regarding policies that relate to the violence, and that repeated exposure to the imagery did not necessarily entail de-sensitisation (for instance, see Scharrer and Blackburn, 2015; Aust and Zillmann, 1996; Scharrer, 2008; Gadarian, 2014; Gartner, 2011; Hayes and Myers, 2009; Morgan, Lewis and Jhally, 1992; Oliver, Mares and Cantor, 1993; Stahl, 2013; Norris, 1994). On the other hand, it is possible that virtual, but realistic, experiencing of such trauma could prove, for some, to be de-sensitising. The ability to film or photograph death, for instance, has created a process whereby the 'unknown' experience of death can be coded, and "the essentially unrepresentable event can be viewed, contained … and opened up to a scrutiny that is culturally sanctioned" (Sobchack, cited in Petley, 2005:182,184; see also Davies, 2010). Similarly, there is some evidence that phobias can be assuaged through repeated on-screen presentation of the object that one is afraid of (for instance, see Teasdale, 1977; Eysenck, 1977; Nias, 1979).

This section has mapped and analysed excerpts from the corpus that were found to adhere to two categories. The first category was the notion that there was an epistemic void in the intersubjective knowledge of cyberterrorism. The second category included excerpts from a Minister (Hancock, 2016d) and two MPs (Moon, 2014; Shannon, 2014) that drew on the utility of fictional representations of the threat of cyberterrorism to highlight its potential to cause severe damage to critical infrastructure. It has been argued that the use of popular fictional representations of cyberterrorism in *Skyfall* and *One Second After* served to partially fill the epistemic void in the socially-constructed discourse of the threat of cyberterrorism to the UK.

Conclusion

This chapter has mapped and analysed two separate strands that can be identified in the official construction of the threat of cyberterrorism in the UK. The first, 'Cyberterrorism as Unique Spatially', was divided into two distinct sub-strands. The first of these, labelled 'Safe Havens', was the notion that the decentralised nature of the internet, and in particular, encrypted 'spaces' epitomised by the 'darknet' offered terrorists a virtual locale in which they could plot and launch attacks against British infrastructure. From the mapping and analysis of the corpus, it was found that barring one instance, mentions of the 'darknet' were largely absent, but that the linguistics of terroristic 'safe havens' had been applied by securitising agents and members of the audience respectively. This was a useful finding, as it demonstrated that some of the linguistic tools typically applied to official narratives of post-9/11 terrorism had been transferred to the discourse of the threat of cyberterrorism. The second of these sub-strands, 'Physical versus Cyber', was the notion that the internet had established an entirely novel, man-made environment. Overarching these sub-strands was the argument that the articulated distinctions between 'spaces' on the web were not technical, but instead social. Indeed, apart from James Morris (2015), those who engaged with the idea of 'spatiality' in their securitising moments did so entirely with respect to the social spatiality of the web, rather than its technical spatiality. This may speak to the knowledge gap amongst our elected representatives about the way in which computers and the internet function. It may also be indicative of legislative pressure; it is far easier to legislate the social spatiality of the internet (even if enforcement may be difficult), than it is to legislate the technical spatiality. This is because governing the technical spatiality of the internet cannot be conducted in the UK in isolation; all major parties to the internet would need to agree to the imposition of legislation and be comfortable enforcing the technical means of delivering this legislation. Nevertheless, this was an important finding, because it demonstrated that the UK's securitisation of cyberterrorism was not tied to any particular software, hardware, terrorist group, region or conflict. Building on the findings of Chapter Five – that the audience's 'chanting' had sought to increase the longevity of the securitisation of cyberterrorism by implying that the threat was likely to increase over time – this suggests that the securitisation was pre-empting the possibility that an existing terrorist organisation might develop the capacity to conduct cyber attacks against the UK, or that entirely new cyberterrorist organisations might emerge.

Lastly, the final strand that this chapter mapped and analysed was ‘From Fiction to Reality’, which was the idea that in the absence of a real-life incident that could agreeably be labelled as an instance of cyberterrorism, securitising agents and members of the audience had, to a certain extent, been informed by popular fictional representations of what a cyberterrorist incident might feel and look like. Given our limited linguistic capabilities of describing the experiencing of our computer-ised world, in combination with the lack of a cyberterrorism case study, there were three instances from the corpus in which popular narratives, in particular those from *Skyfall* and *One Second After*, were found to have been given utility.

The final chapter of this thesis, the Conclusion, serves four functions. Firstly, the concluding chapter summarises the arguments that have been established in the mapping and analysis chapters of this thesis. Secondly, the limitations of the research are considered. Thirdly, this final chapter suggests some future avenues for research that would further elucidate the research questions that have underpinned the mapping and analysis here. The last section offers some final remarks.

Chapter Seven: Conclusion

This concluding chapter to the thesis serves several functions. Firstly, this chapter summarises the contributions that have been made both to our understanding of the securitisation of cyberterrorism and to securitisation theory. Secondly, this chapter reflects on the limitations of the research approach that has been used for the mapping and analysis of the official British securitisation of cyberterrorism. Thirdly, this chapter suggests future avenues for research that are related to either the analysis of securitisations, or to our understanding of cyber threat. Lastly, this chapter offers some final remarks.

This thesis has mapped a corpus of the official British political discourse that constructed the threat of cyberterrorism to the UK between 12th May 2010 and 24th June 2016. The thesis applied an interpretive discourse analysis against the 110 unique sources selected from the corpus in order to dissect them and ascertain the 'strands' that were shared between them. Whilst a plethora of strands could have been identified from the corpus, the thesis was able to make the strongest contribution to our understanding of the process by which the perceived threat of cyberterrorism came to be 'securitised' by focusing on the most prominent of these. The strands that were selected for mapping and analysis were chosen because the greatest number of excerpts adhered to them.

These strands were identified through a process of asking targeted questions against each unique source from the corpus. These questions, which directed the mapping and analysis, were informed by the research aims of the thesis. Accordingly, the research aims were:

1. How has official discourse in the UK represented the threat posed by cyberterrorism to the UK?
2. How do securitising actors and members of the audience securitise a threat that does not exhibit a historical precedent?
3. Given that a cyberterrorist incident may not be attributable, could be delivered in a near-instantaneous fashion, and would rely on a man-made 'fifth sphere' of power, what novel contributions for the framework of securitisation theory, if any, can be inferred from this socially-constructed threat?

The next section summarises the findings of the preceding mapping and analysis chapters.

Findings

It was established that four strands and four sub-strands could be identified as the most concerted themes exhibited by the discourse. The first of these strands was the notion that cyberterrorism represented a 'Tier One' or severe threat to the UK. This was a strand that first acquired formal traction in 2010, with the publication of updated strategy documents (Cabinet Office, 2010b:47), and the emergence of this strand established the securitisation of the threat of cyberterrorism to the UK in official British discourse. The appearance of this strand in the public-facing revision of British security priorities was, in effect, the securitising act.

It was argued that the Government's effort to ascribe a 'securitised' status to the perceived threat of cyberterrorism did not simply begin a process in which cyberterrorism came to be regarded as a significant risk to British national security. By endorsing the discursive (re)construction of a particular illegitimate form of cyber violence, the securitisation of cyberterrorism not only served to justify extraordinary measures against cyberterrorists, but it also tacitly endorsed the UK's cyber weaponry program.

It was apparent that cyberterrorism was regarded as a unique threat. Part of this uniqueness was characterised by its 'temporal' condition; which could be divided into two sub-strands. One of these sub-strands aligned with the problematic, but nevertheless potentially influential, 'New Terrorism' thesis. In its mediation through the 'chanting' of audience members, the conceptual cyberterrorist identity was assumed to be 'evil', 'depraved', and 'menacing'. It was suggested that the discursive treatment of the hypothetical, spoken-into-existence cyberterrorists by MPs, Ministers and Lords befitted a process of 'silencing' that had already been applied to conventional forms of terror. This silencing, in effect, further added to the notion that cyberterrorism was an illegitimate form of violence; there could be no rationale or space for cyberterrorism in a liberal democratic state such as the UK.

The second sub-strand aligned with the notion that cyberterrorism represented a threat that was likely to escalate over time, rather than recede or remain static. Because Ministers, MPs and Lords advocated the fear that this was a threat that would escalate, despite cyberterrorism having not occurred, it was suggested that this was a socially-constructed threat that meshed comfortably with 'anticipatory' (as opposed to preventative or reactive) articulations of threat. The mapped 'ritualistic chanting' from the audience was

found to have been more emphatic than the original statements of the security documents. The pro-active engagement from the audience, it was suggested, had served to extend the shelf-life of the securitised conceptual cyberterrorist. Whilst this evolution of the securitisation did not make it impossible to retract, it did make it harder to contest; particularly given that there were no dissenting voices to be found in the full corpus relating to the threat of cyberterrorism.

The novelty of the threat of cyberterrorism was also attributable in part to its 'spatial' condition, which, similarly, could be divided into two sub-strands. The first of these sub-strands befitted the notion of 'Safe Havens', a phrase which, when used in relation to terrorism, suggests that terrorists seek spaces in which they can operate with relative impunity. It was argued that this sub-strand created a delineation between legitimate and illegitimate forms of *being* in cyberspace. From the corpus, it was apparent that 'cyberterrorists' were regarded as a standalone entity, but they were also 'packaged' with cyber criminals and rogue states. By 'packaging' more than one form of illegitimate cyber *being* together, the 'Safe Havens' sub-strand legitimised legal uses of the internet by the British population at large.

The second sub-strand was the perception that there is a distinction between 'physical' and 'cyber' spatial environments. It was established that the 'cyber' environment, as the man-made 'fifth sphere' of power projection, could be characterised as exhibiting both a 'technical' realm, underpinned by the computers, servers and other infrastructure that enable data packets to be pushed between computer systems, and a 'human' realm. Concerning the securitisation of cyberterrorism, the human, or 'experienced' environment of cyberspace was a priori to the technical environment. Given that computers do not respect laws nor rhetoric, it was suggested that the securitisation of a 'cyberterrorist' identity revolved around the projected and anticipated behaviour of cyberterrorists, rather than the hardware and software that would permit cyberterrorism to occur in the first place. This finding substantiated and re-affirmed the preceding analyses. The securitisation of cyberterrorism was an identity-based securitisation, rather than a securitisation of the technology that enabled cyberterrorism to exist as a potential threat. This suggestion was supported by the relative dearth of discussion of the Tor-enabled 'darknet' within the mapped corpus, and represented a novel contribution to our understanding of the securitisation of a cyber threat.

Finally, it was identified that there was an epistemic void in the discourse of the threat of cyberterrorism. This epistemic void was said to exist because there had not yet been a bona fide case study of

a cyberterrorist incident, and there was an absence of publicly-available information on the propensity of proscribed organisations to actively develop or use cyber weaponry. Through the mapping and analysis of the discourse relating to this strand, it was found that this epistemic void in the securitisation of cyberterrorism had been partially filled-in by references to fictional narratives that were offered by the James Bond film, *Skyfall*, and William Forstchen's (2009) novel, *One Second After*.

Pantomime Audience Framework

An alternative framework for the relationship between securitising actors and the audience was offered. This framework, which I termed the 'Pantomime' model of securitisation, was built on the notion of Oren and Solomon's (2015) 'ritualised chanting', and was an overt response to claims that the existing model for the actor-audience relationship was inadequate. Instead of maintaining the concerted dichotomy between securitising actors and the audience, this framework actively promoted the idea that securitising actors were themselves also a part of the audience. In essence, after the core securitising move which establishes the discursive foundation for the securitisation (for instance, in the case of the threat of cyberterrorism, this was the publishing of the 2010 *National Security Strategy*), the securitising actor(s) can depart the stage but continue to 'feed' the securitisation by chanting from their seated position in the audience. Furthermore, this framework extended the agency of the audience. The original framework for securitisation theory (Buzan, Waever and Wilde, 1998) bestowed upon the audience the power to offer a relatively binary response to a proffered securitisation. The audience could either accept or reject the securitisation, but could not actively debate, deliberate, or invigorate further life upon the securitisation after they had agreed that a 'securitised' label was necessary and proportionate. This was a deficiency that masks the de facto operation of securitisations. For instance, in this mapping of the official British securitisation of the threat of cyberterrorism, a substantive offering from the corpus came from backbench MPs and Lords. It would not be appropriate to suggest that a Member of Parliament who is not part of her Majesty's Government, nor an influential member of a defence or security related committee, nor a member of the Privy Council, could be a bona fide participant in the securitisation process as a securitising actor. However, it is clear from the mapping and analysis that MPs could, and did, offer substantive contributions in which they stated their

belief that cyberterrorism represented a significant threat to the UK, and described characteristics of cyberterrorism. These contributions did more than simply affirm a binary 'yes, I agree to this securitisation'; indeed, these contributions could be said to have furthered the epistemology underpinning the British securitisation of cyberterrorism. Examining such audience contributions would be of utility for any threat, but it is particularly of interest in the case of cyberterrorism because this is a threat that has not occurred and is relatively loosely defined. Each contribution, or what I term 'securitising moment', that has been mapped in this thesis, is an attempt – whether by a securitising actor or a member of the audience – to ascribe a partial fixing to the discourse of cyberterrorism.

An additional contribution of the 'Pantomime' framework of securitisation was that it expanded the audience into a 'tiered' rather than monolithic entity. Membership of a particular tier infers a certain capacity for engagement with a given securitisation. In the case of the official British securitisation of cyberterrorism, the first tier of the audience – consisting of those who are capable of performing as securitising actors – had the greatest capacity to create and influence the securitisation of cyberterrorism. The second tier of the audience, representing MPs and Lords who were outside of the core of the formal Government, had less capacity to influence the securitisation of cyberterrorism; but, importantly, their capacity was greater than that of the third tier, which subsumed those who were outside of political office. Whilst this thesis conceptualised three tiers of the audience, it is possible that I could have created more tiers. As stated previously, tiers would differ depending on the securitisation in question and its context; the international securitisation of the Global War on Terrorism, for instance, would need to incorporate many more tiers. In addition, whilst this thesis dealt with tiers on a purely 'vertical' basis (where each tier had a differing capacity to influence the securitisation), a more in-depth framework could offer 'horizontal' tiers. For example, in the case of the Global War on Terrorism, the governments of France and Germany could be regarded as 'horizontal' tiers, as this would recognise their status as distinct governing entities, whilst acknowledging that they may 'speak' or 'perform' to different audience tiers, such as the French or German parliaments.

The audience was not limited to simply responding to the securitising actor; instead, the audience could enjoy 'securitising moments' amongst themselves, either within their own tier, to a specific alternate tier, or to all audience tiers. Whilst there was almost no consideration given to the 'third tier' in this thesis, it

is conceivable within this framework that the general public could write to their constituency representative on the matter of cyberterrorism, perhaps in the form of an open letter, because their capacity to influence their constituency MP may be greater than their ability to address the Government directly.

The next section outlines some of the limitations of the thesis and the research approach that I have applied.

Limitations of the Thesis

There are a number of limitations regarding this thesis and its research approach that should be acknowledged. By default, analysing discourse through a securitisation-oriented lens imparts a superficiality onto the research findings. The corpus from which the 110 unique sources were sourced is probably only a small snapshot of the overall discussions and deliberations regarding the threat of cyberterrorism that were held at an official level within British political discourse. For instance, the 2010 *Strategic and Review* documents, which seminally classified cyberterrorism as a Tier One threat to the UK, would not have appeared out of thin air. There will have been discussions between Ministers, members of the intelligence services, and representatives from the private sector in discussions on the matter of cyber security, which will have informed the decision to place cyberterrorism as a Tier One threat. Many of these discussions will be absent from public record, and they are therefore out of reach for the securitisation analyst. As has been stated previously, this thesis mapped and analysed the public-facing 'securitising moments', because A) there was sufficient public-facing discursive sources to form a relevant corpus and B) securitising discourse that can reach all audience tiers must, in essence, be unclassified, legal to possess and readily available. I have outlined the means by which I acquired sources in the third chapter, and anyone with an internet connection which can access the gov.uk and Hansard websites would be able to replicate my searches. An analyst's reliance on public-facing documentation and discourse is a necessity in the case of a public-facing securitisation, but it is an important dependency to note. I do not claim that this thesis is a fully comprehensive overview of the construction of the securitisation of cyberterrorism, although I hope that it has provided a reasonable and warranted snapshot.

Some of the context surrounding the 'securitising moments' could have been substantiated by contacting or interviewing those who engaged with the cyberterrorism discourse. However, given the word-count constraint of the thesis, it would have been challenging to incorporate a bona fide analysis of such responses and/or interviews. Furthermore, as respondents would have partaken on a voluntary basis, it would not have been guaranteed that I would have received a sufficient quantity of responses to justify this endeavour.

As has been noted, the 'public' represented the third tier of the conceptualised audience. Notwithstanding this, the public were essentially ignored by this thesis. It was recognised in the fourth chapter that this is partly down to the lack of cyberterrorism-centric polling and surveying to-date. I could have conducted surveys of my own, however, again, as this would have been on a voluntary and non-incentivised basis, I could not have guaranteed a high quantity (or quality) of returns.

The 12th May 2010 date from which sources were collected missed some elements of the discourse that would have helped to inform the discursive construction of the threat of cyberterrorism and the rationale for the Cabinet Office's decision to declare it a Tier One threat in 2010. For example, as was noted in the fourth chapter, the 2009-2010 Annual Report of the Intelligence and Security Committee noted that:

> "GCHQ informed the Committee that it is not known whether terrorist groups intend, or have the capacity, to launch significant attacks over the internet but this, along with extremist use of the internet, remains an area of considerable concern. Nevertheless, we have been told by GCHQ that the greatest threat of electronic attack to the UK comes from State Actors, with Russia and China continuing to pose the greatest threat" (Intelligence and Security Committee, 2010:22).

As a consequence, this thesis could be said to miss the deliberations that led to the formation of the securitisation of the threat of cyberterrorism to the UK, instead leaping straight to the core 'securitising moments' which established the securitisation in official British discourse. It is, nevertheless, interesting that the securitisation of cyberterrorism was established by the Cabinet Office after GCHQ had informed the Intelligence and Security Committee that as far as the intelligence service was concerned, there was no substantive evidence that terrorists were particularly eager to develop, or capable of developing, cyber weapons which could endanger British security. In this regard, the establishment of the securitisation of cyberterrorism could again be said to befit the 'anticipatory' model of security provision.

Another self-imposed limitation of this thesis was my restricting the definition of cyberterrorism to how the discourse itself defined it. Predominantly, cyberterrorism could be read as referring to use of cyber weapons, by terrorists, to damage critical computer systems. The corpus was based on sources that resulted from hits related to cyberterrorism, and sources were used irrespective of how the person in question decided to frame cyberterrorism. However, I could have loosened the constraints of 'cyberterrorism' and added, for instance, 'Electromagnetic Pulse' and 'EMP' to my search queries. This would have increased the number of overall hits, although perhaps not by a great deal. Searching for 'Electromagnetic Pulse' on Hansard under the thesis's timeline parameters returns six hits (Parliament.uk, 2017). By discussing Madeleine Moon's (2014) account of her reading of *One Second After*, I had already indirectly discussed the way in which the British cyberterrorism discourse had been influenced by a fictionalised account of the use of a pervasive EMP. The House of Commons Defence Committee's tenth report of the 2010-2012 session, entitled *Developing Threats: Electro-Magnetic Pulses* is an example of the discourse that was missed, in my intentional avoidance of including hits for 'EMP' when I created the corpus. Some of the contributions made in this report draw on the USA's EMP Commission, which raised concern about the kind of EMP attack upon which *One Second After* is based; the detonation of a thermonuclear warhead in the atmosphere above a state (House of Commons Defence Committee, 2012a). Intriguingly, whilst the Committee's report included references to the potential terrorist application of EMP devices, the Government's response to this report did not (House of Commons Defence Committee, 2012b). However, in defence of my adherence to hits based on 'cyberterror', 'cyberterrorism', 'cyberterrorist' and variations thereof, the express interest of this thesis was to analyse the securitisation of cyberterrorism *however the discourse defined it*. Other than Madeleine Moon's contribution, no other hits from the corpus actively or indirectly linked EMP-related means of attack to cyberterrorism. If I had expressly searched for 'EMP' and had included this in my corpus, I would have been imposing a particular interpretation of cyberterrorism onto the discourse. This would have run counter to my 'interpretive' aims.

The next section considers future novel avenues for research that, having completed this thesis, I would suggest should be a priority in the short-to-medium term. Some future avenues for research were raised in the 'Physical versus Cyber' section of Chapter Five and the 'From Fiction to Reality' section of Chapter Six, but given that transhumanism remains on the horizon and virtual reality portrayals of fictional

narratives are still in their seminal phase, these calls for research may be early. However, the following avenues for research could be accommodated in the immediate present.

Future Avenues for Research

This thesis highlights several under-developed fields that beckon further research, relating to either cyberterrorism, cyber security and/or securitisation theory. These under-developed fields are considered here.

