Kent Academic Repository

Mott, Gareth (2016) *Terror From Behind the Keyboard: Conceptualising Faceless Detractors and Guarantors of Security in Cyberspace.* Critical Studies on Terrorism, 9 (1). pp. 33-53. ISSN 1753-9153.

Downloaded from
https://kar.kent.ac.uk/75950/ The University of Kent's Academic Repository KAR

The version of record is available from
https://doi.org/10.1080/17539153.2016.1147773

This document version
Author's Accepted Manuscript

DOI for this version

Licence for this version
UNSPECIFIED

Additional information

Versions of research works

Versions of Record
If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

Author Accepted Manuscripts
If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in *Title of Journal* , Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

Enquiries
If you have questions about this document contact ResearchSupport@kent.ac.uk. Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies).

Terror From Behind the Keyboard: Conceptualising Faceless Detractors and Guarantors of Security in Cyberspace

Gareth Mott

Division of Politics and International Relations, Nottingham Trent University, Nottingham, UK.

gareth.mott2014@my.ntu.ac.uk

Gareth Mott is a scholarship doctoral researcher at Nottingham Trent University. Gareth's primary research interests include critical security studies, critical terrorism studies, and cyber-security.

Terror From Behind the Keyboard: Conceptualising Faceless Detractors and Guarantors of Security in Cyberspace

By reflecting on active public-domain government documents and statements, this article seeks to develop securitisation theory's articulation of the dichotomy between legitimate and illegitimate violence as it is reflected in British government policy. This dichotomy has (re)developed through a process wherein GCHQ and MI5 are portrayed as 'faceless guarantors' of security, in Manichean juxtaposition to the discursively-created phantom cyberterrorists, who are presented as 'faceless detractors' of security. It has previously been stated that the terrorism discourse associated with the present 'War on Terror' is attributed, in part, to mechanics of fantasy. I argue that, within the securitised discourse of cyberterrorism, the limits of fantasy possesses a murky nuance, which in turn, allows for a deeper – or at least more entrenched – securitisation. The official discourse surrounding the intelligence services' online surveillance apparatus operates with a similar opaque quality, but this is upheld by securitising actors as a strength to be maintained.

Keywords: cyberterrorism, securitisation theory

Introduction

The term 'cyberterrorism' was first coined by Barry Collin in the 1980s (Brickey 2012), and has become a 'buzzword' not just in terrorism studies and cyber-security circles, but also – recognising cyberterror's prowess for eye-catching copy – within the media (Weimann 2005, 131; Gordon and Ford 2002; Jones 2005, 7). This media-friendly characteristic has perhaps encouraged a propensity to conflate cyberterrorism with hacking and cyberattacks more broadly (Taliharm 2010, 62-63), which has applied weight to the need for common conceptual understanding. Denning's testimony before the United States Congress' House Armed Services Committee offers one definition of the term. Accordingly, she 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". Crucially, "to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm

> to generate fear" (Denning 2000).

Hua and Bapna offer a similar definition, stressing the role of 'significance' in the scale of the attack, and the inducement of physical violence or the creation of panic (2012, 176). A clause for cyberterrorism appears in British law in the 2000 Terrorism Act, under which Section (2)(e) detailed attacks "designed seriously to interfere with or seriously to disrupt an electronic system" (National Archives 2000, 1); a clause that, Clive Walker contends, distinguished the dichotomy between 'costly nuisances' and bona fide 'cyberterrorism' (2006, 632).

Given the dearth of a cyberterrorist attack up to the point of writing, cyberterrorism can be considered to be a phenomenon that has been talked into existence (Conway 2005). Regardless, in the UK, cyberterrorism is arguably a securitised risk-based menace, articulated as a Tier One threat under the current *National Security Strategy* (Cabinet Office 2010, 27), and the term appears with a relatively high concentration within the news media (Jarvis, MacDonald, and Whiting 2015, 60). Securitisation theory has done much to invigorate discussion of the power of security discourses (Gad and Petersen 2011), and the theory certainly holds great potential for discussions of the exceptionalisation of a phenomenon that has yet to occur, as is the case with cyberterrorism. However, there is little material examining a broadened conception of violence, and the manner in which discursively-experienced violence forms identities of detractors and guarantors of security.