Whilst this thesis has examined the construction of the threat of cyberterrorism in the UK, the British experience does not necessarily correlate with other states that have also securitised this threat. Studies that map and analyse the construction of the threat of cyberterrorism elsewhere (or that perhaps highlight the absence of this securitisation) would be novel. Further studies could also offer comparisons between the British experience and the securitisations exhibited by other states, for instance the USA.

Cyberterrorism remains an incipient field of research, not only for Security Studies, but also for Psychology, Sociology and Criminology. Broadly, there is a need to apply psychological studies to the way in which catastrophic cyber threat influences human perceptions of threat and human decision-making. This research could include, but need not be singular to, the anticipated threat of cyberterrorism. It would be useful – particularly from a policy and public awareness standpoint – to know whether threats of cyberterrorism provoke a greater or weaker perception of insecurity vis-a-vis conventional terror.

Chapter Four noted that notwithstanding the excellent Cyberterrorism Project survey (MacDonald et al, 2013) there is, at present, a lack of suitable surveys that have expressly considered the threat of cyberterrorism, or at least included this threat in a box-ticking exercise in which respondents are able to rank the threats that they believe to be the greatest risk. Considering that cyberterrorism has been categorised as a Tier One threat to the UK, it is perhaps surprising that pollsters have not been commissioned to undertake surveys of the British public on this issue. Granted, a securitisation does not by default need to heed democratic agreement on the prioritisation of threat; at its core, a securitisation involves the removal of a threat from a ‘politicised’ status and the placement of it in an exceptionalised ‘security’ realm. The public could wholeheartedly disagree with the notion that cyberterrorism should be securitised, but the foundation of the official securitisation of cyberterrorism would remain. That being said, it would be useful, again from

a policy and public awareness standpoint to know: whether the British public agree with this securitisation; whether they are more concerned about the cyber threat posed by other nation states; whether they agree with the development of the British state's cyber arsenal, and whether they believe cyberterrorism will become an increasing risk over time relative to conventional forms of terror.

As has been suggested previously, Swansea University's Cyberterrorism Project and Oxford University's Global Cyber Security Capacity Centre could both be excellent launchpads for such research, but research need not be exclusive to these bodies. Given the UK's exceptional reliance on internet infrastructure and internet-mediated communication for the functioning of its economy (Dean et al, 2012:9), in addition to the UK's role in the development of techniques for cyber offence and cyber surveillance, it would seem apt that British institutions should be taking a lead on tracing public awareness and knowledge of cyber threat. As the latest *Cyber Security Strategy* notes, "offensive cyber forms part of the full spectrum of capabilities we will develop to deter adversaries and to deny them opportunities to attack us, in both cyberspace and the physical sphere. Through our National Offensive Cyber Programme, we have a dedicated capability to act in cyberspace and we will commit the resources to develop and improve this capability" (Cabinet Office, 2016:51). Further research in this area would build on our understanding of the 'legitimate' and 'illegitimate' forms of cyber violence and cyber being.

In general, there is a need to scrutinise discourses justifying the developing and acquisition of cyber weapons by not only non-state actors but also states themselves, particularly at a time when there is no 'Geneva Convention' on cyber weapons. Normatively, it would be best if a cyber Hiroshima or Nagasaki could be avoided. Some of the sources in the corpus may have drawn similarities between cyber and nuclear weapons (Patten, 2010; Hannay, 2010), but there are also marked divergences between cyber and other non-conventional weapons which have direct interplay with weapon storage and application in practice. Nuclear weapons, regulated and monitored by the IAEA, are difficult to transport, maintain, sell, buy, and steal, let alone build. Nuclear material has an awkward tendency to leave a trace of its passage. In contrast, computer code is not restricted by the properties restricting the dissemination of nuclear weaponry. Code can be infinitely copied. Code can be transported across borders and, feasibly, can evade authorities even if they run a search on the device of a detainee. Code can be anonymously sold for a profit on darknet markets and inexpensively distributed around the planet at the speed of light. Code does not need to be transported to its

designated target in a dirty bomb, an aircraft or a ballistic missile; indeed, in some respects, code makes ICBMs appear as antiquated relics of the Cold War. Why would one use an environmentally-devastating nuclear weapon against an adversary's population when a cyber weapon could, if only temporarily, reduce their livelihoods to a pre-electronic age for a sufficient duration for them to run out of food and engage in systematic looting and manslaughter amongst themselves? Deterrence theory may be irrelevant with code which can be delivered through means that make precise attribution difficult. Code can be quietly introduced to a designated target through a malicious virus, either disseminated remotely or installed through a removable storage device. I stress this point not as an exercise in hyperbole, but because the development of code that is capable of destroying a state's banks and utilities is not risk-free.

The Stuxnet attack is the best example of nation states explicitly targeting another state's critical infrastructure, but this attack was only the tip of the iceberg of the capabilities of the USA's Cyber Command. Alex Gibney's *Zero Days* documentary revealed the existence of the 'Nitro Zeus' programme, which, whilst seemingly unused, had been developed to disable Iran's air defences, communications systems and national grid (Sanger and Mazzetti, 2016). The leaking of cyber weaponry has occurred before; in April 2017, 300mb of cyber exploits for Windows operating systems that had been developed by the NSA were released by the covert group The Shadow Brokers, who had been drip-feeding a cache of exploits for the preceding eight months (Goodin, 2017a; 2017b). If cyber weaponry capable of destroying a state's apparatus were to be leaked, a Godwin's Law-type process would ensure that its attempted use would be a matter of *when* rather than *if*. As was highlighted with the NHS ransomware[19] attack (Graham, 2017), a legacy attack may be outdated and impotent against many systems; but for the purposes of cost-reduction and a reluctance to retrain staff with new systems, individuals and organisations have a tenancy to operate outdated software and hardware. Even computer systems on the UK's newest £3.5bn aircraft carrier, the *Queen Elizabeth*, appeared – in images released from a tour of the ship – to have been installed with Windows XP (MacAskill, 2017b), an operating system that has not been supported with Microsoft security updates since 2014. Because the development of cyber weaponry is not a zero-sum process that guarantees British security – and

[19] Ransomware encrypts a computer's hard drive, without the user's permission. Typically, the private key, which is required to de-encrypt the hard drive, is only released to the victim if they pay the ransom. In the case of the May 2017 attack, which affected not only the NHS but around 300,000 computers operated by organisations internationally, the ransom demanded on each infected machine was roughly £230-worth of the pseudoanonymous cryptocurrency, Bitcoin.

indeed, could create risks of its own – there are important, public-facing conversations that are disconcertingly absent from our discourse.

In terms of further research beckoned by the contribution-to-theory that has been offered by this thesis, scholars could apply the 'Pantomime' framework to other cases of securitisation. It would be of great interest to see an in-depth mapping of the way in which vertical and horizontal audiences have interacted with one another in a particular securitisation. As securitisation is predominantly a speech-act based theory, this framework relies first and foremost on qualitative data; however, the Pantomime framework could also serve quantitative purposes. For instance, it could be ascertained from the weight of interaction between two particular audience tiers that that particular route of interactivity had the greatest impetus in the cementing of a securitisation, or perhaps in the snowballing of a process of counter-securitisation. Such research could have policy relevance. For instance, if the interactive pathway between two particular audience tiers could be said to have a significant influence over the nature of a securitisation, certain policies or communicative spaces could be proposed to further facilitate that discursive pathway, or to encourage the development of pathways to and between 'lagging' audience tiers. Securitisations need not be democratic processes, but their exclusivity can be mitigated and scholars should not be afraid of offering frameworks to normatively encourage the disruption of barriers-to-entry for discursive engagement.

Further research could also elaborate on more context-specific determinants of the dividing lines between audience tiers. In this thesis, I defined this through a simple comprehension of 'exclusivity'. This inter-subjectivity of this choice was partially arrested because I selected so few audience tiers, and because there were distinct professional distinctions between each tier: a) the Cabinet Office, b) backbench MPs and Peers, and c) the general public. However, professional roles are not the only means by which to ascribe exclusivity to agency. Exclusivity could, for instance, also be influenced by one's private income, one's education, or one's particular vulnerability to, or positioning within, a security threat. For instance, in the case of cyber threat, Gavin Patterson, the Chief Executive Officer of British Telecommunications might have a greater influence over a securitisation than Anthony Bamford, Chairman of JCB, because of the positioning of BT in the UK's internet communication infrastructure. Similarly, the Chief Executive of an at-risk organisation such as National Grid Plc could also be said to have a privileged exclusive position within the securitisation of a cyber threat to the UK. Whilst this thesis did not incorporate the voice of the private sector

in the so-termed 'official' securitisation of cyberterrorism, this was for the purposes of brevity rather than because the private sector was deemed irrelevant. A framework that incorporates audience tiers for the private sector would need to find alternative means by which to ascribe and quantify 'exclusivity'.

This author agrees with the notion that a securitisation *creates* its audience(s), rather than the audience existing as an a priori entity. Different securitisations could create entirely different audience tiers. However, it is possible that a securitisation analyst could juxtapose two securitisations against one another. Whilst this thesis has identified some correlations between the securitisation of cyberterrorism and the securitisation of post-9/11 terrorism more broadly, it is possible that the securitisation of cyberterrorism could have been influenced by a wider range of securitisations. Such influence could be observed by examining the exchanges between the audience tiers of one securitisation with the audience tiers of another.

The next section offers some final remarks.

Final Remarks

It has been stated throughout this thesis – perhaps to the point of cliché – that cyberterrorism is a socially-constructed threat to the UK that does not, at the time of writing, have any true historical precedent. It is not my place to speculate whether the Cabinet Office's decision in 2010 to position cyberterrorism as Tier One threat will be proven foretelling or overly precautionary either in a five year, ten year, or fifty year timespan. This thesis has sought simply to map and analyse the strands of the official British securitisation of cyberterrorism, rather than pass judgement upon it.

In his book, *Hacking the Hacker*, Roger Grimes states that:

> "if we do an intellectual comparison alone, the defenders on average are smarter than the attackers. A defender has to know everything a malicious hacker does plus how to stop the attack. And that defence won't work unless it has almost no end-user involvement, works silently behind the scenes, and works perfectly (or almost perfectly) all the time. Show me a malicious hacker with a particular technique, and I'll show you more defenders that are smarter and better" (2017:12.2/524).

In the case of the terrorist application of cyber weapons against critical computer systems, even a layman can propose that the odds are not stacked in the terrorist's favour. Terrorist organisations come and go: causes encouraging a group's existence can dissipate; senior membership can be incarcerated; or they

may lose the support of their key constituencies. States, in contrast, exist for centuries. Surveying their pieces on the chess-board of the strategic application of violence, a state can sit and watch the clock whilst terrorist entities sweat. Cyber weapons may be exceptional in several respects, as has been argued in this thesis, but they take time to develop and there is no guarantee that they will work as intended. If individuals want to guarantee that their faces – and their causes – are on the front pages of tomorrow's newspapers, there are more sure ways of achieving this than sitting in front of a computer terminal, writing code with a steady flow of Red Bull and coffee.

This is not to advocate complacency, however. Some catastrophic exploits may be sought intentionally for months or years, but others can be stumbled upon by accident. Here, the story of Dan Kaminsky is instructive.

You probably use the Domain Name System (DNS) every day. The DNS is a network service that translates convoluted, difficult-to-remember IP addresses to the familiar domain names that you know; for instance, yahoo.com and bbc.co.uk. In 2008, Dan Kaminsky pondered an exploit that he had used previously to access free wifi in a Starbucks branch. This exploit, he realised, was more powerful than simply being a means of bypassing the Starbucks webpage to pay for wifi usage. As Alexander Klimburg writes:

> "what Kaminsky discovered was that under certain conditions, if you provided the DNS server with the location of a fake page in someone else's domain, the DNS server would start trusting you about other pages in that same domain, regardless of who you were and whether you were affiliated with the owner of the domain at all. He could basically send all traffic from any web site anywhere in the world to himself. And, even worse, his realisation wasn't merely theoretical; it actually worked when he tried it. This meant he could effectively impersonate any web site in the world – from Bank of America to the Department of Defence – and therefore steal the log-in data of those trying to access their networks through the web site" (2017:156.6/893).

However, rather than become stupendously wealthy very quickly, Kaminsky telephoned Paul Vixie, one of the developers of the DNS, who agreed to find a solution to the problem, hastily summoning 16 of the world's DNS experts to quietly fix the bug before it became publicly-known (Zetter, 2008). A system with the subsequently-created patch would have a one in four-billion chance of being hacked, compared to a one in 65,536 chance for an unpatched system (Klimburg, 2017:158/893). Had Kaminsky been a 'blackhat'[20] hacker, however, the story could have been starkly different.

[20] The terms 'whitehat', 'blackhat' and 'greyhat' are often used to characterise computer hackers. Whitehat hackers hack for positive causes; particularly proficient whitehat hackers are hired by firms to intentionally target their

Cyberspace, as the fifth sphere of power projection, is perhaps unique in its democratisation of power. A lone individual cannot hope to compete with advanced states in military power projection on land, at sea, in the air or in space; but, equipped with a computer, under the right circumstances and with the requisite abilities, a malicious actor could cause a state entity genuine concern. Whether proscribed terrorist organisations adopt cyber arsenals and become ad-hoc or fully fledged cyberterrorists may only become apparent with the revelation of time.

systems so that the vulnerabilities can be patched. Blackhat hackers will hack for malicious intention or for profit irrespective of the consequences. Greyhat hackers may dabble with both positive and harmful forms of hacking.

Reference List

Aaviksoo, J. (2010) "Cyberattacks Against Estonia Raised Awareness of Cyberthreats", *Defence Against Terrorism Review*, Vol.3, pp.13-22
Abbey, N. (2015) "Straight outta Tatton: it's Easy to See why George Osborne is a Fan of Gangsta Rap", *Guardian*, 5 October, https://www.theguardian.com/commentisfree/2015/oct/05/george-osborne-gangsta-rap-nwa-public-enemy, accessed on 3 May 2017
Abraham, T. (2011) "The Chronicle of a Disease Foretold: Pandemic H1N1 and the Construction of Global Health Security Threat", *Political Studies*, Vol.59, pp.797-812
Adey, P. (2009) "Facing Airport Security: Affect, Biopolitics, and the Preemptive Securitisation of the Mobile Body", *Environment and Planning D: Society and Space*, Vol.27, pp.274-295
Ahmad, R and Z Yunos. (2012) "A Dynamic Cyber Terrorism Framework", *International Journal of Computer Science and Information Security*, Vol.10 No.2, pp.149-158
Ahmad, T. (2015) "Aviation Security in an Increasingly Complex Environment", *Gov.uk*, 21 October, https://www.gov.uk/government/speeches/aviation-security-in-an-increasingly-complex-environment, accessed on 6 April 2017
Ahmed, S. (2004) *The Cultural Politics of Emotion*, Edinburgh: Edinburgh University Press
Alderdice, J. (2011a) *Hansard Volume 733*, 12 December, Intelligence and Security Committee Annual Report, https://hansard.parliament.uk/Lords/2011-12-12/debates/11121228000135/IntelligenceAndSecurityCommitteeAnnualReportFor2010-11?highlight=cyber%20terrorism#contribution-11121233000018, accessed on 15th March 2017
Alderdice, J. (2011b) *Hansard Volume 725*, 10 February, NATO, https://hansard.parliament.uk/Lords/2011-02-10/debates/11021054000682/NATO?highlight=cyber%20terrorists, accessed on 29 March 2017
Alderdice, J. (2011c) *Hansard Volume 733*, 5 December, Digital Technology, https://hansard.parliament.uk/Lords/2011-12-05/debates/11120535000230/DigitalTechnology?highlight=cyber%20terrorism#contribution-11120535000040, accessed on 11 April 2017
Alderdice, J. (2013) *Hansard Volume 745*, 15 May, Queen's Speech, https://hansard.parliament.uk/Lords/2013-05-15/debates/13051539000301/Queen%E2%80%99SSpeech?highlight=cyberterrorism#contribution-13051546000018, accessed on 10 April 2017
Alderdice, J. (2015) *Hansard Volume 762*, 28 May, Queen's Speech, https://hansard.parliament.uk/Lords/2015-05-28/debates/15052829000452/Queen%E2%80%99SSpeech?highlight=cyber%20terrorism#contribution-15052829000188, accessed on 12 April 2017
Altheide, D. (2010) "Fear and Terrorism and Popular Culture", pp.11-22 in ed. J Birkenstein, A Froula and K Randell, *Reframing 9/11: Film, Popular Culture and the War on Terror*, New York: Continuum Publishing
Amoore, L and A Hall. (2009) "Taking People Apart: Digitised Dissection and the Body at the Border", *Environment and Planning D: Society and Space*, Vol.27 No.3, pp.444-464
Anderson, B. (2007a) "Hope for Nanotechnology: Anticipatory Knowledge and Governance of Affect", *Area*, Vol.39, pp.156-165
Anderson, B. (2007b) "Affect and the War on Terror", paper presented at the Association of American Geographers Annual Meeting, San Francisco
Anderson, B. (2010) "Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies", *Progress in Human Geography*, Vol.34, pp.777-798
Anderson, J. (2010) *Hansard Volume 721*, 14 October, Cyberattacks: EU Committee Report, https://hansard.parliament.uk/Lords/2010-10-14/debates/10101424000811/CyberattacksEUCommitteeReport?highlight=cyberterrorism#contribution-10101424000554, accessed on 10 April 2017
Andersen, R and F Moller. (2013) "Engaging the Limits of Visibility: Photography, Security and Surveillance", *Security Dialogue*, Vol.44 No.3, pp.203-221
Aradau, C. (2010) "Derrida: Aporias of Otherness", pp.107-118 in ed. C Moore and C Farrands, *International Relations Theory and Philosophy: Interpretive Dialogues*, Abingdon: Routledge
Aradau, C and R Munster. (2007) "Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future", *European Journal of International Relations*, Vol.13 No.1, pp.89-115

Aradau, C and R Munster. (2012) “The Time/Space of Preparedness: Anticipating the ‘Next Terrorist Attack’”, *Space and Culture*, Vol.15 No.2, pp.98-109
Archive.org. (2014) “The Lone Gunmen”, *TV Tango*, https://web.archive.org/web/20140711003100/http://tvtango.com/series/lone_gunmen/episodes, accessed on 16 August 2017
Archive.org. (2015) “ISIS Tor Guide”, 4 October, https://archive.org/details/ISIL-tor-guide, accessed on 9 August 2017
Arquilla, J and D Ronfeldt. (2001) “The Advent of Netwar”, pp.1-25 in ed. J Arquilla and D Ronfeldt, *Networks and Netwars*, Santa Monica: RAND Corporation
Ashley, R and R Walker. (1990) “Reading Dissidence/Writing the Discipline: Crisis and the Question of Sovereignty in International Studies”, *International Studies Quarterly*, Vol.34 No.3, pp.367-416
Assange, J. (2012) “Transcript: Interview with Julian Assange in the Ecuadorian Embassy”, *Wikileaks etc*, http://wikileaksetc.blogspot.co.uk/2012/09/transcript-interview-with-julian.html, accessed on 3 August 2017
Aust, C and D Zillmann. (1996) “Effects of Victim Exemplification in Television News on Viewer Perception on Social Issues”, *Journalism and Mass Communication Quarterly*, Vol.73 No.4, pp.787-803
Avert. (2017) “HIV and Aids in the United Kingdom”, https://www.avert.org/professionals/hiv-around-world/western-central-europe-north-america/uk, accessed on 3 August 2017
Axelrod, R and R Iliev. (2014) “Timing of Cyber Conflict”, *Proceedings of the National Academy of Sciences*, Vol.111 No.4, pp.1298-1303
Bad Religion. (2000) *I Love My Computer*, Los Angeles: Epitaph Records
Bainbridge, W. (2010) *The Warcraft Civilisation: Social Science in a Virtual World*, Cambridge MA: MIT Press
Baker-Beall, C. (2016) *The European Union’s ‘Fight Against Terrorism’: Discourse, Policies, Identity*, Manchester: Manchester University Press
Bakhtin, M. (1981) *The Dialogic Imagination: Four Essays*, Austin: University of Texas Press
Ball, J. (2015) “Cameron Wants to Ban Encryption – He can Say Goodbye to Digital Britain”, *The Guardian*, 13 January, https://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror, accessed on 10 November 2017
Ball, J, B Schneier and G Greenwald. (2013) “NSA and GCHQ Target Tor Network that Protects Anonymity of Web Users”, *The Guardian*, 4 October, http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption, accessed on 5 January 2016
Balzacq, T. (2004) “The Pragmatic Act of Security: Politics and Methods”, unpublished manuscript.
Balzacq, T. (2005) “The Three Faces of Securitisation: Political Agency, Audience and Context”, *European Journal of International Relations*, Vol.11 No.2, pp.171-201
Balzacq, T, S Léonard and J Ruzicka. (2016) “'Securitisation' Revisited: Theory and Cases”, *International Relations*, Vol.30 No.4, pp.494-531
Banta, B. (2012) “Analysing Discourse as a Causal Mechanism”, *European Journal of International Relations*, Vol.19 No.2, pp.379-402
Barker, D and M Barker. (2013) *Internet Research Illustrated*, Independence: Cengage Learning
Barthes, R. (1977a) “The Rhetoric of the Image”, pp.32-51 in ed. S Heath, *Image-Music-Text*, London: Fontana
Barthes, R. [1977b] (1993) “Inaugural Lecture, College de France”, pp.457-478 in ed. S Sontag, *A Roland Barthes Reader*, London: Vintage
Bartlett, J and A Krasodomski-Jones. (2015) *Online Anonymity: Islamic State and Surveillance*, London: Demos March
Bataille, G. (1985) “The Deviations of Nature”, pp,53-56 in ed. A Stoekl, *Visions of Excess: Selected Writings 1927-1939*, Minneapolis: University of Minnesota Press
Bayley, H. (2013) *Hansard Volume 565*, 4 July, NATO, https://hansard.parliament.uk/Commons/2013-07-04/debates/13070444000001/NATO?highlight=cyber%20terrorism#contribution-13070444000565, accessed on 11 April 2017
Bazin, A. (1972) *What is Cinema?*, Vol.2, Berkeley: University of California Press
BBC News. (2014a) “Hack Attack Causes ‘Massive Damage’ at Steel Works”, 22 December, http://www.bbc.co.uk/news/technology-30575104, accessed on 20 July 2015
BBC News. (2014b) “Google and Facebook can be Legally Intercepted, says UK Spy Boss”, 17 June, http://www.bbc.co.uk/news/technology-27887639, accessed on 20 July 2015

BBC News. (2015). “CCTV: Too Many Cameras Useless, Warns Surveillance Watchdog Tony Porter”, 26 January, http://www.bbc.co.uk/news/uk-30978995, accessed on 10 February 2016
BBC News. (2016) “Met Police to get 600 More Armed Police to Boost Terror Response”, 14 January, http://www.bbc.co.uk/news/uk-35308467, accessed on 22 February 2016
Bean, P. (2010) *Legalising Drugs: Debate and Dilemmas*, Bristol: Policy Press
Beck, U. (1992) *Risk Society: Towards a New Modernity*, London: Sage
Beckford, M. (2011) “Nanotechnology Hope for Antibiotics”, *The Telegraph*, 4 April, https://www.telegraph.co.uk/news/health/news/8425009/Nanotechnology-hope-for-antibiotics.html, accessed on 11 April 2018
Beer, F and C De Landtsheer. (2004) “Metaphors, Politics and World Politics”, pp.5-52 in ed. F Beer and C De Landtsheer, *Metaphorical World Politics: Rhetorics of Democracy, War and Globalisation*, East Lansing: Michigan State University Press
Beith, A. (2010) *Hansard Volume 517*, 28 October, The Internet and Privacy, https://hansard.parliament.uk/Commons/2010-10-28/debates/10102828000001/TheInternetAndPrivacy?highlight=cyber%20terrorism#contribution-10102828000080, accessed on 21 June 2018
Bendrath, R. (2001) “The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection”, *Information and Security: An International Journal*, Vol.7, pp.80-103
Bendrath, R. (2003) “The American Cyber-angst and the Real World- Any Link?”, pp.49-73 in ed. R Latham, *Bombs and Bandwidth: The Emerging Relationship Between IT and Security*, New York: The New Press
Berger, L. (2013) *Hansard Volume 567*, 10 September, Climate Change Act, https://hansard.parliament.uk/Commons/2013-09-10/debates/13091045000001/ClimateChangeAct?highlight=cyber%20terrorism#contribution-13091045000144, accessed on 11 April 2017
Bergman, M. (2001) “White Paper: The Deep Web: Surfacing Hidden Value”, *Taking License*, Vol.7 No.1, available at: http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main, accessed on 9 August 2017
Berner, S. (2003) “Cyber-Terrorism: Reality or Paranoia?”, *South African Journal of Information Management*, Vol.5 No.1, pp.1-4
Berry, T and A Fournier. (2014) “Examining University Students' Sneezing and Coughing Etiquette”, *American Journal of Infection Control*, Vol.42 No.12, pp.1317-1318
Berton, B. (2015) *The Dark Side of the Web: ISIL’s One-Stop Shop?*, Paris: European Union Institute for Security Studies
Bertram, E, M Blachman, K Sharpe and P Andreas. (1996) *Drug War Politics*, Berkeley: University of California Press
Bessiere, K, F Seay and S Kiesler. (2007) “The Ideal Elf: Identity Exploration in World of Warcraft”, *Cyberpsychology and Behaviour*, Vol.10 No.4, pp.530-535
Bevir, M and R Rhodes. (2004) “Interpretation as Method, Explanation and Critique: A Reply”, pp.156-161 in The Interpretive Approach in Political Science: A Symposium, *British Journal of Politics and International Relations*, Vol.6, pp.129-164
Bevir, M and R Rhodes. (2005) “Interpretation and its Others”, *Australian Journal of Political Science*, Vol.40 No.2, pp.169-187
Bevir, M, O Dadddow and I Hall. (2013) “Introduction: Interpreting British Foreign Policy”, *The British Journal of Politics and International Relations*, Vol.15 No.2, pp.163-174
Bialasiewicz, L, D Campbell, S Elden, S Graham, A Jeffrey and A Williams. (2007) “Performing Security: The Imaginative Geographies of Current US Strategy”, *Political Geography*, Vol.26, pp.405-422
Biddle, P, P England, M Peinado and B Willman. (2002) “The Darknet and the Future of Content Distribution”, ACM Workshop on Digital Rights Management, 18 November, https://crypto.stanford.edu/DRM2002/prog.html, accessed on 9 August 2017
Bigo, D. (2004) “Identifier, Categoriser et Controller: Police et Logiques Proactives”, pp.56-88 in ed. L Bonelli and G Sainati, *La Machine à Punir: Pratiques et Discourse Securitaires*, Paris: L'Esprit Frappeur
Bigo, D. (2006) “Globalised (in)Security: The Field and the Ban-Opticon”, pp.10-48 in ed. D Bigo and A Tsoukala, *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*, New York: Routledge

Bigo, D. (2014) "The (in)Securitisation Practices of the Three Universes of EU Border Control: Military/Navy – Border Guards/Police – Database Analysts", *Security Dialogue*, Vol.45 No.3, pp.209-225
Bingham, N, S Holloway and G Valentine. (1999) "Where do you Want to go Tomorrow? The Connection and Organisation of Children and the Internet", *Environment and Planning D: Society and Space*, Vol.17, pp.655-672
Blair, T. (2001a) "Full Text: Tony Blair's speech (part one)", Labour Conference, *The Guardian*, 2 October, https://www.theguardian.com/politics/2001/oct/02/labourconference.labour6, accessed on 9 August 2017
Blair, T. (2001b) "Full Text of Tony Blair's Speech to Parliament", *The Guardian*, 4 October, https://www.theguardian.com/world/2001/oct/04/september11.usa3, accessed on 9 August 2017
Blair, T. (2005) "Full Text: Blair Speech on Terror", *BBC News*, 16 July, http://news.bbc.co.uk/1/hi/uk/4689363.stm, accessed on 9 November 2017
Blakeley, R. (2007) "Bringing the State Back into Terrorism Studies", *European Political Science*, Vol.6 No.3, pp.228-235
Bleed, R. (2005) *Visual Literacy in Higher Education*, Stanford: ELI Explorations
Bleiker, R and M Chou. (2010) "Nietzsche's Style: on Language, Knowledge and Power in International Relations", pp.8-19 in ed. C Moore and C Farrands, *International Relations Theory and Philosophy: Interpretive Dialogues*, Abingdon: Routledge
Blum, A. (2012) *Tubes: Behind the Scenes at the Internet*, London: Penguin
Blunkett, D. (2011) *Hansard Volume 537*, 5 December 2011, UK Extradition Arrangements, https://hansard.parliament.uk/Commons/2011-12-05/debates/11120526000001/UKExtraditionArrangements?highlight=cyber%20terrorism, accessed on 3 April 2017
Blunkett, D. (2015) interview with A Pearson. "UK not Ready for Cyber Attacks – Blunkett", *Yorkshire Post*, 4 April, http://www.yorkshirepost.co.uk/news/uk-not-ready-for-cyber-terror-attacks-blunkett-1-7192952, accessed on 3 April 2017
Booth, K. (1991) "Security and Emancipation", *Review of International Studies*, Vol.17 No.4, pp.313-326
Booth, K. (1994) "Security and Self Reflections of a Fallen Realist", YCISS Occasional Paper Number 26, October, prepared for presentation at the conference *Strategies in Conflict Critical Approaches to Security Studies*, Centre for International and Strategic Studies, York University, Toronto 12-14 May 1994
Booth, K. (2005) "Beyond Critical Security Studies", pp.259-278 in ed. K Booth, *Critical Security Studies and World Politics*, Boulder: Lynne Rienner
Borger, J, A Luhn and R Norton-Taylor. (2014) "EU Announces Further Sanctions on Russia After Downing of MH17", *The Guardian*, 22 July, https://www.theguardian.com/world/2014/jul/22/eu-plans-further-sanctions-russia-putin-mh17, accessed on 2 August 2017
Bos, R and R Kaulingfreks. (2002) "Life Between Faces", *Ephemera: Critical Dialogues on Organization*, Vol.2 No.1, pp.6-27
Bowcott, O. (2016) "Terrorism Act Incompatible with Human Rights, Court Rules in David Miranda Case", *The Guardian*, 19 January, http://www.theguardian.com/world/2016/jan/19/terrorism-act-incompatible-with-human-rights-court-rules-in-david-miranda-case, accessed on 23 January 2016
Brand, S. (1987) *The Media Lab: Inventing the Future at MIT*, New York: Viking
Brazier, J. (2010) *Hansard Volume 517*, 1 November, European Council, https://hansard.parliament.uk/Commons/2010-11-01/debates/1011019000001/EuropeanCouncil?highlight=cyber%20terrorism#contribution-1011019000303, accessed on 11 April 2017
Brill, A. (2010) "From Hit and Run to Invade and Stay: How Cyberterrorists Could be Living Inside Your Systems", *Defence Against Terrorism Review*, Vol.3 No.2, pp.23-36
Brinn, D. (2005) "Israeli Airport Technology Detects Intent of Terrorists", *Israel21c*, 8 May, https://www.israel21c.org/israeli-airport-technology-detects-intent-of-terrorists/, accessed on 18 August 2017
British Science Association. (2016) "One in Three Believe that the Rise of Artificial Intelligence is a Threat to Humanity", http://www.britishscienceassociation.org/news/rise-of-artificial-intelligence-is-a-threat-to-humanity, accessed on 18 March 2016
Brokenshire, J. (2012) "Securing Asia Conference on 27 June 2012: James Brokenshire Speech", *Gov.uk*, 27 June, https://www.gov.uk/government/news/securing-asia-conference-on-27-june-2012-james-brokenshire-speech, accessed on 21 March 2017

Brokenshire, J. (2013) “Keynote Speech for the Internet Service Providers’ Association Annual Conference”, *Gov.uk*, 27 November, https://www.gov.uk/government/speeches/keynote-speech-for-the-internet-service-providers-association-ispa-annual-conference, accessed on 21 March 2017
Brown, G. (2009) “Gordon Brown’s Speech to Congress: The Full Text”, *The Telegraph*, 4 March, http://www.telegraph.co.uk/news/politics/gordon-brown/4938252/Gordon-Browns-speech-to-Congress-the-full-text.html, accessed on 8 May 2017
Brown, M. (2013) “Skyfall Highest Grossing Film of all Time at UK Box Office”, *The Guardian*, 23 July, https://www.theguardian.com/film/2013/jul/23/skyfall-highest-grossing-film-uk-box-office, accessed on 24 April 2017
Brown, R. (2012) *Hansard Volume 554*, 29 November, Scotland and the Union, https://hansard.parliament.uk/Commons/2012-11-29/debates/12112958000001/ScotlandAndTheUnion?highlight=cyber%20terrorism#contribution-12112958000653, accessed on 11 April 2017
Browne, D. (2013) *Hansard Volume 742*, 24 January, Nuclear Disarmament, https://hansard.parliament.uk/Lords/2013-01-24/debates/13012450000874/NuclearDisarmament?highlight=cyber%20terrorism#contribution-13012450000244, accessed on 11 April 2017
Browning, C and M McDonald. (2011) “The Future of Critical Security Studies: Ethics and the Politics of Security”, *European Journal of International Relations*, Vol.19 No.2, pp.235-255
Brzoska, M and A Oels. (2011) “'Versicherheitlichung' des Klimawandels?” ['Securitisation of climate change?], pp.51-66 in ed. *Klimawandel und Konflikte*, [Climate change and conflict], Baden-Baden: Nomos
BSI [Federal Office for Information Security]. (2014) *The Management of IT Security in Germany 2014*, Bonn: BSI
Burke, A. (2002) “Aporias of Security”, *Alternatives*, Vol.27, pp.1-28
Burnett, J and D Whyte. (2005) “Embedded Expertise and the New Terrorism”, *Journal for Crime, Conflict and the Media*, Vol.1 No.4, pp.1-18
Burnham, A. (2016) *Hansard Volume 606*, Police Funding, Crime and Community Safety, https://hansard.parliament.uk/Commons/2016-02-24/debates/16022449000003/PoliceFundingCrimeAndCommunitySafety?highlight=cyber%20terrorism#contribution-16022449001330, accessed on 21 June 2018
Bush, G. (2001) “State of the Union Address”, *The Guardian*, 21 September, https://www.theguardian.com/world/2001/sep/21/september11.usa13, accessed on 9 August 2017
Buzan, B. (1997) “Rethinking Security after the Cold War”, *Cooperation and Conflict*, Vol.32 No.1, pp.5-28
Buzan, B, O Waever and J Wilde. (1998) *Security: A New Framework for Analysis*, London: Rienner
Buzan, B. (2010) interview with Foreign Affairs and International Trade Canada, available at http://blogs.lse.ac.uk/internationalrelations/2010/03/23/professor-barry-buzan-discusses-the-concept-of-security/, accessed on 12 November, 2015
Buzan, B and L Hansen. (2009) *The Evolution of International Security Studies*, Cambridge: Cambridge University Press
Buzan, B and O Waever. (2009) “Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory”, *Review of International Studies*, Vol.35, pp.253-276
Buzan, B, O Waever and J Wilde. (1998) *A New Framework for Analysis*, Boulder: Lynne Rienner
Cabinet Office. (2008) *The National Security Strategy of the United Kingdom: Security in an Interdependent World*, London: Cabinet Office
Cabinet Office. (2009) *The National Security Strategy of the United Kingdom: Update 2009, Security for the Next Generation*, London: Cabinet Office
Cabinet Office. (2010a) *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, London: Cabinet Office
Cabinet Office. (2010b) *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, London: Cabinet Office
Cabinet Office. (2011) *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, London: Cabinet Office
Cabinet Office. (2015a) *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, London: Cabinet Office.
Cabinet Office. (2015b) *2010 to 2015 Government Policy: Cyber Security*, London: Cabinet Office

Cabinet Office. (2016) *National Cyber Security Strategy 2016 to 2021*, London: Cabinet Office
Cabinet Office and Marsh. (2015) *UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk*, London: Marsh
Cameron, D. (2010) *Hansard Volume 517*, 1 November, European Council debate, https://hansard.parliament.uk/Commons/2010-11-01/debates/1011019000001/EuropeanCouncil?highlight=cyber%20terror#contribution-1011019000304, accessed on 10 April 2017
Cameron, D. (2011) "Prime Minister's Speech on Cyberspace", *Gov.uk*, 1st November, https://www.gov.uk/government/news/prime-ministers-speech-on-cyberspace, accessed on 15th March 2017
Cameron, D. (2014) "Huge Investment in Armed Forces Means a More Secure Future for Britain", *The Telegraph*, 14 July, http://www.telegraph.co.uk/news/uknews/defence/10965217/Huge-investment-in-Armed-Forces-means-a-more-secure-future-for-Britain.html, accessed on 3 April 2017
Cameron, D. (2015a) *Hansard Volume 602*, 23 November, National Security and Defence, https://hansard.parliament.uk/Commons/2015-11-23/debates/1511232000002/NationalSecurityAndDefence?highlight=cyber%20terrorism#contribution-1511232000196, accessed on 12 April 2017
Cameron, D. (2015b) *Hansard Volume 602*, 17 November, G20 and Paris Attacks, https://hansard.parliament.uk/Commons/2015-11-17/debates/15111751000004/G20AndParisAttacks?highlight=cyber%20terrorists, accessed on 27 July 2017
Cameron, D. (2015c) "Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference", *Obama White House*, 16 January, https://obamawhitehouse.archives.gov/the-press-office/2015/01/16/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint-, accessed on 24 April 2017
Cameron, D. (2015d) "Prime Minister's Statement on Paris Attacks and G20 Summit", *Gov.uk*, https://www.gov.uk/government/speeches/prime-ministers-statement-on-paris-attacks-and-g20-summit, accessed on 31 July 2017
Campbell, D. (1998a) *Writing Security: United States Foreign Policy and the Politics of Identity*, 2nd ed, Manchester: Manchester University Press
Campbell, D. (1998b) *National Deconstruction: Violence, Identity and Justice in Bosnia*, Minneapolis: University of Minnesota Press
Campbell, D. (2003) "Cultural Governance and Pictorial Resistance: Reflections on the Imaging of War", *Review of International Studies*, Vol.29, pp.57-73
Canar, B. (2011) "Deleuze and the Face", *Lingua ac Communitas*, Vol.21, pp.33-52
Cavelty, M. (2007) "Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate", *Journal of Information Technology and Politics*, Vol.4 No.1, pp.19-36
Cavelty, M and V Mauer. (2009) "Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence", *Security Dialogue*, Vol.40 No.2, pp.123-144
Cavelty, M, M Kaufmann and K Kristensen. (2015) "Resilience and (in)Security: Practices, Subjects, Temporalities", *Security Dialogue*, Vol.46 No.1, pp.3-14
Charlton, C. (2014) "Islamic State Jihadists Planning Encryption-protected 'Cyber Caliphate' so They can Carry out Hacking Attacks on West", *MailOnline*, 11 September, http://www.dailymail.co.uk/news/article-2751896/Islamic-State-jihadists-planning-encryption-protected-cyber-caliphate-carry-hacking-attacks-West.html, accessed on 8 August 2017
Charrett, C. (2009) *A Critical Application of Securitisation Theory: Overcoming the Normative Dilemma of Writing Security*, Catalan: International Catalan Institute for Peace
Charteris-Black, J. (2004) *Corpus Approaches to Critical Metaphor Analysis*, Basingstoke: Palgrave Macmillan
Chatterjee, P. (2005) "Sovereign Violence and the Domain of the Political", pp.82-100 in ed. T Hansen and F Stepputat, *Sovereign Bodies: Citizens, Migrants, and States in the Postcolonial World*, Princeton: Princeton University Press
Chau, C, P Kirwan, A Brown, N Gill and V Delpech. (2016) *HIV Diagnoses, Late Diagnoses and Numbers Accessing Treatment and Care*, 2016 Report, London: Public Health England
Chen, T, L Jarvis and S MacDonald. (2014) *Cyberterrorism and the News Media*, Cyberterrorism Project Research Report, No.3