This article scrutinises British government statements, documents, and public polls issued between May 2010 and July 2015, to observe a discourse that has constructed threatening 'faceless detractors' of security, whilst simultaneously legitimising – or obscuring – the violence, risks, and liberty-diminishing implications of the 'faceless guarantors' of British national security. To begin, I first discuss how violence can be linked to identities that are implied when individuals engage with cyberspace. I then offer an analysis of the formation of faceless detractors of security, which is followed by an analysis of faceless guarantors of security and some concluding remarks. The 'detracting' entity considered in this article is the spectre of the cyberterrorist, and the 'guaranteeing' entities are the British intelligence services. The analysis is underpinned by securitisation theory, which is a pertinent approach given that a securitising discourse inherently offers a delineation between legitimate and illegitimate violence. Specifically, securitisation theory facilitates the critique regarding how discourses of 'facelessness' and security in cyberspace can be manifested in both positive and negative lights, but still operate simultaneously without apparent discursive contestation.

I will expand on the concept of facelessness at greater length throughout this article. Broadly, the tenets that make facelessness distinct include: the potential spatial distance between the source and target of the attack or surveillance, the difficulty and delay involved in determining the detractor or guarantor of security, and the inherent challenge of successfully capturing the violent aestheticism (for instance, in live television coverage, online news thumbnails, and front-page imagery in print media).

Understanding violence in fibre-optic cables

Conceptualising violence in fibre-optic cables may, on first appearance, seem counter-intuitive. One potential means for observing the violence implicated in the use of the internet for security-detracting purposes is to use a broader understanding of violence, chiefly, that concerning identification, both of the environment itself, and the individuals who operate within that environment. Concerning online phenomena, there is a precedent for drawing distinctions in this way; for instance, both academia and culture have demonstrated a tendency to draw a binary distinction between online and offline (or alternatively, ‘real’ and ‘unreal’) ‘worlds’. This is demonstrated when Mark Slouka stated that society was on a “road to unreality”, which would lead to “a world that exists only as a trick of the senses, a computer-induced hallucination” (1995, 2,5). Some believed that this dichotomy extended into society itself, wherein one could observe a ‘digital divide’, which was not a willed-into-existence segregation per se, but rather a natural divide between digital ‘natives’ (those who had experienced childhood or adolescence amidst the proliferation of the world-wide-web) and digital ‘migrants’ (those who did not) (Tapscott 1998). Marc Prensky (2001), who described the ‘digital natives’ as native speakers of the digital language of computers, roughly divided these groups between those who were born before 1980, and those who were born following that year. Certainly, such a black-and-white divide would seem contentious if rigorously applied, but we can ascertain from such literature a belief that the online ‘world’ is experienced differently by differing actors.

There is a tendency for ‘cyber’ to be used as a go-to prefix for phenomena associated with online-mediation; for instance, ‘cyber-law’, ‘cyber-crime’, ‘cyber-psychology’ and ‘cyberterrorism’ to name just a few examples. Simply put, when used as a prefix, ‘cyber’ denotes an online activity; a modem must be involved (Iqbal 2004, 398-399). Cyber is not limited to use as a prefix, however, and it can also be considered a verb; as O’Connor states, regarding cyber there is “always action, movement, evolving motivations, adventure and interaction when you cyber. It’s impossible to just *be* cyber … there’s no steady state of being cyber” (2011). One can also talk of a ‘cyberspace’; a space that ultimately exists as a global sphere of power, in a similar sense to land, sea, air and space, but is differentiated by its – perceived – ethereal nature. No one country or geographical entity can be denoted as a ‘cyberisland’ (Aaviskoo 2010). Unlike the other spheres of power, which can be considered finite, cyberspace “is an intangible, fluid and counterintuitive phenomenon that defies the neat categorizations of the other strategic domains”, with one of the most distinct differences being that cyberspace can be constantly replicated (Sheldon 2012, 3,13; see also Libicki 2007, 5-6).