Chesney, R. (2005) “The Sleeper Scenario: Terrorism-Support Laws and the Demands for Prevention”, *Harvard Journal on Legislation*, Vol.42 No.1, pp.1-89
Chesney, R. (2007) “Beyond Conspiracy? Anticipatory Prosecution and the Challenge of Unaffiliated Terrorism”, *Southern California Law Review*, Vol.80 No.3, pp.425-502
Chilton, P. (1999) *Security Metaphors: Cold War Discourse from Containment to Common House*, New York: Peter Lang
Chilton, P and G Lakoff. (1999) “Foreign Policy by Metaphor”, pp.37-59 in ed. C Schaffner and A Wenden, *Language and Peace*, Amsterdam: Harwood Academic Publishers
Chorley, M. (2015) “Web Firms Like Facebook and WhatsApp Must not be a ‘Safe Haven’ for Terrorists, Vows Cameron but Obama Warns of Need to Balance Security and Privacy”, *Mail Online*, 16 January, http://www.dailymail.co.uk/news/article-2913802/Web-firms-safe-haven-terrorists-vows-Cameron-Obama-warns-need-balance-security-privacy.html, accessed on 10 August 2017
Chulov, M and J Grierson. (2017) “British Jihadi Aine Davis Convicted in Turkey on Terror Charges”, *The Guardian*, 9 May, https://www.theguardian.com/world/2017/may/09/british-jihadist-aine-davis-convicted-in-turkey-on-terror-charges, accessed on 18 July 2017
Cilliers, J. (2003) “Terrorism and Africa”, *African Security Review*, Vol.12 No.4, pp.91-103
CISCO. (2016) “United Kingdom – 2020 Forecast Highlights”, *VNI Complete Forecast Highlights*, available at: http://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/United_Kingdom_2020_Forecast_Highlights.pdf, accessed on 28 July 2017
Claridge, D. (1996) “State Terrorism? Applying a Definitional Model”, *Terrorism and Political Violence*, Vol.8 No.3, pp.47-63
Coaffee, J, P O’Hare and M Hawkesworth. (2009) “The Invisibility of (in)Security: The Aesthetics of Planning Urban Defences Against Terrorism”, *Security Dialogue*, Vol.40, pp.489-511
Coates, S. (2016) “Lynton Crosby: Fear is the Key to Winning Brexit Votes”, *The Times*, 15 March, https://www.thetimes.co.uk/article/crosby-fear-is-is-key-to-winning-brexit-votes-9cxxw02gf, accessed on 10 April 2018
Collin, B. (1997) “The Future of Cyberterrorism: The Physical and Virtual Worlds Converge”, *Crime and Justice International*, pp.14-18
Collin, B. (2002) quoted in J Ballard, J Hornik and D McKenzie, “Technological Facilitation of Terrorism: Definitional, Legal and Policy Issues”, *American Behavioural Scientist*, Vol.45 No.6, pp.989-1016
Collier, S and A Lakoff. (2008) “Distributed Preparedness: The Spatial Logic of Domestic Security in the United States”, *Environment and Planning D: Society and Space*, Vol.26, pp.7-28
Connett, D, L Barber and A Griffin. (2015) “UK Government Rewrites Surveillance Law to Get Away with Hacking and Allow Cyber Attacks, Campaigners Claim”, *Independent*, 15 May, http://www.independent.co.uk/life-style/gadgets-and-tech/news/uk-government-rewrites-surveillance-law-to-get-away-with-hacking-and-allow-cyber-attacks-campaigners-10253485.html, accessed on 16 June 2016
Clegg, N. (2014) “Security and Privacy in the Internet Age”, 4 March, https://www.gov.uk/government/speeches/security-and-privacy-in-the-internet-age, accessed on 21 March 2017
Coaffee, J and P Fussey. (2015) “Constructing Resilience through Security and Surveillance: The Politics, Practices and Tensions of Security-Driven Resilience”, *Security Dialogue*, Vol.46 No.1, pp.86-105
Coaker, V. (2015) *Hansard Volume 597*, 2 July 2015, Britain and International Security, https://hansard.parliament.uk/Commons/2015-07-02/debates/15070233000001/BritainAndInternationalSecurity?highlight=cyber%20terrorist#contribution-15070238000011, accessed on 24 April 2017
Conway, M. (2002) “Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet”, *First Monday*, Vol.7 No.11, http://firstmonday.org/ojs/index.php/fm/article/view/1001/922, accessed on 22 March 2015
Conway, M. (2005) “The Media and Cyberterrorism: a Study in the Construction of ‘Reality’”, paper presented at the First International Conference on the Information Revolution and the Changing face of International Relations and Security, Lucerne, Switzerland, 23-25 May
Converse, P. (1964) “The Nature of Belief Systems”, pp.206-261 in ed. D Apter, *Ideology and Discontent*, New York: The Free Press
Cooley, C. (1902) *Human Nature and the Social Order*, New Brunswick NJ: Transaction
Corry, O. (2012) “Securitisation and 'Riskification': Second-order Security and the Politics of Climate Change”, *Millennium: Journal of International Studies*, Vol.40 No.2, pp.235-258

Coskun, B. (2012) "Words, Images, Enemies: Macro-Securitisation of the Islamic Terror, Popular TV Drama and the War on Terror", *Turkish Journal of Politics*, Vol.3 No.1, pp.37-51
Côte, A. (2016) "Agents Without Agency: Assessing the Role of the Audience in Securitisation Theory", *Security Dialogue*, Vol.47 No.6, pp.541-558
Courtown, P. (2015) *Hansard Volume 762*, 2 July, Global Challenges, https://hansard.parliament.uk/Lords/2015-07-02/debates/15070243000900/GlobalChallenges?highlight=cyber%20terrorism#contribution-15070243000450, accessed on 12 April 2017
Cox, R. (1981) "Social Forces, States and World Orders: Beyond International Relations Theory", *Millennium: Journal of International Studies*, Vol.10 No.2, pp.126-155
Cox, R. (1986) "Social Forces, States and World Orders: Beyond International Relations Theory", pp.204-254 in ed. R Keohane, *Neorealism and its Critics*, New York: Columbia University Press
Creagh, M. (2016) *Hansard Volume 604*, 6 January, Flooding, https://hansard.parliament.uk/Commons/2016-01-06/debates/16010644000001/Flooding?highlight=cyber%20terrorism#contribution-16010651000114, accessed on 15th March 2017
Crenshaw, M. (2011) "The Debate over 'Old' vs 'New' Terrorism", pp.57-67 in ed. R Coolsaet and T Voorde, *Jihadi Terrorism and the Radicalisation Challenge: European and American Experiences*, Farnham: Ashgate
Croft, S. (2006) *Culture, Crisis and America's War on Terror*, Cambridge: Cambridge University Press
Croft, S. (2012) *Securitising Islam*, Cambridge: Cambridge University Press
Curzon, F. (2015a) *Hansard Volume 764*, 15 September, The Role and Capabilities of the UK Armed Forces, in the Light of Global and Domestic Threats to Stability and Security, https://hansard.parliament.uk/Lords/2015-09-15/debates/15091559000157/TheRoleAndCapabilitiesOfTheUKArmedForcesInTheLightOfGlobalAndDomesticThreatsToStabilityAndSecurity?highlight=cyber%20terror#contribution-15091559000002, accessed on 21 March 2017
Curzon, F. (2015b) *Hansard Volume 767*, 23 November, National Security Strategy and Strategic Defence and Security Review 2015, https://hansard.parliament.uk/Lords/2015-11-23/debates/1511235000464/NationalSecurityStrategyAndStrategicDefenceAndSecurityReview2015?highlight=cyber%20terrorism#contribution-15112311000013, accessed on 12 April 2017
Daddow, O. (2011) *New Labour and the European Union: Blair and Brown's Logic of History*, Manchester: Manchester University Press
Dahlgreen, W. (2015) "Brits Less Accepting of Syrian Refugees in Wake of Paris Attacks", *Yougov*, 18 November, https://yougov.co.uk/news/2015/11/18/brits-less-accepting-syrian-refugees-wake-paris-at/, accessed on 22 February 2016
Davies, C. (2010) "Technological Taxidermy: Recognisable Faces in Celebrity Deaths", *Mortality*, Vol.15 No.2, pp.138-153
Davies, M. (2015) *Hansard Volume 597*, 25 June, Reports into Investigatory Powers, https://hansard.parliament.uk/Commons/2015-06-25/debates/15062549000001/ReportsIntoInvestigatoryPowers?highlight=cyber%20terrorism#contribution-15062549000346, accessed on 12 April 2017
Davis, T. (2004) *The Face on the Screen: Death, Recognition and Spectatorship*, Bristol: Intellect
De Leonardis, F. (2008) "War as Medicine: The Medical Metaphor in Contemporary Italian Political Language", *Social Semiotics*, Vol.18 No.1, pp.33-45
Deacon, M. (2015) "How David Cameron Plans to Stop the Bad Men Doing Bad Things", *The Telegraph*, 2 November, http://www.telegraph.co.uk/news/politics/david-cameron/11970623/How-David-Cameron-plans-to-stop-the-bad-men-doing-bad-things.html, accessed on 9 March 2016
Dean, D et al. (2012) "The Internet Economy in the G20: The $4.2 Trillion Growth Opportunity", *Boston Consulting Group*, available at: https://www.bcg.com/documents/file100409.pdf, accessed on 28 July 2017
Dehghan, S. (2011) "Iran Accuses Siemans of Helping Launch Stuxnet Cyber-Attack", *The Guardian*, 17 April, https://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack, accessed on 29 June 2016
Deibert, R. (2011) "Tracking the Emerging Arms Race in Cyberspace", *Bulletin of the Atomic Scientists*, Vol.67 No.1, pp.1-8

Deibert, R and R Rohozinski. (2008) "Good for Liberty Bad for Security? Global Civil Society and the Securitisation of the Internet", pp.123-149 in ed. R Deibert, *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, MA: MIT Press
Deleuze, G and F Guattari. (1987) *A Thousand Plateaus: Capitalism and Schizophrenia*, Minneapolis: University of Minnesota Press
Deleuze, G and F Guattari. (1993) *A Thousand Plateaus: Capitalism and Schizophrenia*, trans. B Massumi, 4th ed, Minneapolis: University of Minnesota Press
Denning, D. (2000) "Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives", 23 May, *Naval Postgraduate School*, http://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm, accessed on 28 October 2015
Department for Transport. (2016) "Provisional Road Traffic Estimates Great Britain: January 2015 – December 2015", Statistical Release, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/499046/prov-road-traffic-estimates-jan-to-dec-2015.pdf, accessed on 28 July 2017
Der Derian, J. (1997) "The Virtualisation of Violence and the Disappearance of War", *Cultural Values*, Vol.1 No.2, pp.205-218
Derrida, J. (1981) *Positions*, Chicago: University of Chicago Press
Devost, M, B Houghton and N Pollard. (1997) "Information Terrorism: Political Violence in the Information Age", *Terrorism and Political Violence*, Vol.9 No.1, pp.72-83
Dews, F. (2014) "Squirrels – a Bigger Threat than Cyber Terrorists?", *Brookings*, 6 January, http://www.brookings.edu/blogs/brookings-now/posts/2014/01/squirrels-a-bigger-threat-than-cyber-terrorists, accessed on 28 January 2016
Dipert, R. (2010) "The Ethics of Cyberwarfare", *Journal of Military Ethics*, Vol.9 No.4, pp.384-410
Dodds, N. (2012) *Hansard Volume 545*, 23 May, G8 and NATO Summits, https://hansard.parliament.uk/Commons/2012-05-23/debates/12052368000003/G8AndNATOSummits?highlight=cyber%20terrorism, accessed on 11 April 2017
Dominiczak, P. (2013) "Tony Blair: The UK Must Continue to Tackle Terrorists", *The Telegraph*, 23 January, http://www.telegraph.co.uk/news/politics/tony-blair/9820254/Tony-Blair-The-UK-must-continue-to-tackle-terrorists.html, accessed on 8 May 2017
Dominiczak, P. (2014) "David Cameron Pledges £1.1 billion for Defence to Fight Cyber Terrorists", *The Telegraph*, 14 July, http://www.telegraph.co.uk/news/uknews/defence/10965182/David-Cameron-pledges-1.1-billion-for-defence-to-fight-cyber-terrorists.html, accessed on 23 January 2016
Donath, J. (1999) "Identity and Deception in the Virtual Community", pp.29-59 in ed. P Kollock and M Smith, *Communities in Cyberspace*, New York: Routledge
Doty, R. (1998) "Immigration and the Politics of Security", *Security Studies*, Vol.8 No.2-3, pp.71-93
Douglass, W and J Zulaika. (1990) "On the Interpretation of Terrorist Violence: ETA and the Basque Political Process", *Comparative Studies on Society and History*, Vol.32 No.2, pp.238-257
Dunsmuir, L. (2015) "FBI Chief Warns Encryption Emboldens Would-be Islamic State Attackers", *Reuters*, 8 July, http://www.reuters.com/article/us-usa-fbi-islamic-state-idUSKCN0PI24J20150708, accessed on 10 April 2017
Duyvesteyn, I. (2004) "How New is the New Terrorism?", *Studies in Conflict and Terrorism*, Vol.27 No.5, pp.439-454
Edelman, M. (1971) *Politics as Symbolic Action*, Chicago: Markham Publishing Company
Edelman, M. (1988) *Constructing the Political Spectacle*, Chicago: University of Chicago Press
Edkins, J and V Pin-Fat. (1999) "The Subject of the Political", pp.1-18 in ed. J Edkins, N Persram and V Pin-Fat, *Sovereignty and Subjectivity*, Boulder: Lynne Rienner
El Refaie, E. (2003) "Understanding Visual Metaphor: The Example of Newspaper Cartoons", *Visual Communication*, Vol.2 No.1, pp.75-95
Erlenbusch, V. (2010) "Notes on Violence: Walter Benjamin's Relevance for the Study of Terrorism", *Journal of Global Ethics*, Vol.6 No.2, pp.167-178
Erlenbusch, V. (2014) "How (not) to Study Terrorism", *Critical Review of International Social and Political Philosophy*, Vol.14 No.4, pp.470-491

Eroukhmanoff, C. (2015) “The Remote Securitisation of Islam in the US post-9/11: Euphemisation, Metaphors and the ‘Logic of Expected Consequences’ in Counter-Radicalisation Discourse”, Vol.8 No.2, pp.246-265
Evans, M. (2015a) “Hackers Steal 650 Million in World's Biggest Bank Raid”, *The Telegraph*, 15 February, http://www.telegraph.co.uk/news/uknews/crime/11414191/Hackers-steal-650-million-in-worlds-biggest-bank-raid.html, accessed on 8 February 2016
Evans, M. (2015b) “’Dark Web’ Drug Dealer Operating from an Idyllic Welsh Resort is Jailed”, *The Telegraph*, 24 July, http://www.telegraph.co.uk/news/uknews/crime/11761081/Dark-web-drug-dealer-operating-from-an-idyllic-Welsh-resort-is-jailed.html, accessed on 9 August 2017
Eysenck, H. (1977) *You and Neurosis*, London: Temple Smith
Fallon, M. (2015) *Hansard Volume 597*, 2 July, Britain and International Security, https://hansard.parliament.uk/Commons/2015-07-02/debates/15070233000001/BritainAndInternationalSecurity?highlight=cyber%20terrorism#contribution-15070233000574, accessed on 12 April 2017
Faulkner, W. (2001) “The Technology Question in Feminism: A View from Feminist Technology Studies”, *Women's Studies in International Forum*, Vol.24 No.1, pp.79-95
Fidler, D. (2003) “Public Health and National Security in the Global Age: Infectious Diseases, Bioterrorism and Realpolitik”, *The George Washington International Law Review*, Vol.35 No.4, pp.787-856
Fildes, J. (2011) “Stuxnet Virus Targets and Spread Revealed”, *BBC News*, 15 February, http://www.bbc.co.uk/news/technology-1246588, accessed on 20 July 2015
Finlay, I. (2011) *Hansard Volume 733*, 5 December, Health and Social Care Bill, https://hansard.parliament.uk/Lords/2011-12-05/debates/1112056000411/HealthAndSocialCareBill?highlight=cyberterrorism#contribution-1112056000107, accessed on 10 April 2017
Finnemore, M and K Sikkink. (1998) “International Norm Dynamics and Political Change”, *International Organization*, Vol.52 No.4, pp.887-917
Fisher, K. (2013) “Exploring the Temporality in/of British Counterterrorism Law and Law Making”, *Critical Studies on Terrorism*, Vol.6 No.1, pp.50-72
Flade, F. (2016) “Dschihadistische Kryptologie” [Jihadist Cryptology], *Investigativ.de*, 4 January, http://investigativ.welt.de/2016/01/04/dschihadistische-kryptologie/, accessed on 5 January 2016
Flemming, P and M Stohl. (2001) “Myths and Realities of Cyber Terrorism”, pp.70-105, in ed. A Schmid, *Countering Terrorism Through International Cooperation*, Vienna: ISPAC
Floyd, R. (2007) “Towards a Consequentialist Evaluation of Security: Bringing Together the Copenhagen and Welsh Schools of Security Studies”, *Review of International Studies*, Vol.33, pp.327-350
Floyd, R. (2010) *Security and the Environment: Securitisation Theory and US Environmental Security Policy*, Cambridge: Cambridge University Press
Foltyn, J. (2008) “Dead Famous and Dead Sexy: Popular Culture, Forensics, and the Rise of the Corpse”, *Mortality*, Vol.13 No.2, pp.153-173
Forstchen, W. (2009) *One Second After*, New York: Tor Books
Foucault, M. (1977) *Discipline and Punish*, New York
Foucault, M. (1980) “Two Lectures”, pp.78-108 in ed. C Gordon, *Power/Knowledge: Selected Interviews*, New York: Pantheon
Foucault, M. (2003) *Society Must be Defended*, New York: Pantheon
Foucault, M. (2006) “Madness and Civilisation: A History of Insanity in the Age of Reason”, trans. R Howard, London: Routledge
France24. (2015) “France’s TV5Monde Targeted in IS Group Cyberattack”, 9 April, http://www.france24.com/en/20150409-france-tv5monde-is-group-hacking, accessed on 8 August 2017
Frank, M. (2015) “Conjuring up the Next Attack: The Future-Orientedness of Terror and the Counterterrorist Imagination”, *Critical Studies on Terrorism*, Vol.8 No.1, pp.90-109
Furnell, S and M Warren. (1999) “Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium”, *Computers and Security*, Vol.18, pp.28-34
Future of Life Institute. (2015) “An Open Letter: Research Priorities for Robust and Beneficial Artificial Intelligence”, http://futureoflife.org/ai-open-letter/, accessed on 18 March 2016
Gadarian, S. (2014) “Scary Pictures: How Terrorism Imagery Affects Voter Evaluations”, *Political Communication*, Vol.31 No.2, pp.282-302

Galbraith, T. (2010) *Hansard Volume 721*, 19 October, Strategic Defence and Security Review, https://hansard.parliament.uk/Lords/2010-10-19/debates/10101930000474/StrategicDefenceAndSecurityReview?highlight=cyberterrorism#contribution-10101930000158, accessed on 10 April 2017
Galison, P. (2001) "War Against the Center", *Grey Room*, Vol.4, pp.5-33
Gallagher, I. (2015) "ISIS 'Cyber Caliphate' Hacks 54,000 Twitter Accounts and Posts Phone Numbers of Heads of the CIA and FBI in Revenge for the Drone Attack that Killed a British Extremist", *Main on Sunday*, 8 November, http://www.dailymail.co.uk/news/article-3308734/ISIS-cyber-caliphate-takes-54-000-Twitter-accounts-Terrorists-hack-social-media-site-spread-vile-propaganda.html, accessed on 8 August 2017
Gapes, M. (2015) *Hansard Volume 565*, 4 July, NATO, https://hansard.parliament.uk/Commons/2013-07-04/debates/13070444000001/NATO?highlight=cyber%20terrorist, accessed on 3 April 2017
Gareau, F. (2004) *State Terrorism and the United States: From Counterinsurgency to the War on Terrorism*, London: Zed
Garside, J. (2014) "Facebook Will Lose 80% of Users by 2017, say Princeton Researchers", *The Guardian*, 22 January, http://www.theguardian.com/technology/2014/jan/22/facebook-princeton-researchers-infectious-disease, accessed on 25 January 2016
Gartner, S. (2011) "On Behalf of a Grateful Nation: Conventionalised Images of Loss and Individual Opinion Change in War", *International Studies Quarterly*, Vol.55, pp.545-561
Gentry, C. (2015) "Anxiety and the Creation of the Scapegoated Other", *Critical Studies on Security*, Vol.3 No.2, pp.133-146
Gentry, C and L Sjoberg. (2014) "Terrorism and Political Violence", pp.120-130 in ed. L Shepherd, *Gender Matters in Global Politics*, London: Routledge
Giacomello, G. (2004) "Bangs for the Buck: A Cost-benefit Analysis of Cyber Terrorism", *Studies in Conflict and Terrorism*, Vol.27, pp.387-408
Gibbs, S and L Beckett. (2017) "Dark Web Marketplaces Alphabay and Hansa Shut Down", 20 July, https://www.theguardian.com/technology/2017/jul/20/dark-web-marketplaces-alphabay-hansa-shut-down, accessed on 9 August 2017
Gilbert, D et al. (2003) "Technophobia, Gender Influences and Consumer Decision-making for Technology-related Products", *European Journal of Innovation Management*, Vol.6 No.4, pp.253-263
Gilbert, S. (2013) *Hansard Volume 565*, 4 July, NATO, https://hansard.parliament.uk/Commons/2013-07-04/debates/13070444000001/NATO?highlight=cyber%20terrorism#contribution-13070444000565, accessed on 11 April 2017
Giles, K. (2016) *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, Research Paper, London: Chatham House
Glenny, G. (2009) *McMafia: Seriously Organised Crime*, London: Vintage
Global Terrorism Database. (2017) https://www.start.umd.edu/gtd/, accessed on 6th November 2017
Goede, M. (2008) "Beyond Risk: Premediation and the Post-9/11 Security Imagination", *Security Dialogue*, Vol.39 No.2-3, pp.155-176
Goede, M. (2011) *European Security Culture: Preemption and Precaution in European Security*, Inaugural Lecture, available at: http://www.oratiereeks.nl/upload/pdf/PDF-1587De_Goede.pdf, accessed on 3 August 2017
Goede, M and B Graaf. (2013) "Sentencing Risk: Temporality and Precaution in Terrorism Trials", *International Political Sociology*, Vol.7, pp.313-331
Goldberg, G. (2010) "Rethinking the Public/virtual Sphere: The Problem with Participation", *New Media and Society*, Vol.13 No.5, pp.739-754
Goodin, D. (2016) "Analysis Confirms Coordinated Hack Attack Caused Ukrainian Power Outage", *Arstechnica*, 11 January, http://arstechnica.com/security/2016/01/analysis-confirms-coordinated-hack-attack-caused-ukrainian-power-outage/, accessed on 28 January 2016
Goodin, D. (2017a) "NSA-leaking Shadow Brokers Just Dumped its Most Damaging Release Yet", *Arstechnica*, 14 April, https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/, accessed on 14 September 2017
Goodin, D. (2017b) "Mysterious Microsoft Patch Killed 0-days Released by NSA-leaking Shadow Brokers", *Arstechnica*, 15 April, https://arstechnica.com/information-technology/2017/04/purported-shadow-brokers-0days-were-in-fact-killed-by-mysterious-patch accessed on 14 September 2017
Gordon, S and R Ford. (2002) "Cyberterrorism?", *Computers and Security*, Vol.21 No.7, pp.636-647

Graham, C. (2017) "NHS Cyber Attack: Everything you Need to Know About 'Biggest Ransomware' Offensive in History", *The Telegraph*, http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/, accessed on 14 September 2017
Graham, S. (2004) "Postmodern City", *City*, Vol.8 No.2, pp.165-196
Graham-Harrison, E. (2015) "Could ISIS's 'Cyber Caliphate' Unleash a Deadly Attack on Key Targets?", *The Guardian*, 12 April, https://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race, accessed on 8 August 2017
Gray, J. (2015) *Hansard Volume 593*, 2 March, Defence and Security Review (NATO), https://hansard.parliament.uk/Commons/2015-03-02/debates/15030240000001/DefenceAndSecurityReview(NATO)?highlight=cyber%20terrorist, accessed on 24 April 2017
Gray, M. (2003) "Urban Surveillance and Panopticism: Will We Recognise the Facial Recognition Society?", *Surveillance and Society*, Vol.1 No.3, pp.314-330
Green, J. (2002) "The Myth of Cyberterrorism", *Washington Monthly*, November, http://www.washingtonmonthly.com/features/2001/0211.green.html, accessed on 28 October 2015
Griffin, M. (1999) "The Great War Photographs: Constructing Myths of History and Photojournalism", pp.122-157 in ed. B Brennen and H Hart, *Picturing the Past: Media, History, and Photography*, Urbana: University of Illinois Press
Griffiths, M, S Roach and M Solomon. (2009) *Fifty Key Thinkers in International Relations*, 2nd ed, London: Routledge
Grimes, R. (2017) *Hacking the Hacker: Learn from the Experts who Take Down Hackers*, Hoboken: Wiley, Kindle edition
Grusin, R. (2004) "Premediation", *Criticism*, Vol.46 No.1, pp.17-39
Gurr, N and B Cole. (2000) *The New Face of Terrorism: Threats from Weapons of Mass Destruction*, London: IB Tauris
Guzik, K. (2009) "Discrimination by Design: Data Mining in the United States's 'War on Terrorism'", *Surveillance and Society*, Vol.7 No.1, pp.1-17
Ha, J et al. (2011) "A Study on Technophobia and Mobile Device Design", *International Journal of Contents*, Vol.7 No.2, pp.17-25
Guzzini, S. (2011) "Securitisation as a Causal Mechanism", *Security Dialogue*, Vol.42 No.4-5, pp.329-341
Hagmann, J and M Dunn Cavelty. (2012) "National Risk Registers: Security Scientism and the Propagation of Permanent Insecurity", *Security Dialogue*, Vol.43 No.1, pp.79-96
Hague, W. (2013a) "Foreign Secretary statement to the House of Commons – GCHQ", 10 June, https://www.gov.uk/government/speeches/foreign-secretary-statement-to-the-house-of-commons-gchq, accessed on 21 March 2017
Hague, W. (2013b) "Building a New International Consensus on the Future of Cyberspace", *Gov.uk*, 16 October, https://www.gov.uk/government/speeches/building-a-new-international-consensus-on-the-future-of-cyberspace, accessed on 21 March 2017
Hague, W. (2013c) "Foreign Secretary visits GCHQ", *Gov.uk*, 1st August, https://www.gov.uk/government/news/foreign-secretary-visits-gchq, accessed on 6 April 2017
Hall, I. (2013) "Kenneth Waltz: The Man Who Saved Realism", *E-International Relations*, 24 June, http://www.e-ir.info/2013/06/24/kenneth-waltz-the-man-who-saved-realism/, accessed on 23 February 2016
Hall, J. (1993) "Ideas and Social Sciences", pp.31-56 in ed. J Goldstein and R Keohane, *Ideas and Foreign Policy: Beliefs, Institutions and Political Change*, Ithaca: Cornell University Press
Hall, S. (1987) "Minimal Selves", ICA *Documents* 6, London: ICA:44-46
Hamilton, F and J Dean. (2015) "GCHQ Foils 200 Cyberattacks a Month", *The Times*, 10 November, http://www.thetimes.co.uk/tto/news/uk/crime/article4609588.ece, accessed on 8 February 2016
Hammond, J. (2015) "The Government's Cyberterrorism 'Concerns' are a Pretext for their Own Hacking Operations", *The Guardian*, 4 February, https://www.theguardian.com/commentisfree/2015/feb/04/government-cyberterrorism-concerns-pretext-their-own-hacking, accessed on 11 April 2018
Hammond, P. (2013) interview with S Walters, "Hammond's 500m New Cyber Army: As he Reveals Top-secret Whitehall Bunker for the First Time, Defence Secretary says Future Wars Will be Fought with Viruses", *Mail on Sunday*, 29 September, http://www.dailymail.co.uk/news/article-2436946/Hammonds-

500m-new-cyber-army-As-reveals-secret-Whitehall-bunker-time-Defence-Secretary-says-future-wars-fought-viruses.html, accessed on 3 April 2017
Hammond, S. (2016) *Hansard 607*, Investigatory Powers Bill, https://hansard.parliament.uk/Commons/2016-03-15/debates/16031546000001/InvestigatoryPowersBill?highlight=cyber%20terrorism#contribution-84F8C145-F9DD-4F1F-A4B9-0D8DE06F8F10, accessed on 21 June 2018
Hancock, M. (2016a) "UK Cyber Security Strategy: Statement on the Final Annual Report", *Gov.uk*, 14 April, https://www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-the-final-annual-report, accessed on 21 March 2017
Hancock, M. (2016b) "Government's Role in Supporting the Cyber Security Sector: Matt Hancock Speech", *Gov.uk*, 16 February, https://www.gov.uk/government/speeches/governments-role-in-supporting-the-cyber-security-sector-matt-hancock-speech, accessed on 6 April 2017
Hancock, M. (2016c) "New National Cyber Security Centre Set to Bring UK Expertise Together", *Gov.uk*, 18 March, https://www.gov.uk/government/news/new-national-cyber-security-centre-set-to-bring-uk-expertise-together, accessed on 6 April 2017
Hancock, M. (2016d) "Expanding the Cyber First Programme: Speech by Matt Hancock", *Gov.uk*, 3 March, https://www.gov.uk/government/speeches/expanding-the-cyber-first-programme-speech-by-matt-hancock, accessed on 3 May 2017
Hannay, D. (2010) *Hansard Volume 721*, 14 October, Cyberattacks: EU Committee Report, https://hansard.parliament.uk/Lords/2010-10-14/debates/10101424000811/CyberattacksEUCommitteeReport?highlight=cyber%20terrorists#contribution-10101424000536, accessed on 10 April 2017
Hansen, L. (2006) *Security as Practice: Discourse Analysis and the Bosnian War*, London: Routledge
Hansen, L. (2011) "The Politics of Securitisation and the Muhammad Cartoon Crisis: A Post-structuralist Perspective", *Security Dialogue*, Vol.42 No.4-5, pp.357-369
Hansen, L. (2015) "How Images Make World Politics: International Icons and the Case of Abu Ghraib", *Review of International Studies*, Vol.41, pp.263-288
Hansen, L and H Nissenbaum. (2009) "Digital Disaster, Cyber Security, and the Copenhagen School", *International Studies Quarterly*, Vol.53, pp.1155-1175
Harris, J. (2015) *Hansard Volume 765*, 3 November, Electricity System Resilience (S&T Committee Report), https://hansard.parliament.uk/Lords/2015-11-03/debates/15110341000429/ElectricitySystemResilience(SAndTCommitteeReport)?highlight=cyber%20terrorism, accessed on 24 April 2017
Harvey, F. (2015) "Paris Climate Change Agreement: The World's Greatest Diplomatic Success", *The Guardian*, 14 December, http://www.theguardian.com/environment/2015/dec/13/paris-climate-deal-cop-diplomacy-developing-united-nations, accessed on 1 March 2016
Harvey, N. (2015) *Hansard Volume 594*, 12 March, Defence Spending, https://hansard.parliament.uk/Commons/2015-03-12/debates/15031223000001/DefenceSpending?highlight=cyber%20terrorism, accessed on 12 April 2017
Hay, C. (2004) "'Taking Ideas Seriously' in Explanatory Political Analysis", pp.142-149 in The Interpretive Approach in Political Science: A Symposium, *British Journal of Politics and International Relations*, Vol.6, pp.129-164
Hay, C. (2011) "Interpreting Interpretivism Interpreting Interpretations: The New Hermeneutics of Public Administration", *Public Administration*, Vol.89 No.1, pp.167-182
Hayes, A and T Myers. (2009) "Testing the 'Proximate Casualties Hypothesis': Local Troop Loss, Attention to News, and Support for Military Intervention", *Mass Communication and Society*, Vol.12 No.4, pp.379-402
Hayes, J. (2016) "Security Minister: What is Real is Reasonable", *Gov.uk*, 25 February, https://www.gov.uk/government/speeches/security-minister-what-is-real-is-reasonable, accessed on 21 March 2017
Heck, A and G Schlag. (2013) "Securitising Images: The Female Body and the War in Afghanistan", *European Journal of International Relations*, Vol.19 No.4, pp.891-913
Heeter, C. (1992) "Being There: The Subjective Experience of Presence", *Presence: Teleoperators and Virtual Environments*, Vol.1 No.2, pp.262-271
Heim, M. (1991) "The Erotic Ontology of Cyberspace", pp.75-76 in ed. M Benedikt, *Cyberspace*, Cambridge MA: MIT Press

Hellmich, C. (2008) “Creating the Ideology of Al Qaeda: From Hypocrites to Salafi-Jihadists”, *Studies in Conflict and Terrorism*, Vol.31 No.2, pp.111-124
Hern, A. (2014) “US Government Increases Funding for Tor, Giving $1.8m in 2013”, *The Guardian*, 29 July, https://www.theguardian.com/technology/2014/jul/29/us-government-funding-tor-18m-onion-router, accessed on 10 November 2017
Hern, A. (2015) “Infidelity Site Ashley Madison Hacked as Attackers Demand Total Shutdown”, *The Guardian*, 20 July, http://www.theguardian.com/technology/2015/jul/20/ashley-madison-hacked-cheating-site-total-shutdown, accessed on 14 March 2016
Hodgson, F. (2016) *Hansard Volume 768*, 11 February, Armed Forces Bill, https://hansard.parliament.uk/Lords/2016-02-11/debates/16021145000725/ArmedForcesBill?highlight=cyber%20terrorism#contribution-16021145000174, accessed on 21 June 2018
Hoffman, B. (1998) *Inside Terrorism*, London: St Andrew’s University Press
Hoffmann, S. (1987) “Structural Realism and the Causes of War”, *Mershon International Studies Review*, Vol.39 No.2, pp.181-208
Hogan, M. (2009) “Age Differences in Technophobia: An Irish Study”, *Information Systems Development: Challenges in Practice, Theory and Education*, Vol.1, pp.117-130
Holland, J. (2011) “When You Think of the Taliban, Think of the Nazis: Teaching Americans 9/11 in NBC’s the West Wing”, *Millennium*, Vol.40 No.1, pp.85-106
Holland, J. (2013) “Foreign Policy and Political Possibility”, *European Journal of International Relations*, Vol.19 No.1, pp.48-67
Holland, J. (2014) “Video Use and the Student Learning Experience in Politics and International Relations, *Politics*, Vol.34 No.3, pp.263-274
Holland, J. (2016) “Visual Literacy in International Relations: Teaching Critical Evaluative Skills Through Fictional Television”, *International Studies Perspectives*, Vol.17, pp.173-186
Holm, N. (2009) “Conspiracy Theorising Surveillance: Considering Modalities of Paranoia and Conspiracy in Surveillance Studies”, *Surveillance and Society*, Vol.7 No.1, pp.36-48
Holzscheiter, A. (2005) “Discourse as Capability: Non-State Actors’ Capital in Global Governance”, *Journal of International Studies*, Vol.33 No.3, pp.723-746
Home Office. (2002) *Secure Borders, Safe Haven: Integration with Diversity in Modern Britain*, London: The Stationary Office
Home Office. (2011) *CONTEST: The United Kingdom’s Strategy for Countering Terrorism*, Norwich: The Stationary Office
Home Office. (2017) *Proscribed Terrorist Organisations*, London: Home Office
Home Office and J Brokenshire. (2013) “James Brokenshire speech on Cyber Crime”, *Gov.uk*, 14 March, https://www.gov.uk/government/speeches/james-brokenshire-speech-on-cyber-crime, accessed on 6 April 2017
Hopf, T. (1998) “The Promise of Constructivism in International Relations Theory”, *International Security*, Vol.23 No.1, pp.171-200
Hopkins, N. (2011) “UK Developing Cyber-weapons Program to Counter Cyber War Threat”, *The Guardian*, 30 May, https://www.theguardian.com/uk/2011/may/30/military-cyberwar-offensive, accessed on 6 November 2017
Horwood, M. (2014) *Hansard Volume 576*, 4 March, Defence and Cyber-Security, https://hansard.parliament.uk/Commons/2014-03-04/debates/14030455000001/DefenceAndCyber-Security?highlight=cyber%20terrorism, accessed on 15th March 2017
House of Commons Defence Committee. (2012a) *Developing Threats: Electromagnetic Pulses (EMP)*, Tenth Report of Session 2010-2012, London: Stationary Office
House of Commons Defence Committee. (2012b) *Developing Threats: Electromagnetic Pulses (EMP): Government Response to the Committee’s Tenth Report of Session 2010-2012*, London: Stationary Office
House of Commons Library. (1998) *The Strategic Defence Review White Paper*, London: House of Commons Library
Howard, R and R Sawyer. (2004) *Terrorism and Counter-Terrorism: Understanding the New Security Environment*, Maidenhead: McGraw-Hill
Howarth, G. (2007) *Death and Drying: A Sociological Introduction*, Cambridge: Polity Press

Hua, J and S Bapna. (2012) "The Economic Impact of Cyber Terrorism", *Journal of Strategic Information Systems*, Vol.22 No.2, pp.175-186
Hudson, R. (1999) *The Sociology and Psychology of Terrorism: Who Became a Terrorist and Why?*, Washington DC: Library of Congress
Hulsse, R and A Spencer. (2008) "The Metaphor of Terror: Terrorism Studies and the Constructivist Turn", *Security Dialogue*, Vol.39 No.6, pp.571-592
Intelligence and Security Committee. (2010) *Intelligence and Security Committee Annual Report 2009-2010*, London: Stationary Office
Idaho National Laboratory. (2016) *Cyber Threat and Vulnerability Analysis of the US Electric Sector: Mission Support Center Analysis Report*, Idaho Falls: Idaho National Laboratory
Iqbal, M. (2004) "Defining Cyberterrorism", *Journal of Computer and Information Law*, Vol.22, pp.397-408
Jackson, R. (2005) *Writing the War on Terrorism: Language, Politics and Counterterrorism*, Manchester: Manchester University Press
Jackson, R. (2007) "The Core Commitments of Critical Terrorism Studies", *European Political Science*, Vol.6 No.3, pp.244-251
Jackson, R. (2008) "The Ghosts of State Terror: Knowledge, Politics and Terrorism Studies", *Critical Studies on Terrorism*, Vol.1 No.3, pp.377-392
Jackson, R. (2012) "The Study of Terrorism 10 Years After 9/11: Success, Issues, Challenges", *Uluslararasu Iliskiler*, Vol.8 No.32, pp.1-16
Jackson, R. (2015) "The Epistemological Crisis of Counterterrorism", *Critical Studies on Terrorism*, Vol.8 No.1, pp.33-54
Jarvis, D. (2015) *Hansard Volume 597*, 2 July, Britain and International Security, https://hansard.parliament.uk/Commons/2015-07-02/debates/15070233000001/BritainAndInternationalSecurity?highlight=cyber%20terrorism#contribution-15070238000313, accessed on 12 April 2017
Jarvis, L. (2009) "The Spaces and Faces of Critical Terrorism Studies", *Security Dialogue*, Vol.40 No.1, pp.5-27
Jarvis, L. (2015) "I am Somewhat Puzzled: Terrorism, Proscription and Securitisation", Guest Seminar, *Nottingham Trent University Politics and International Relations Departmental Seminar Series*, 2 December, .MP3 recording available on request
Jarvis, L and M Lister. (2012) "Disconnected Citizenship? The Impacts of Anti-Terrorism Policy on Citizenship in the UK", *Political Studies*, Vol.61 No.3, pp.656-675
Jarvis, L and M Lister. (2013) "Vernacular Securities and their Study: A Qualitative Analysis and Research Agenda", *International Relations*, Vol.27 No.2, pp.158-179
Jarvis, L and M Lister. (2014) "State Terrorism Research and Critical Terrorism Studies: An Assessment", *Critical Studies on Terrorism*, Vol.7 No.1, pp.43-61
Jarvis, L, L Nouri and Andrew Whiting. (2014) "Understanding, Locating and Constructing Cyberterrorism", pp.25-41 in ed. T Chen, L Jarvis and S MacDonald, *Cyberterrorism*, New York: Springer
Jarvis, L and S MacDonald. (2015) "What is Cyberterrorism? Findings from a Survey of Researchers", *Terrorism and Political Violence*, Vol.27 No.4, pp.657-678
Jarvis, L, S MacDonald and A Whiting. (2016a) "Unpacking Cyberterrorism Discourse: Specificity, Status, and Scale in News Media Constructions of Threat", *European Journal of International Security*, Vol.2 No.1, pp.64-87
Jarvis, L, S MacDonald and A Whiting. (2016b) "Analogy and Authority in Cyberterrorism Discourse: An Analysis of Global News Media Coverage", *Global Society*, Vol.30 No.4, pp.605-623
Jarvis, L, S MacDonald and L Nouri. (2014) "The Cyberterrorism Threat: Findings from a Survey of Researchers", *Studies in Conflict and Terrorism*, Vol.37 No.1, pp.68-90
Jarvis, L and T Legrand. (2017) "'I am Somewhat Puzzled': Questions, Audiences and Securitisation in the Proscription of Terrorist Organisations", *Security Dialogue*, Vol.48 No.2, pp.149-167
Jay, T. (1981) "Computerphobia – What to Do About it", *Educational Technology*, Vol.1, pp.47-48
Johnson-Laird, P. (1983) *Mental Models: Towards a Cognitive Science of Language, Inference and Consciousness*, Cambridge: Cambridge University Press
Jolly, J. (2015) *Hansard Volume 767*, 3 December, Strategic Defence and Security Review, https://hansard.parliament.uk/Lords/2015-12-