Cyber-attacks delivered via the internet *can* have physical, and potentially violent consequences. There are three known examples of computer-mediated attack that have exhibited physical or kinetic consequences. In 2001, an Australian man, disgruntled after having a prospective job application rejected by his local council, successfully hacked the council's waste management system, leading 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 Iran nuclear facilities, to disrupt the contentious nuclear enrichment programme. This attack occurred despite fears of a 'new Chernobyl' (Fildes 2011). In 2014, it was disclosed that a cyberattack successfully led to infrastructural failures at a German steel mill (BBC 2014a; BSI 2014, 31).

In these kinds of cyber-attack, which were delivered remotely in the form of malware, the violence reflected in the method of delivery cannot be precisely the same, compared to other methods that require the perpetrator to be physically present at the locale of attack. The fibre-optic cables delivering the data packets of the attack transmit this data with rapidly blinking light. This light is theoretically visible, but it would simply be impossible for the human brain to either observe the rapidity of the blinking, or to comprehend what the light *means*, without being able to observe the data at either the server from which the data request was made, or the device that is receiving the packets. The aesthetic element of the violence is therefore different to that, say, of a hand-held firearm, where both victim and observer could theoretically observe the pulling of the trigger, the action of the hammer snapping forward to strike the primer, the subsequent spark igniting the gunpowder, and the propulsion of the bullet.

William Mitchell (2011) has argued that threatening phenomena that cannot be seen is more powerful than that which can be seen, on the basis that these kinds of unseen threats possess greater potential to activate the imagination (see also Andersen and Moller 2013). To elucidate this point, consider the example of a horror film, in which representational codes render the threat comprehensible as a result of its status as being hidden. If an audience fathoms the representational codes of a horror story, they will harbour expectations of their viewing experience prior to the full completion of the cinematic reel (O'Loughlin 2011, 86). If the unseen possesses a heightened potential to elucidate fear, this could have policy relevance, for instance in the case of anti-terror legislation. Psychological studies have indicated that fear elevates an individual's perception of risk (Lerner and Keltner 2000; 2001; Matthews and Macleod 1986). Given that there has yet to be a single catastrophic cyber-terrorist attack, one can imagine a form of *Live Free or Die Hard* (2007) effect, where fictional attacks 'fill-in' a pre-constructed narrative regarding the likely events in a tumultuous cyber-attack. Certainly, it is interesting that, due to a lack of historical grounding for visual narratives within the discourse of cyberterrorism and cyberwarfare, policy-making agents use spectre-raising terminology such as an ‘electronic Pearl Harbour’ to artificially construct a historical analogy (Bendrath 2003, 50).

An integral part of the toolkit one would require to access a critical comprehension of violence in fibre-optic cables could be a critical theory of violence. The OED definition of violence is: “Behaviour involving *physical force* intended to hurt, damage, or kill someone or something” (2015, author’s emphasis). But this definition appears self-limiting in the case of data packets delivered in binary code.

In his book, *Aspects of Violence: A critical theory*, Willem Schinkel (2010) proposes an alternative comprehension of violence. On the traditional conception of violence, he writes:

> “For the commonsense notion of violence – that of intentional physical hurt, imparted by one person upon another – is quite simply, by and large, the contemporary states definition of violence … language itself is a man’s tool by which certain things – certain violent things – can be omitted from the definition of violence by allusion to the familiarity and the conceptual realism present in most use of language. The very existence of a certain concept of violence seduces us into thinking that there is no violence outside the denotation and connotation of that concept”. (2010, 32-33).