03/debates/15120364000830/StrategicDefenceAndSecurityReview?highlight=cyber%20terrorist#contributio n-15120364000497, accessed on 3 April 2017
Jones, A. (2005) "Cyber Terrorism: Fact or Fiction?", *Computer Fraud and Security*, No.6, pp.4-7
Jones, K. (2013) *Hansard Volume 556*, 17 January, Nuclear Deterrent, https://hansard.parliament.uk/Commons/2013-01-17/debates/13011761000005/NuclearDeterrent?highlight=cyber%20terrorism#contribution-13011761000961, accessed on 11 April 2017
Jones, S. (2017) "Russia Mobilises an Elite Band of Cyber Warriors", *Financial Times*, 23 February, https://www.ft.com/content/f41e1dc4-ef83-11e6-ba01-119a44939bb6, accessed on 2 August 2017
Jopling, T. (2010) *Hansard Volume 721*, 14 October, Cyberattacks: EU Committee Report, https://hansard.parliament.uk/Lords/2010-10-14/debates/10101424000811/CyberattacksEUCommitteeReport?highlight=cyber%20terrorists#contribution-10101424000536, accessed on 10 April 2017
Kahn, D. (1997) *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, New York: Scribner
Kalapesi, C, S Willersdorf and P Zwillenberg. (2010) "The Connected Kingdom: How the Internet is Transforming the UK Economy", *Boston Consulting Group*, available at: https://www.bcg.com/documents/file62983.pdf, accessed on 28 July 2017
Keet, M. (2003) *Terrorism and Game Theory: Coalitions, Negotiations and Audience Costs*, Limerick: University of Limerick
Kellner, D. (2004) "9/11, Spectacles of Terror, and Media Manipulation", *Critical Discourse Studies*, Vol.1 No.1, pp.41-64
Kelly, S, M Truong, A Shahbaz and M Earp. *Freedom on the Net: Silencing the Messenger: Communication Apps under Pressure*, Washington DC: Freedom House
Kermode, F. (1967) *The Sense of An Ending: Studies in the Theory of Fiction*, London: Oxford University Press
Kertzer, D. (1988) *Ritual, Politics and Power*, New Haven: Yale University Press
Kessler, O. (2008) "Is Risk Changing the Politics of Legal Argumentation?", *Leiden Journal of International Law*, Vol.21 No.4, pp.863-884
Khomami, N. (2015) "TalkTalk Hacking Crisis Deepens as More Details Emerge", *Guardian*, 23 October, http://www.theguardian.com/business/2015/oct/23/talktalk-hacking-crisis-deepens-as-more-details-emerge, accessed on 14 March 2016
Kingsmith, A. (2013) "Virtual Roadblocks: The Securitisation of the Information Superhighway", *Bridges: Conversations in Global Politics and Public Policy*, Vol.1 No.1, available at: https://escarpmentpress.org/bridges/article/view/1199, accessed on 7 March 2016
Kinnvall, C. (2004) "Globalisation and Religious Nationalism: Self, Identity, and the Search for Ontological Security", *Political Psychology*, Vol.25 No.5, pp.741-767
Kittner, C. (2007) "The Role of Safe Havens in Islamist Terrorism", *Terrorism and Political Violence*, Vol.19 No.3, pp.307-329
Klimburg, A. (2017) *The Darkening Web: The War for Cyberspace*, New York: Penguin Press, Kindle edition
Knapton, S. (2014) "BBC Staff Told to Stop Inviting Cranks on to Science Programmes", *The Telegraph*, 4 July, http://www.telegraph.co.uk/culture/tvandradio/bbc/10944629/BBC-staff-told-to-stop-inviting-cranks-on-to-science-programmes.html, accessed on 1 March 2016
Kollock, P and M Smith. (1996) "Managing the Virtual Commons: Cooperation and Conflict in Computer Communities", pp.109-128 in ed. S Herring, *Computer-Mediated Communication*, Amsterdam: John Benjamins
Koskela, H. (2002) "Video Surveillance, Gender and the Safety of Public Urban Space: 'Peeping Tom' Goes High Tech?", *Urban Geography*, Vol.23 No.3, pp.257-278
Kowert, P. (2001) "Toward a Constructivist Theory of Foreign Policy", pp.266-289 in ed. V Kabulkova, *Foreign Policy in a Constructed World*, New York: M.E. Sharpe
Krause, K and M Williams. (1996) "Broadening the Agenda of Security Studies: Politics and Methods", *Mershon International Studies Review*, Vol.40 No.2, pp.229-254
Krause, K and M Williams. (1997) "Preface: Toward Critical Security Studies", pp.vii-xxi in ed. K Krause and M Williams, *Critical Security Studies: Concepts and Cases*, London: UCL Press

Krepinevich, A. (2012) “Cyber Warfare: a ‘Nuclear Option’”, *Center for Strategic and Budgetary Assessments*, Washington DC: Center for Strategic and Budgetary Assessments
Kress, G. (1994) “Text and Grammar as Explanation”, pp.24-46 in ed. U Meinhof and K Richardson, *Text, Discourse and Context: Representations of Poverty in Britain*, London: Longman
Krueger, A and J Maleckova. (2003) “Education, Poverty, Political Violence, and Terrorism: is there a Connection?”, *Journal of Economic Perspectives*, Vol.17 No.4, pp.119-144
Kumagai, J. (2001) “The Web as Weapon: Will the Networked World Become a New Digital Battleground?”, *IEEE Spectrum*, (January)
Kravets, D. (2015) “It’s Official: Sharks no Longer a Threat to Subsea Internet Cables”, *Arstechnica*, 7 October, https://arstechnica.co.uk/information-technology/2015/07/its-official-sharks-no-longer-a-threat-to-subsea-internet-cables/, accessed on 10 Novemebr 2017
Lacan, J. (2007) *Ecrits*, trans. B Fink, New York: W.W. Norton and Company
Laclau, E and C Mouffe. (2001) *Hegemony and Socialist Strategy*, 2nd ed, New York: Verso
Lake, E. (2017) “CUFF HIM ‘James Bond jihadi’ Samata Ullah who used cyber cufflinks to hide ISIS data and was branded new breed of terrorist is caged”, *The Sun*, 2 May, https://www.thesun.co.uk/news/3459144/james-bond-jihadi-samata-ullah-who-used-cyber-cufflinks-to-hide-isis-data-and-was-branded-new-breed-of-terrorist-is-caged/, accessed on 9 May 2017
Lakoff, A. (2007) “Preparing for the Next Emergency”, *Public Culture*, Vol.19, pp.247-271
Lakoff, G and M Johnson. (1980) *Metaphors We Live By*, Chicago: University of Chicago Press
Laqueur, W. (2000) *The New Terrorism: Fanaticism and the Arms of Mass Destruction*, New York: Oxford University Press
Lebow, R. (1994) “The Long Peace, the End of the Cold War, and the Failure of Realism”, *International Organization*, Vol.48 No.2, pp.249-277
Lee, A. (2017) “Theresa May’s Crackdown on the Internet Will Let Terror in the Backdoor”, *The Guardian*, 20 June, https://www.theguardian.com/commentisfree/2017/jun/20/theresa-may-crackdown-snoopers-charter-encryption-terror-backdoor, accessed on 10 November 2017
Legislation.gov.uk. (1990) *The Computer Misuse Act 1990*, Chapter 18, http://www.legislation.gov.uk/ukpga/1990/18/contents, accessed on 16 June 2016
Legislation.gov.uk. (2000) *The Terrorism Act 2000*, Chapter 11, http://www.legislation.gov.uk/ukpga/2000/11/contents, accessed on 22 March 2015
Lerner, J and D Keltner. (2000) “Beyond Valence: Toward a Model of Emotion-specific Influences on Judgement and Choice”, *Cognition and Emotion*, Vol.14 No.4, pp.473-493
Lerner, J and D Keltner. (2001) “Fear, Anger and Risk”, *Journal of Personality and Social Psychology*, Vol.81 No.1, pp.146-159
Lerner, J et al. (2003) “Emotion and Perceived Risks of Terrorism: A National Field Experiment”, *Psychological Science*, Vol.14, pp.144-150
Lesser, I. (1999) “Countering the New Terrorism: Implications for Strategy”, pp.85-144 in I Lesser et al, *Countering the New Terrorism*, Santa Monica: RAND Corporation
Lesser, I et al. (2002) *Countering the New Terrorism*, Santa Monica: RAND Corporation
Libicki, M. (2007) *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge: Cambridge University Press
Liff, A. (2012) “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War”, *Journal of Strategic Studies*, Vol.35 No.3, pp.401-428
Lin, P. (2010) “Ethical Blowback from Emerging Technologies”, *Journal of Military Ethics*, Vol.9 No.4, pp.313-331
Lynch, C. (2014) *Interpreting International Politics*, London: Routledge
Lynfield, B. (2015) “Israel Accused of ‘War Crime’ over Bulldozing of Palestinian Olive Groves”, *Independent*, 15 June, https://www.independent.co.uk/news/world/middle-east/israel-accused-of-war-crime-over-bulldozing-of-palestinian-olive-groves-10321936.html, accessed on 31 May 2017
MacAskill, E. (2010) “Countries are Risking Cyber Terrorism, Security Expert Tells First World Summit”, *The Guardian*, 5 May, https://www.theguardian.com/technology/2010/may/05/terrorism-uksecurity, accessed on 11 April 2018.
MacAskill, E. (2017a) “Cage Director Charged under Terrorism Act after Failing to Hand over Passwords”, *The Guardian*, 17 May, https://www.theguardian.com/uk-news/2017/may/17/cage-campaign-group-director-muhammed-rabbani-charged-under-terrorism-act, accessed on 9 November 2017

MacAskill, E. (2017b) “HMS Queen Elizabeth Could be Vulnerable to Cyber-attack”, *The Guardian*, 27 June, https://www.theguardian.com/technology/2017/jun/27/hms-queen-elizabeth-royal-navy-vulnerable-cyber-attack, accessed on 14 September 2017
MacAskill, E, J Borger, N Hopkins, N Davies and J Ball. (2013) “GCHQ Taps Fibre-Optic Cables for Secret Access to World’s Communications”, *The Guardian*, 21 June, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa, accessed on 20 July 2015
MacAskill, E and S Syal. (2017) “Cyber-attack on UK Parliament: Russia is Suspected Culprit”, *The Guardian*, 25 June, https://www.theguardian.com/politics/2017/jun/25/cyber-attack-on-uk-parliament-russia-is-suspected-culprit, accessed on 7 July 2017
MacDonald, S, L Jarvis, T Chen and S Lavis. (2013) *Cyberterrorism: A Survey of Researchers*, Cyberterrorism Project Research Report No.1, Swansea: Swansea University
MacDougall, D. (1998) *Transcultural Cinema*, Princeton: Princeton University Press
Makarenko, T. (2004) “The Crime-Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism”, *Global Crime*, Vol.6 No.1, pp.129-145
Manson, G. (2011) “Cyberwar: The United States and China Prepare for the Next Generation of Conflict”, *Comparative Strategy*, Vol.30 No.2, pp.121-133
Markoff, J. (2017) “A Better, Safer Battery Could be Coming to a Laptop Near You”, *New York Times*, 1 August, https://www.nytimes.com/2017/08/01/technology/alkaline-batteries-replace-lithium-ion.html, accessed on 11 April 2018
Mason, R. (2014) “MH17 Crash: Sanctions Against Russia are Illegal, Ambassador Claims”, *Guardian*, 24 July, https://www.theguardian.com/world/2014/jul/24/malaysia-airlines-flight-mh17-russia, accessed on 2 August 2017
Mason, R and P Wintour. (2014) “UK to Press European allies for Tougher Sanctions Against Russia over MH17”, *Guardian*, 21 July, https://www.theguardian.com/world/2014/jul/21/uk-europe-tougher-sanctions-russia-mh17-putin, accessed on 2 August 2017
Massumi, B. (2005) “Fear (the spectrum said)”, *Positions*, Vol.31, pp.31-48
Matthews, A and C Macleod. (1986) “Discrimination of Threat Cues Without Awareness in Anxiety States”, *Journal of Abnormal Psychology*, Vol.95, pp.131-138
Matthews, J. (2005) “Visual Culture and Critical Pedagogy in ‘Terrorist Times’”, *Discourse Studies in the Cultural Politics of Education*, Vol.26 No.2, pp.203-224
Maude, F. (2011) *Hansard Volume 536*, 25 November, Cyber-security Strategy, https://hansard.parliament.uk/Commons/2011-11-25/debates/11112516000009/Cyber-SecurityStrategy?highlight=cyber%20terrorism#contribution-11112516000019, accessed on 10 April 2017
Maude, F. (2012a) “Francis Maude Speech at the International Centre for Defence Studies in Estonia”, *Gov.uk*, 3 May, https://www.gov.uk/government/speeches/francis-maude-speech-at-the-international-centre-for-defence-studies-icds-in-estonia, accessed on 21 March 2017
Maude, F. (2012b) “Francis Maude speech at IA12 – Cyber Security Strategy One Year On”, *Gov.uk*, 4 December, https://www.gov.uk/government/speeches/francis-maude-speech-at-ia12-cyber-security-strategy-one-year-on, accessed on 21 March 2017
Maude, F. (2012c) “UK Announces Extra Funding for Cyber Security Capacity Building”, *Gov.uk*, 4 October, https://www.gov.uk/government/news/uk-announces-extra-funding-for-cyber-security-capacity-building, accessed on 6 April 2017
Maude, F. (2012d) “Cyber Security Strategy: statement 1 year on”, *Gov.uk*, 3 December, https://www.gov.uk/government/speeches/cyber-security-strategy-statement-1-year-on, accessed on 6 April 2017
Maude, F. (2013a) “Digital Britain, Digital India, Digital World”, *Gov.uk*, 12 September, https://www.gov.uk/government/speeches/digital-britain-digital-india-digital-world, accessed on 21 March 2017
Maude, F. (2013b) “Cyber Security Information Sharing Partnership”, *Gov.uk*, 27 March, https://www.gov.uk/government/speeches/cyber-security-information-sharing-programme, accessed on 6 April 2017
Maude, F. (2014a) “Govnet Cyber Security Summit 2014: Francis Maude”, *Gov.uk*, 20 November, https://www.gov.uk/government/speeches/govnet-cyber-security-summit-2014-francis-maude, accessed on 21 March 2017

Maude, F. (2014b) “Francis Maude on the Launch of CERT-UK”, *Gov.uk*, 31 March, https://www.gov.uk/government/speeches/francis-maude-on-the-launch-of-cert-uk, accessed on 21 March 2017
Maude, F. (2014c) “Cyber Security: City Week 2014”, *Gov.uk*, 31 March, https://www.gov.uk/government/speeches/cyber-security-city-week-2014, accessed on 21 March 2017
Maude, F. (2014d) “Francis Maude Speech at Payments Council Cyber Security Seminar”, *Gov.uk*, 30 October, https://www.gov.uk/government/speeches/francis-maude-speech-at-payments-council-cyber-security-seminar, accessed on 21 March 2017
Maude, F. (2014e) “Francis Maude Speech at Cyber Security Challenge Masterclass”, *Gov.uk*, 13 March, https://www.gov.uk/government/speeches/francis-maude-speech-at-cyber-security-challenge-masterclass, accessed on 6 April 2017
May, T. (2011a) “Terrorism: Home Secretary’s Speech to the Council on Foreign Relations”, *Gov.uk*, 16 September, https://www.gov.uk/government/speeches/terrorism-home-secretarys-speech-to-the-council-on-foreign-relations, accessed on 5 April 2017
May, T. (2011b) *Hansard Volume 536*, 21 November, Intelligence and Security Committee, https://hansard.parliament.uk/Commons/2011-11-21/debates/11112126000001/IntelligenceAndSecurityCommittee?highlight=cyber%20terrorism, accessed on 11 April 2017
May, T. (2014) “Home Secretary’s Defence and Security Lecture”, *Gov.uk*, 24 June, https://www.gov.uk/government/speeches/home-secretarys-defence-and-security-lecture, accessed on 21 March 2017
May, T. (2015) “Home Secretary: Publication of Draft Investigatory Powers Bill”, *Gov.uk*, 4 November, https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill, accessed on 6 April 2017
Maidment, J. (2017) “’Brute Force’ Cyber Attack on Parliament Compromised up to 90 Email Accounts”, *The Telegraph*, 25 June, http://www.telegraph.co.uk/news/2017/06/25/brute-force-cyber-attack-parliament-compromised-90-email-accounts/, accessed on 7 July 2017
Mazid, B. (2008) “Cowboy and Misanthrope: A Critical (Discourse) Analysis of Bush and bin Laden Cartoons”, *Discourse and Communication*, Vol.2 No.4, pp.433-457
McAfee. (2014) *Net Losses: Estimating the Global Cost of Cybercrime*, Santa Clara: Intel Security, MacAfee
McAlaney, J, J Taylor and S Faily. (2015) “The Social Psychology of Cybersecurity”, *Working Papers of the Sustainable Society Network+: Conference Proceedings, First International Conference on Cyber Security for Sustainable Society*, Vol.3, pp.96-10, .MP3 recording of panel available on request
McCarthy, K. (2016) *Hansard Volume 604*, 6th January, Flooding, https://hansard.parliament.uk/Commons/2016-01-06/debates/16010644000001/Flooding?highlight=cyber%20terrorism#contribution-16010644000753, accessed on 15th March 2017
McCormic, G. (2003) “Terrorist Decision Making”, *Annual Review of Political Science*, Vol.6, pp.473-507
McCulloch, J and S Pickering. (2009) “Precrime and Counterterrorism: Imagining Future Crime in the ‘War on Terror’”, *British Journal of Criminology*, Vol.49 No.5, pp.628-645
McKenna, B. (2004) “Critical Discourse Studies: Where to from Here?”, *Critical Discourse Studies*, Vol.1 No.1, pp.9-39
McKenzie, I. (2014) *Hansard Volume 576*, 4 March, Defence and Cyber-Security, https://hansard.parliament.uk/Commons/2014-03-04/debates/14030455000001/DefenceAndCyber-Security?highlight=cyber%20terrorism, accessed on 15th March 2017
McDonald, M. (2008) “Securitisation and the Construction of Security”, *European Journal of International Relations*, Vol.14 No.4, pp.563-587
McLaughlin, M, K Osbourne and C Smith. (1995) “Standards of Conduct on the Usenet”, pp.90-111 in ed. S Jones, *Cybersociety: Computer-mediated Communication and Community*, London: Sage
McTague, T. (2014) “Computer Hackers Face Life in Prison under New Government Crackdown on Cyber Terrorism”, *Mail Online*, 5 June, http://www.dailymail.co.uk/news/article-2649452/Computer-hackers-face-life-prison-new-Government-crackdown-cyber-terrorism.html, accessed on 11 April 2018
Meisels, T. (2009) “Defining Terrorism – A Typology”, *Critical Review of International Social and Political Philosophy*, Vol.12 No.3, pp.331-351

Methmann, C and D Rothe. (2012) "Politics for the Day After Tomorrow: The Logic of Apocalypse in Global Climate Politics", *Security Dialogue*, Vol.43 No.4, pp.323-344
MI5. (2015) *Terrorism – Threat Levels*, https://www.mi5.gov.uk/home/the-threats/terrorism/threat-levels.html, accessed on 12 November, 2015
Miller, C. (2011) "Is it Possible and Preferable to Negotiate with Terrorists?", *Defence Studies*, Vol.11 No.1, pp.145-185
Milliken, J. (1999) "The Study of Discourse in International Relations: A Critique of Research and Methods", *European Journal of International Relations*, Vol.5 No.2, pp.225-254
Mirzoeff, N. (1999) *An Introduction to Visual Culture*, London: Routledge
Mitchell, J. (2017) "Jailed: Cyber-terrorist Samata Ullah Who Used James Bond-style Cufflinks to Hide Isis Propaganda", *Evening Standard*, 2 May, http://www.standard.co.uk/news/uk/jailed-cyberterrorist-samata-ullah-who-used-james-bondstyled-cufflinks-to-hide-isis-propaganda-a3528451.html, accessed on 9 May 2017
Mitchell, W. (1994) *Picture Theory: Essays on Verbal and Visual Representation*, Chicago: University of Chicago Press
Mitchell, W. (2011) *Cloning Terror: The War of Images, 9/11 to the Present*, Chicago: University of Chicago Press
Mirzoeff, N. (1999) *An Introduction to Visual Culture*, London: Routledge
Moller, F. (2007) "Photographic Interventions in Post-9/11 Security Policy", *Security Dialogue*, Vol.38 No.2, pp.179-196
Moon, M. (2014) *Hansard Volume 576*, 4 March, Defence and Cyber-security, https://hansard.parliament.uk/Commons/2014-03-04/debates/14030455000001/DefenceAndCyber-Security?highlight=cyber%20terrorists, accessed on 3 May 2017
Moore, D and T Rid. (2016) "Cryptopolitik and the Darknet", *Survival*, Vol.58 No.1, pp.7-38
Morgan, M, J Lewis and S Jhally. (1992) "More Viewing, Less Knowledge", pp.216-233 in ed. H Mowlana, G Gerber and L Schiller, *Triumph of the Image: The Media's War in the Gulf, a Global Perspective*, Boulder: Westview
Morgenthau, H. (2005) *Politics Among Nations*, New York: McGraw Hill
Morris, J. (2015) *Hansard Volume 597*, 25 June, Reports into Investigatory Powers, https://hansard.parliament.uk/Commons/2015-06-25/debates/15062549000001/ReportsIntoInvestigatoryPowers?highlight=cyber%20terror#contribution-15062549000265, accessed on 10 April 2017
Morris, N. (2015) "David Cameron to Seek US Help over Terrorists' Use of Facebook and Twitter", *Independent*, 15 January, https://www.independent.co.uk/news/uk/politics/david-cameron-to-seek-us-help-over-terrorists-use-of-facebook-and-twitter-9978680.html, accessed on 8 May 2017
Morris, R. (1993) "Visual Rhetoric in Political Cartoons: A Structuralist Approach", *Metaphor and Symbolic Activity*, Vol.8 No.3, pp.195-210
Phillips, L and M Jorgensen. (2002) *Discourse Analysis as Theory and Method*, London: Sage Publications
Morton, W. (2015) *Hansard Volume 602*, 17 November, G20 and Paris Attacks, https://hansard.parliament.uk/Commons/2015-11-17/debates/15111751000004/G20AndParisAttacks?highlight=cyber%20terrorists#contribution-15111751000307, accessed on 29 March 2017
Mott, G. (2016) "Terror from Behind the Keyboard: Conceptualising Faceless Detractors and Guarantors of Security in Cyberspace", *Critical Studies on Terrorism*, Vol.9 No.1, pp.33-53
Mulholland, H. (2010) "UK can no Longer Mount Military Operations like Iraq Invasion, Government Decides", *The Guardian*, 19 October, https://www.theguardian.com/politics/2010/oct/19/uk-can-no-longer-mount-military-operations-like-iraq, accessed on 8 May 2017
Murphy, J. (2010) *Hansard Volume 517*, 4 November, Strategic Defence and Security Review, https://hansard.parliament.uk/Commons/2010-11-04/debates/10110444000001/StrategicDefenceAndSecurityReview?highlight=cyber%20terrorism#contribution-10110444000389, accessed on 11 April 2017
Mythen, G, S Walklate and F Khan. (2012) "'Why Should We Have to Prove We're Alright?': Counter-Terrorism, Risk and Partial Securities", *Sociology*, Vol.47 No.2, pp.383-398
National Commission on Terrorist Attacks on the United States. (2004) *The 9/11 Commission Report*, New York: Norton and Company

National Intelligence Council. (2000) *The Global Infectious Disease Threat and its Implications for the United States*, Washington DC: US National Intelligence Council
Natter, A and M Chediak. (2017) "US Grid in 'Imminent Danger' from Cyber-Attack, Study Says", *Bloomberg*, 6 January, https://www.bloomberg.com/news/articles/2017-01-06/grid-in-imminent-danger-from-cyber-threats-energy-report-says, accessed on 27 March 2018
Nayak, M. (2006) "Orientalism and 'Saving' US State Identity after 9/11", *International Feminist Journal of Politics*, Vol.8 No.1, pp.42-61
Nayak, M and C Malone. (2009) "American Orientalism and American Exceptionalism: A Critical Rethinking of US Hegemony", *International Studies Review*, Vol.11 No.2, pp.253-276
Neumann, P. (2009) *Old and New Terrorism*, Cambridge: Polity Press
Neville-Jones, P. (2010) *Hansard Volume 721*, 2 November, Intellectual Assets: Crime, https://hansard.parliament.uk/Lords/2010-11-02/debates/10110262000452/IntellectualAssetsCrime, accessed on 11 April 2017
Neville-Jones, P. (2011a) "Pauline Neville Jones: Speech on CONTEST to the Cityforum", *Gov.uk*, 28 February, https://www.gov.uk/government/speeches/pauline-neville-jones-speech-on-contest-to-the-cityforum, accessed on 5 April 2017
Neville-Jones, P. (2011b) "Tackling Online Jihad: Pauline Neville-Jones's Speech", *Gov.uk*, 31 January, https://www.gov.uk/government/speeches/tackling-online-jihad-pauline-neville-joness-speech, accessed on 24 April 2017
Neville-Jones, P. (2014) *Hansard Volume 751*, 30th January, Scotland: Independence Referendum, https://hansard.parliament.uk/Lords/2014-01-30/debates/14013072000875/ScotlandIndependenceReferendum?highlight=cyber%20terrorism, accessed on 15th March 2017
Nias, D. (1979) "Desensitisation and Media Violence", *Journal of Psychosomatic Research*, Vol.23, pp.363-367
Nielsen, J. (2016) "The Distribution of Users' Computer Skills: Worse Than You Think", *Nielsen Norman Group*, 13 November, https://www.nngroup.com/articles/computer-skill-levels/, accessed on 24 April 2017
Nietzsche, F. (1982) *Die Frohliche Wissenschaft*, Frankfurt am Main: Insel Verlag
Nietzsche, F. (1999) "On Truth and Lying in a Non-Moral Sense", in ed. R Geuss and R Speirs, *The Birth of Tragedy and Other Writings*, Cambridge: Cambridge University Press
Nilges, M. (2010) "The Aesthetics of Destruction: Contemporary US Cinema and TV Culture", pp.23-34 in ed. J Birkenstein, A Froula and K Randell, *Reframing 9/11: Film, Popular Culture and the War on Terror*, New York: Continuum Publishing
Norris, M. (1994) "Only the Guns have Eyes: Military Censorship and the Body Count", pp.285-300 in ed. S Jeffords and L Rabinovitz, *Seeing Through the Media: The Persian Gulf War*, New Brunswick: Rutgers University Press
O'Connor, T. (2011) "Cyberterrorism", *Megalinks in Criminal Justice*, http://www.drtomoconnor.com/3400/3400lect06a.htm, accessed on 22 March 2015
Oels, A. (2012) "From 'Securitisation' of Climate Change to 'Climatisation' of the Security Field: Comparing Three Theoretical Perspectives", pp.185-205 in ed. J Scheffran et al, *Climate Change, Human Security and Violent Conflict*, Berlin: Springer
Ofcom. (2015) "The UK is Now a Smartphone Society", 6 August, https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2015/cmr-uk-2015 accessed on 28 March 2018
Office for National Statistics. (2010) *Internet Access 2010: Households and Individuals*, Statistical Bulletin, available at: https://www.ons.gov.uk/ons/rel/rdit2/internet-access---households-and-individuals/historical-internet-access/internet-access-2010-households-and-individuals.pdf, accessed on 28 July 2017
Office for National Statistics. (2016) *Internet Users in the UK: 2016*, Statistical Bulletin, available at: https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2016/pdf, accessed on 28 July 2017
Office for National Statistics. (2017) *Internet Users in the UK: 2017*, Statistical Bulletin, available at https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2017, accessed on 26 March 2018
O'Hara, B. (2015) *Hansard Volume 602*, 24 November, Trident, https://hansard.parliament.uk/Commons/2015-11-

24/debates/15112439000001/Trident?highlight=cyber%20terrorism#contribution-15112439000630, accessed on 3 April 2017
Oliver, M, B Mares and J Cantor. (1993) "News Viewing, Authoritarianism, and Attitudes Toward the Gulf War", pp.145-164 in ed. R Denton, *The Media and the Persian Gulf War*, Westport: Praeger
O'Loughlin, B. (2011) "Images as Weapons of War: Representation, Mediation and Interpretation", *Review of International Studies*, Vol.37 No.1, pp.71-91
Opitz, S. (2011) "Conflicting Temporalities: Law in Times of Risk", *Behemoth*, Vol.4 No.2, pp.58-82
Oren, I and T Solomon. (2015) "WMD, WMD, WMD: Securitisation Through Ritualised Incantation of Ambiguous Phrases", *Review of International Studies*, Vol.41, pp.313-336
Osborne, A. (2016) "Davos: BT Chief Warns of Huge Rise in Cyberattacks", *The Times*, 21 January, http://www.thetimes.co.uk/tto/business/davos/article4670343.ece, accessed on 21 January, 2016
Osborne, G. (2013) *Hansard Volume 565*, 26 June, Spending Review, https://hansard.parliament.uk/Commons/2013-06-26/debates/13062665000002/SpendingReview?highlight=cyber%20terrorism#contribution-13062665000196, accessed on 11 April 2017
Osborne, G. (2015) "Chancellor's Speech to GCHQ on Cyber Security", 17 November, *Gov.uk*, https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security, accessed on 3 April 2017
Oxford English Dictionary. (2016a) "Discourse", http://www.oxforddictionaries.com/definition/english/discourse, accessed on 31 May 2016
Oxford English Dictionary. (2016b) "Metaphor", http://www.oxforddictionaries.com/definition/english/metaphor, accessed on 21 June 2016
Oxford English Dictionary. (2017a) "Unknown", https://en.oxforddictionaries.com/definition/unknown, accessed on 27 July 2017
Oxford English Dictionary. (2017b) "Complex", https://en.oxforddictionaries.com/definition/complex, accessed on 27 July 2017
Oxford English Dictionary. (2017c) "Catastrophic", https://en.oxforddictionaries.com/definition/catastrophic, accessed on 8 August 2017
Paganini, P. (2015) "Cyber Warfare – Cyber Space and the Status Quo Balance of Power; Dichotomy or Symphony? How Technology Backfires", *Security Affairs*, 12 February, http://securityaffairs.co/wordpress/33448/cyber-warfare-2/cyber-warfare-balance-of-power.html, accessed on 22 March 2015
Pantazis, C and S Pemberton. (2009) "Policy Transfer and the UK's 'War on Terror': A Political Economy Approach", *Policy and Politics*, Vol.37 No.3, pp.363-387
Papacharissi, Z. (2002) "The Virtual Sphere: The Internet as a Public Sphere", *New Media and Society*, Vol.4 No.1, pp.9-27
Parfitt, T. (2011) "Georgian Woman Cuts off Web Access to Whole of Armenia", *The Guardian*, 6 April, https://www.theguardian.com/world/2011/apr/06/georgian-woman-cuts-web-access, accessed on 10 November 2017
Paris, R. (2002) "Kosovo and the Metaphor War", *Political Science Quarterly*, Vol.117 No.3, pp.423-450
Parliament.uk. (2017) "Frequently Asked Questions: MPs", http://www.parliament.uk/about/faqs/house-of-commons-faqs/members-faq-page2/, accessed on 10 November 2017
Paterson, S. (2015) *Hansard Volume 602*, 24 November, Trident, https://hansard.parliament.uk/Commons/2015-11-24/debates/15112439000001/Trident?highlight=cyber%20terrorism#contribution-15112439000630, accessed on 3 April 2017
Patten, J. (2010) *Hansard Volume 720*, 27 July, Terrorist-asset Freezing etc Bill, https://hansard.parliament.uk/Lords/2010-07-27/debates/10072739000584/TerroristAsset-FreezingEtcBill(HL)?highlight=cyberterrorism#contribution-10072739000221, accessed on 10 April 2017
Patten, J. (2011) *Hansard Volume 732*, 15 November, London Olympic Games and Paralympic Games (Amendment) Bill, https://hansard.parliament.uk/Lords/2011-11-15/debates/11111569000499/LondonOlympicGamesAndParalympicGames(Amendment)Bill?highlight=cyber%20terrorism, accessed on 11 April 2017
Pattenden, M. (2015) "Step Inside the Mind of a Teenage Hacker", *The Times*, 29 October, http://www.thetimes.co.uk/tto/life/article4598980.ece, accessed on 8 February 2016

Parliament.uk. (2017) “Search Hansard”, ‘Electromagnetic Pulse’, search parameters 12 May 2010 to 24 June 2016, https://hansard.parliament.uk/search?startDate=2010-05-12&endDate=2016-06-24&searchTerm=Electromagnetic%20Pulse, accessed on 12 September 2017
Parveen, N. (2017) “Guantanamo UK? Durham Jail First to Have ‘Terrorist Only’ Wing”, *The Guardian*, 31 March, https://www.theguardian.com/society/2017/mar/31/guantanamo-uk-durham-jail-first-to-have-terrorists-only-wing, accessed on 18 July 2017
PBS. (2014) “Osama bin Laden v. The US: Edicts and Statements”, http://www.pbs.org/wgbh/pages/frontline/shows/binladen/who/edicts.html, accessed on 24 July 2017
Perlmutter, D. (1999) *Visions of War: Picturing Warfare from the Stone Age to the Cyber War*, New York: St Martin's Press
Petley, J. (2005) “Cannibal Holocaust and the Pornography of Death”, pp.173-185 in ed. G King, *The Spectacle of the Real*, Bristol: Intellect
Pew Research Center. (2015) *Climate Change Seen as Top Global Threat*, Washington: Pew Research Center
Post, J. (2007) *The Mind of the Terrorist*, New York: Palgrave Macmillan
Poulsen, K. (2008) “Did Hackers Cause the 2003 Northeast Blackout? Umm, No”, *Wired*, 29 May, http://www.wired.com/2008/05/did-hackers-cau/, accessed on 28 January 2016
Prensky, M. (2001) “Digital Natives, Digital Immigrants: Part 1”, *On the Horizon*, Vol.9 No.5, pp.1-6
Puar, J and A Rai. (2002) “Monster, Terrorist, Fag: The War on Terrorism and the Production of Docile Patriots”, *Social Text*, Vol.20, pp.117-148
Ramsay, G. (2015) “Why Terrorism can, but Should not be Defined”, *Critical Studies on Terrorism*, Vol.8 No.2, pp.211-228
Ramsbottom, D. (2013) *Hansard Volume 742*, 24 January, Nuclear Disarmament, https://hansard.parliament.uk/Lords/2013-01-24/debates/13012450000874/NuclearDisarmament?highlight=cyber%20terrorism#contribution-13012450000244, accessed on 11 April 2017
Rathmell, A. (1997) “Cyber-Terrorism: The Shape of Future Conflict?”, *The RUSI Journal*, Vol.142 No.5, pp.40-45
Reeves, B, B Detenber and J Steuer. (1993) “New Televisions: The Effects of Big Pictures and Big Sound on Viewer Responses to the Screen”, Paper presented at the conference of the International Communication Association, Washington DC, May
Reeves, B, M Lombard and G Melwani. (1992) “Faces on the Screen: Pictures or Natural Experience?”, Paper presented at the conference of the International Communication Association, Miami FL, May
Reid, J. (2010) *Hansard Volume 721*, 2 November, Intellectual Assets: Crime, https://hansard.parliament.uk/Lords/2010-11-02/debates/10110262000452/IntellectualAssetsCrime?highlight=cyber%20terrorists#contribution-10110262000036, accessed on 10 April 2017
Reynolds, D. (2002) “From World War to Cold War: The Wartime Alliance and Post-War Transitions, 1941-1947”, *The Historical Journal*, Vol.45 No.1, pp.223-224
Richards, A. (2014) “Conceptualising Terrorism”, *Studies in Conflict and Terrorism*, Vol.37 No.3, pp.213-236
Risse-Kappen, T. (1994) “Ideas do not Float Freely: Transnational Coalitions, Domestic Structures, and the End of the Cold War”, *International Organization*, Vol.48 No.2, pp.185-214
Ritchie, M. (2013) *Hansard Volume 571*, 3 December, https://hansard.parliament.uk/Commons/2013-12-03/debates/13120351000001/Cyber-Bullying?highlight=cyber%20terrorism, accessed on 11 April 2017
Roe, P. (2008) “Actor, Audience(s) and Emergency Measures: Securitisation and the UK’s Decision to Invade Iraq”, *Security Dialogue*, Vol.39 No.6, pp.615-635
Roe, P. (2012) “Is Securitisation a 'Negative' Concept? Revisiting the Normative Debate over Normal Versus Extraordinary Politics”, *Security Dialogue*, Vol.43 No.3, pp.249-266
Rodriguez, L and D Dimitrova. (2011) “The Levels of Visual Framing”, *Journal of Visual Literacy*, Vol.30 No.1, pp.48-65
Rogers, J. (2014) “Report on British Attitudes to Defence, Security and the Armed Forces”, *Yougov*, 25 October, https://yougov.co.uk/news/2014/10/25/report-british-attitudes-defence-security-and-arme/, accessed on 10 July 2017
Ronfeldt, D and J Arquilla. (2001) “Networks, Netwars, and the Fight for the Future”, *First Monday*, Vol.6 No.10, available at: http://firstmonday.org/ojs/index.php/fm/article/view/889/798, accessed on 24 July 2017

Rosen, L et al. (1987) “Session VII Computerphobia”, *Behaviour and Research Methods, Instruments and Computers*, Vol.19 No.2, pp.167-179
Rosen, L and P Maguire. (1990) “Myths and Realities of Computerphobia: A Meta-Analysis”, *Anxiety Research*, Vol.3, pp.175-191
Rosenbach, M, L Poitras and H Stark. (2013) “How the NSA Accesses Smartphone Data”, *Spiegel Online*, 9 September, http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html, accessed on 30 August 2017
Rosenfield, D. (2009) “Rethinking Cyber War”, *Critical Review*, Vol.21 No.1, pp.77-90
Rudisill, C, J Costa-Font and E Mossialos. (2012) “Behavioural Adjustment to Avian Flu in Europe During Spring 2006: The Roles of Knowledge and Proximity to Risk”, *Social Science and Medicine*, Vol.75 No.8, pp.1362-1371
Rumsfeld, D. (2002) “Press Conference, *NATO*, 7 June, http://www.nato.int/docu/speech/2002/s020606g.htm, accessed on 2 February 2016
Rushton, R. (2002) “What Can a Face Do? On Deleuze and Faces”, *Cultural Critique*, No.51, pp.219-237
Ryan, M. (2006) “Filling in the 'Unknowns': Hypothesis-Based Intelligence and the Rumsfeld Commission”, *Intelligence and National Security*, Vol.21 No.2, pp.286-315
Sales, R. (2005) “Secure Borders, Safe Haven: A Contradiction in Terms?”, *Ethnic and Racial Studies*, Vol.28 No.3, pp.445-462
Salter, M. (2008a) “Imagining Numbers: Risk, Quantification, and Aviation Security”, *Security Dialogue*, Vol.39 No.2-3, pp.243-266
Salter, M. (2008b) “Securitisation and Desecuritisation: A Dramaturgical Analysis of the Canadian Air Transport Security Authority”, *Journal of International Relations and Development*, Vol.11 No.4, pp.321-349
Sanger, D and M Mazzetti. (2016) “US Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict”, *New York Times*, 16 February, https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html, accessed on 14 September 2017
Sanger, D and W Broad. (2018) “Pentagon Suggests Countering Devastating Cyberattacks with Nuclear Arms”, *The New York Times*, January 16, https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html, accessed on 27 March 2018
Sarat, A, L Douglas and M Umphrey. (2007) ed. *Law and Catastrophe*, Stanford: Stanford University Press
Schafer, M, J Scheffran and L Penniket. (2015) “Securitisation of Media Reporting on Climate Change? A Cross-national Analysis in Nine Countries”, *Security Dialogue*, Vol.47 No.1, pp.76-96
Scharrer, E. (2008) “Media Exposure and Sensitivity to Violence in News Reports: Evidence of Desensitisation?”, *Journalism and Mass Communication Quarterly*, Vol.85 No.2, pp.291-310
Scharrer, E and G Blackburn. (2015) “Images of Injury: Graphic News Visuals’ Effects on Attitudes Toward the Use of Unmanned Drones”, *Mass Communication and Society*, Vol.18 No.6, pp.799-820
Schell, H. (1997) “Outburst! A Chilling True Story about Emerging-Virus Narratives and Pandemic Social Change”, *Configurations*, Vol.5 No.1, pp.93-133
Schott, M. (2013) “Resilience, Normativity and Vulnerability”, *Resilience*, Vol.1 No.3, pp.210-218
Schmid, A and A Jongman. (1988) *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*, New Brunswick: Transaction Books
Schmidt, E. (2010) “Google’s CEO: ‘The Laws are Written by Lobbyists”, *The Atlantic*, 1 October, http://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/#video, accessed on 20 July 2015
Schouten, P. (2014) “Security as Controversy: Reassembling Security at Amsterdam Airport”, *Security Dialogue*, Vol.45 No.1, pp.23-42
Schwab, N. (2015) “ISIS is Winning and Obama is at Fault: Just Two in 10 Americans Think the US is Winning the War on Terror”, *Mail Online*, 28 December, http://www.dailymail.co.uk/news/article-3376607/ISIS-winning-Obama-fault-Just-two-10-Americans-think-U-S-winning-war-terror.html, accessed on 22 February 2016
Scwarz, E. (2015) “Prescription Drones: On the Techno-Biopolitical Regimes of Contemporary ‘Ethical Killing’”, *Security Dialogue*, Vol.47 No.1, pp.59-75
Shannon, J. (2014) *Hansard Volume 576*, 4 March, Defence and Cyber-security, https://hansard.parliament.uk/Commons/2014-03-04/debates/14030455000001/DefenceAndCyber-Security?highlight=cyber%20terrorism, accessed on 3 April 2017

Shapiro, M. (1989) “Textualising Global Politics”, pp.11-22 in ed. J Der Derian and M Shapiro, *International/Intertextual Relations*, Lexington: Lexington Books
Sheldon, J. (2012) “State of the Art: Attackers and Targets in Cyberspace”, *Journal of Military and Strategic Studies*, Vol.14 No.2, pp.1-19
Shelley, L and J Picarelli. (2002) “Methods not Motives: Implications of the Convergence of International Organised Crime and Terrorism”, *Police Practice and Research*, Vol.3 No.4, pp.305-318
Shepherd, L. (2008) “Visualising Violence: Legitimacy and Authority in the 'War on Terror'”, *Critical Studies on Terrorism*, Vol.1 No.2, pp.213-226
Shepherd, L and J Weldes. (2009) “Security: The State (of) Being Free From Danger?”, pp.529-536 in ed. H Brauch, *Globalisation and Environmental Challenges*, Mosbach: Springer
Shilling, C. (1993) *The Body and Social Theory*, London: Sage
Shimko, K. (1994) “Metaphors and Foreign Policy Decision Making”, *Political Psychology*, Vol.15 No.4, pp.655-71
Shubert, A. (2011) “Cyber Warfare: A Different Way to Attack Iran’s Reactors”, *CNN*, 8 November, http://edition.cnn.com/2011/11/08/tech/iran-stuxnet/, accessed on 29 June 2016
Simpson, J and D Gardham. (2017) “ISIS Hacker who Hid Terror Files on Cufflinks is Jailed”, *The Times*, 3 May, https://www.thetimes.co.uk/article/isis-hacker-who-hid-terror-files-on-cufflinks-is-jailed-t8008sqph, accessed on 9 May 2017
Singer, P. (2009) *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, New York: Penguin
Sloterdijk, P. (1998) *Spharen I: Blasen*, Frankfurt am Main: Suhrkamp
Sluga, G. (1996) “Cold War Casualties: Ethnicity, Gender, and the Writing of History”, *Women's Studies International Forum*, Vol.19 Mo.1-2, pp.75-85
Sluka, J. (2011) “Death from Above: UAVs and Losing Hearts and Minds”, *Military Review*, pp.70-76
Smeets, M. (2018) “A Matter of Time: On the Transitory Nature of Cyberweapons”, *Journal of Strategic Studies*, Vol.41 No.1-2, pp.6-32
Smith, G. (2004) “Behind the Screens: Examining Constructions of Deviance and Informal Practices among CCTV Control Room Operations in the UK”, *Surveillance and Society*, Vol.2 No.2-3, pp.376-395
Smith, J. (2015) *Hansard Volume 767*, 3 December, Strategic Defence and Security Review, https://hansard.parliament.uk/Lords/2015-12-03/debates/15120364000830/StrategicDefenceAndSecurityReview?highlight=cyber%20terrorism#contribution-15120364000324, accessed on 15 March 2017
Smith, T. (2001) “Hacker Jailed for Revenge Sewage Attacks”, *The Register*, 31 October, http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/, accessed on 22 March 2015
Snetkov, A. (2017) “Theories, Methods and Practices – a Longitudinal Spatial Analysis of the (de)Securitisation of the Insurgency Threat in Russia”, *Security Dialogue*, Vol.48 No.3, pp.259-275
Snyder, J and K Ballentine. (1996) “Nationalism and the Marketplace of Ideas”, *International Security*, Vol.21 No.2, pp.5-40
Soames, N. (2015) *Hansard Volume 593*, 2 March, Defence and Security Review (NATO), https://hansard.parliament.uk/Commons/2015-03-02/debates/15030240000001/DefenceAndSecurityReview(NATO)?highlight=cyber%20terror, accessed on 21 March 2017
Solomon, T. (2012) “’I Wasn’t Angry, Because I Couldn’t Believe it Was Happening’: Affect and Discourse in Responses to 9/11”, *Review of International Studies*, Vol.38 No.4, pp.907-928
Solsman, J. (2013) “Netflix, Youtube Gobble up Half of Internet Traffic”, *CNET*, 11 November, https://www.cnet.com/news/netflix-youtube-gobble-up-half-of-internet-traffic/, accessed on 9 August 2017
Sontag, S. (2003) *Regarding the Pain of Others*, New York: Farrar, Straus and Giroux
Soshnikov, A. (2016) “Bears with Keyboards: Russian Hackers Snoop on West”, *BBC News*, 20 September, http://www.bbc.co.uk/news/world-europe-37409456, accessed on 2 August 2017
Soukup, C. (2002) “Television Viewing as Vicarious Resistance: The X-Files and Conspiracy Discourse”, *Southern Communication Journal*, Vol.68 No.1, pp.14-26
Spencer, A. (2010) *The Tabloid Terrorist: The Predicative Construction of New Terrorism in the Media*, Basingstoke: Palgrave Macmillan
Spencer, A. (2012) “The Social Construction of Terrorism: Media, Metaphors and Policy Implications”, *Journal of International Relations and Development*, Vol.15, pp.393-419

Spencer, R. (2011) “Dumped in the Desert: Gaddafi’s Yellowcake Stockpile”, *The Telegraph*, 25 September, http://www.telegraph.co.uk/news/worldnews/africaandindianocean/libya/8787721/Dumped-in-the-desert-...-Gaddafis-yellowcake-stockpile.html, accessed on 8 November 2017
Spillett, R. (2017) “Up to 10,000 Britons Signed up to ‘Dark Web’ Paedophile Network Paradise Village Before it was Shut Down After Being Targeted by Hackers”, *Mail Online*, 8 May, http://www.dailymail.co.uk/news/article-4485060/Thousands-Britons-used-dark-web-paedophile-network.html, accessed on 9 August 2017
Stanford School of Medicine. (2016) “Stanford Research into the Impact of Tobacco Advertising”, http://tobacco.stanford.edu/tobacco_main/images.php?token2=fm_st003.php&token1=fm_img0111.php&theme_file=fm_mt001.php&theme_name=Doctors%20Smoking&subtheme_name=Throat%20Doctors, accessed on 1 June 2016
Stahl, R. (2013) “What the Drone Saw: The Cultural Optics of the Unmanned War”, *Australian Journal of International Affairs*, Vol.67 No.5, pp.659-674
Stampnitzky, L. (2013) *Disciplining Terror: How Experts Invented Terrorism*, Cambridge: Cambridge University Press
Statista. (2017) “Number of Worldwide Internet Users from 2005 to 2017”, https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/, accessed on 26 March 2018
Statista. (2015b) “Number of Daily Internet Users in Great Britain from 2006 to 2015 (in million users)”, http://www.statista.com/statistics/275786/daily-internet-users-in-great-britain/, accessed on 28 October 2015
Steuer, J. (1993) *Defining Virtual Reality: Dimensions Determining Telepresence*, SRCT Paper No. 104, San Francisco: Stanford University
Stimson, G and R Lart. (1991) “HIV, Drugs, and Public Health in England: New Worlds, Old Tunes”, *International Journal of the Addictions*, Vol.26 No.12, pp.1263-1277
Stoll, C. (1995) *Silicon Snake Oil: Second Thoughts on the Information Highway*, New York: Doubleday
Stratton, A. (2011) “David Cameron Says Russia and US Must ‘Rebuild’ Relationship”, *The Guardian*, 12 September, https://www.theguardian.com/politics/2011/sep/12/david-cameron-russia-rebuild-relationship, accessed on 2 August 2017
Stritzel, H. (2007) “Towards a Theory of Securitisation: Copenhagen and Beyond”, *European Journal of International Relations*, Vol.13 No.3, pp.357-383
Stritzel, H. (2011) “Security, the Translation”, *Security Dialogue*, Vol.42 No.4-5, pp.343-355
Stritzel, H and S Chang. (2015) “Securitisation and Counter-securitisation in Afghanistan”, *Security Dialogue*, Vol.46 No.6, pp.548-567
Stuart, J. (1604) “A Counterblaste to Tobacco”, *The University of Texas*, https://www.laits.utexas.edu/poltheory/james/blaste/blaste.html, accessed on 1 June 2016
Taliharm, A. (2010) “Cyberterrorism: in Theory or in Practice?”, *Defence Against Terrorism Review*, Vol.3 No.2, pp.59-74
Taureck, R. (2006) “Securitisation Theory and Securitisation Studies”, *Journal of International Relations and Development*, Vol.9 No.1, pp.53-61
Taylor, J. (2014) *Hansard Volume 755*, 8th July, Serious Crime Bill, https://hansard.parliament.uk/Lords/2014-07-08/debates/14070883000515/SeriousCrimeBill(HL)?highlight=cyber%20terrorism, accessed on 15th March 2017
Taylor, M. (1998) *Hiding*, Chicago: Chicago University Press
Teasdale, J. (1977) “Psychological Treatment of Phobias”, pp.137-163 in ed. N Sutherland, *Tutorial Essays in Psychology*, London: Wiley
Teffer, P. (2015) “EU to Force Firms to Report Major Cyber Incidents”, *EUObserver*, 8 December, https://euobserver.com/digital/131427, accessed on 28 January 2016
TeleGeography. (2017) “Global Internet Map 2017”, http://www2.telegeography.com/global-internet-map, accessed on 15 August 2017
Terry, L. (1964) “The 1964 Report on Smoking and Health”, *National Library of Medicine*, https://profiles.nlm.nih.gov/ps/retrieve/Narrative/NN/p-nid/60, accessed on 1 May 2016
The Guardian. (2017) “Cyber-attack on Parliament Leaves MPs Unable to Access Emails”, 25 June, https://www.theguardian.com/politics/2017/jun/24/cyber-attack-parliament-email-access, accessed on 7 July 2017

The Telegraph. (2015) “Australian Airport Website Hacked by Islamic State”, 13 April, http://www.telegraph.co.uk/news/worldnews/islamic-state/11531794/Australian-airport-website-hacked-by-Islamic-State.html, accessed on 8 August 2017
The Telegraph. (2016) “British Air Strikes in Syria have Killed Just Seven Islamic State Fighters”, 19 February, http://www.telegraph.co.uk/news/uknews/defence/12164292/British-air-strikes-in-Syria-have-killed-just-seven-Islamic-State-fighters.html, accessed on 22 February 2016
Thomas, T. (2003) “Al-Qaeda and the Internet: The Danger of 'Cyberplanning'”, *Parameters*, Vol.33 No.1, pp.112-123
Thu-Nguyen, D and J Alexander. (1996) “The Coming of Cyberspace Time and the End of Polity”, pp.99-124 in ed. R Shields, *Cultures of Internet: Virtual Spaces, Real Histories, Living Bodies*, London: Sage
Torfing, J. (1999) *New Theories of Discourse: Laclau, Mouffe and Zizek*, Oxford: Blackwell
Torfing, J. (2005) “Discourse Theory: Achievements, Arguments, and Challenges”, pp.1-30 in ed D Howarth and J Torfing, *Discourse Theory in European Politics*, New York: Palgrave Macmillan
TorProject. (2015) “Some Statistics about Onions”, 26 February, https://blog.torproject.org/blog/some-statistics-about-onions, accessed on 9 August 2017
TorProject. (2017a) “Users”, *TorMetrics*, https://metrics.torproject.org/userstats-relay-country.html?start=2010-05-12&end=2016-06-24&country=all&events=off, accessed on 9 August 2017
TorProject. (2017b) “Traffic”, *TorMetrics*, https://metrics.torproject.org/bandwidth.html?start=2010-05-12&end=2016-06-24, accessed on 9 August 2017
Touhig, D. (2016) *Hansard Volume 773*, 23 May, Queen’s Speech, https://hansard.parliament.uk/Lords/2016-05-23/debates/1605234000428/Queen%E2%80%99SSpeech?highlight=cyber%20terrorist#contribution-1605241000038, accessed on 3 April 2017
Travis, A. (2015) “Crime Rate to Rise by 40% after Inclusion of Cyber-offences”, *Guardian*, 15 October, http://www.theguardian.com/uk-news/2015/oct/15/crime-rate-rise-cyber-offences, accessed on 28 October 2015
Travis, A, M Taylor and P Wintour. (2014) “David Miranda Detention at Heathrow Airport was Lawful, High Court Rules”, *The Guardian*, 19 February, http://www.theguardian.com/world/2014/feb/19/david-miranda-detention-lawful-court-glenn-greenwald, accessed on 23 January 2016
Tuastad, D. (2003) “Neo-Orientalism and the New Barbarism Thesis: Aspects of Symbolic Violence in the Middle East Conflict(s)”, *Third World Quarterly*, Vol.24 No.4, pp.591-599
Tucker, D. (1997) *Skirmishes at the Edge of Empire*, Westport: Praeger
UNDP. (1994) *Human Development Report 1994*, Oxford: Oxford University Press
Turkle, S. (2008) “Always-on/aways-on-you: The Tethered Self”, pp.121-137 in ed. J Katz, *The Handbook of Mobile Communications and Social Change*, Cambridge MA: MIT Press
USA Today. (2001) “Hollywood Think Tank Creating Terror Scenarios”, *USA Today*, 9 October, http://usatoday30.usatoday.com/news/sept11/2001/10/09/hollywood.htm, accessed on 16 August 2017
Vaizey, Ed. (2016) *FTSE 350 Cyber Governance Health Check Report 2015*, London: Department for Culture, Media and Sport
Valentine, G and S Holloway. (2002) “Cyberkids? Exploring Children’s Identities and Social Networks in Online and Offline Words”, *Annals of the Association of American Geographers*, Vol.92 No.2, pp.302-319
Vaughan-Williams, N and D Stevens. (2015) “Vernacular Theories of Everyday (in)Security: The Disruptive Potential of Non-Elite Knowledge”, *Security Dialogue*, Vol.47 No.1, pp.40-58
Victoroff, J. (2005) “The Mind of Terrorist: A Review and Critique of Psychological Approach”, *The Journal of Conflict Resolution*, Vol.49 No.1, pp.3-41
Virilio, P. (1988) “Interview with Jerome Sans”, *Flash Art*, Vol.138, pp.57-61
Vodafone. (2012) *The Internet Economy in the United Kingdom*, available at: https://www.vodafone.com/content/dam/group/policy/downloads/internet_economy_uk.pdf, accessed on 28 July 2017
Vogler, J. (2002) “The European Union and the 'Securitisation' of the Environment”, pp.179-198 in ed. E Page and M Redclift, *Human Security and the Environment*, Cheltenham: Edward Elgar
Vuori, J. (2008) “Illocutionary Logic and Strands of Securitisation: Applying the Theory of Securitisation to the Study of Non-Democratic Political Orders”, *European Journal of International Relations*, Vol.14 No.1, pp.65-99
Vuori, J. (2010) “A Timely Prophet? The Doomsday Clock as a Visualisation of Securitisation Moves with a Global Referent Object”, *Security Dialogue*, Vol.41 No.3, pp.255-277

Waever, O and B Buzan. (2007) “After the Return to Theory: The Past, Present, and Future of Security Studies”, pp.383-399, in ed. A Collins, *Contemporary Security Studies*, Oxford: Oxford University Press
Wagenaar, H. (2012) “Dwellers on the Threshold of Practice: The Interpretivism of Bevir and Rhodes”, *Critical Policy Studies*, Vol.6 No.1, pp.85-99
Walker, C. (2006) “Cyber-Terrorism: Legal Principle and Law in the United Kingdom”, *Penn State Law Review*, Vol.110 No.3, pp.625-665
Walker, R. (1993) *Inside/Outside: International Relations as Political Theory*, Cambridge: Cambridge University Press
Walt, S. (1991) “The Renaissance of Security Studies”, *International Studies Quarterly*, Vol.35 No.2, pp.211-239
Walters, W. (2004) “Secure Borders, Safe Haven, Domopolitics”, *Citizenship Studies*, Vol.8 No.3, pp.237-260
Waltz, K. (1990) “Realist Thought and Neorealist Theory”, *Journal of International Affairs*, Vol.44 No.1, pp.21-37
Wang, J. (2014) “Criticising Images: Critical Discourse Analysis of Visual Semiosis in Picture News”, *Critical Arts*, Vol.28 No.2, pp.264-286
Ward, J. “US No Longer at War with 'Terrorism'”, *Washington Times*, 7 August, http://www.washingtontimes.com/news/2009/aug/07/us-no-longer-at-war-with-terrorism/?page=all, accessed on 22 February 2016
Watson, J. (2005) “The Face of Christ: Deleuze and Guattari on the Politics of Word and Image”, *The Bible and Critical Theory*, Vol.1 No.2, pp.04.1-04.14
Watson, S. (2012) “'Framing' the Copenhagen School: Integrating the Literature on Threat Construction”, *Millennium: Journal of International Studies*, Vol.40 No.2, pp.279-301
Watt, N. (2015) “David Cameron Accuses Jeremy Corbyn of Being ‘Terrorist Sympathiser”, *The Guardian*, 2 December, https://www.theguardian.com/politics/2015/dec/01/cameron-accuses-corbyn-of-being-terrorist-sympathiser, accessed on 9 November 2017
Weimann, G. (2005) “Cyberterrorism: The Sum of All Fears?”, *Studies in Conflict and Terrorism*, Vol.28, pp.129-149
Weimann, G. (2016) “Going Dark: Terrorism on the Dark Web”, *Studies in Conflict and Terrorism*, Vol.39 No.3, pp.195-206
Weldes, J. (1999) *Constructing National Interests: The US and the Cuban Missile Crisis*, Minneapolis: University of Minnesota Press
Wellman, B and M Gulia. (1999) “Net Surfers Don’t Ride Alone: Virtual Communities as Communities”, pp.167-194 in ed. P Kollock and M Smith, *Communities and Cyberspace*, New York: Routledge
Welzer, H. (2002) *Das Kommunikative Gedachtnis. Eine Theorie der Erinnerung* [Communicative Memory: A Theory of Rememberance], Munich: C.H. Beck
Wendt, A. (1992) “Anarchy is What States Make of It: The Social Construction of Power Politics”, *International Organization*, Vol.46 No.2, pp.391-425
Wendt, A. (1995) “Constructing International Politics”, *International Security*, Vol.20 No.1, pp.71-81
Wertheim, M. (1999) *The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet*, New York: Norton
Wheeler, B. (2017) “Amber Rudd Accesses Tech Giants of ‘Sneering’ at Politicians”, *BBC News*, 2 October, http://www.bbc.co.uk/news/uk-politics-41463401, accessed on 10 November 2017
White House. (1987) *National Security Strategy of the United States*, Washington DC: White House
Whitehead, T. (2016) “Police Firearms Officers Trained by SAS to Shoot Terrorists in the Head”, *The Telegraph*, 1 January, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/12077459/Police-firearms-officers-trained-by-SAS-to-shoot-terrorists-in-the-head.html, accessed on 22 February 2016
Whiting, A. (2013) “Understanding, Locating and Constructing Cyberterrorism”, paper presented at the Cyberterrorism Project's Conference: A Multidisciplinary Conference on Cyberterrorism”, Birmingham 11-12 April 2013
Whitney, L. (2013) “Gartner: Global IT Spending to Hit $3.7 trillion in '13”, *CNET*, 3 January, http://www.cnet.com/news/gartner-global-it-spending-to-hit-3-7-trillion-in-13/, accessed on 28 October 2015
Wilhelmsen, J. (2017) “How Does War Become a Legitimate Undertaking? Re-Engaging the Post-Structuralist Foundation of Securitisation Theory”, *Cooperation and Conflict*, Vol.51 No.2, pp.166-183

Williams, C. (2011b) “Stuxnet: Cyber Attack on Iran ‘Was Carried out by Western Powers and Israel”, *The Telegraph*, 21 January, http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html, accessed on 29 June 2016
Williams, M. (2003) “Words, Images, Enemies: Securitisation and International Politics”, *International Studies Quarterly*, Vol.47 No.4, pp.511-532
Williams, M. (2011a) “The Continuing Evolution of Securitisation Theory”, pp.212-222 in ed. T Balzacq, *Securitisation Theory: How Security Problems Emerge and Dissolve*, New York: Routledge
World Steel Association. (2015) *Steel Statistical Yearbook 2015*, Brussels: Worldsteel
Zedner, L. (2007) “Pre-Crime and Post-Criminology?”, *Theoretical Criminology*, Vol.11 No.2, pp.261-281
Zeltzer, D. (1992) “Autonomy, Interaction, and Presence”, *Presence: Teleoperators and Virtual Environments* Vol.1 No.1, pp.127-132
Zetter, K. (2008) “Kaminsky on How he Discovered DNS Flaw and More”, *Wired*, 22 July, https://www.wired.com/2008/07/kaminsky-on-how/, accessed on 14 September 2017
Zizek, S. (2002) *Welcome to the Desert of the Real*, London: Verso
Zulaika, J and W Douglass. (1996) *Terror and Taboo: The Follies, Fables, and Faces of Terrorism*, Abingdon: Routledge
Zulaika, J. (2012) “Drones, Witches and Other Flying Objects: The Force of Fantasy in US Counterterrorism”, *Critical Studies on Terrorism*, Vol.5 No.1, pp.51-68
Zulaika, J. (2014) “Drones and Fantasy in US Counterterrorism”, *Cultural Research*, Vol.18 No.2, pp.171-187