Using the example of an inherent violence in the act of ordering a coffee from a café waiter, Schinkel argues that violence is the “political aspect of any situation”; essentially, the process by which there is a reduction of individuals, which, in this example, would be two individuals reduced to either customer or waiter. Were the waiter to physically strike the customer, violence would move to the foreground of the instance – and a bystander would be more likely to classify the situation as one of violence – but that would only be one aspect of the violence (ibid, 2010, 77). Schinkel’s distinction allows for a comprehension of violence that permits acts of violence to exist outside of kinetic, physical harm. Drawing on this understanding of violence, when scrutinising the case of fibre-optic cables, I suggest that the process of internet-mediated communication inherently entails a reduction of identities to client, server or peer; plus the context and content-specific reduction such as consumer, friend, colleague, or, indeed, hacker.

It is in this light that I observe the official British discursive construction of both faceless guarantors and faceless detractors of security. The distinction between identities that can either be subsumed under the broad conception of either a ‘detractor’, and a ‘guarantor’ of a thing to be securitised (in the the case of cyberterrorism this is likely to be critical infrastructure, or economic stability) is significant, because the act of making such a distinction inherently entails assumptions regarding the identity’s status as an (il)legitimate form of violence. I now outline the methodology of my analysis, and discuss my findings.

Method

Securitisation theory emerged from the Copenhagen School a quarter of a century ago (Waever 1989; 1995), and began to assimilate prominence following its application in *Security: A New Framework for Analysis* (Buzan, Wilde, and Waever 1998). Securitisation theory was formulated to offer a conceptualisation of security beyond limited military concerns, whilst still allowing for 'security' to be differentiated from other forms of politics (Waever 2010). In essence, securitisation theory maintains that security can be considered a speech act; rather than existing as an objective 'fact', security is summoned – although not created per se – through an utterance (McDonald 2008). As Waever states, by "uttering 'security', a state representative moves a particular development into a specific area, and thereby claims a special right to use whatever means are necessary to block it" (1995, 55). Revolving around an embodied threat – for instance a terrorist, a pirate, an illicit narcotic etc – the discourse of that threat enters a field dominated by 'security', in which a legitimate 'security speaking' unit is able to exclude political debate (Hellberg 2011). A successful securitisation creates a dichotomy where the referent object, or 'Self', needs to be protected from the existential threat or 'Other' (Herschinger 2011). A successful securitisation also ordains the values and behaviours that can be considered either acceptable or unacceptable (Abrahamsen 2005, 69), and, importantly, does not require *unanimous* acceptance from the audience in order to remain effective; indeed, disputing a securitisation can be viewed to endorse it as a legitimate entity (Oren and Solomon 2015). In essence, securitisation theory thus provides us with a means through which one can scrutinise the social construction of cyberterrorism as a particular type of threat to the security of the British state.

British discourses of faceless guarantors and detractors in cyberspace, like any discourse, offer a series of "codes and conventions that each individual needs to employ to make oneself comprehensible" (Hansen, 2006, 16). In a similar vein to the methodology articulated by Stuart Croft in his book, *Securitising Islam*, this article identifies key identity signs in securitising moves, as well as the signs in the responses to those securitising moves (2012, 94-104). Specifically, I engage with active government statements and policies. Consequently, the analysis centres around statements and documents produced in or after May 2010, during the tenure of the Coalition government and the current Conservative government, until July 2015. This article also scrutinises public polls that have previously been conducted concerning issues such as national threats and state surveillance, to ascertain the efficacy of the securitisation of cyberterrorism and the top-down establishment of faceless detractors and guarantors of security. Polls are revealing not only because of the public response provided in relevant surveys, but because the polls cannot be written in a social vacuum. The authors of a poll are inherent subjects of the dominant official discourse of the time – whether wittingly or not – and this inherently frames a (re)production of that discourse

(Solomon 2009, 281). For instance, a ‘tick all that apply’ poll concerning threats to the UK that includes terrorism, cyber-threats and climate change effectively acts to legitimate these phenomena as *potential* threats, and simultaneously silences or at least diminishes alternatives that are not included on the list.

This article uses a discourse analysis approach, on the basis that discourse functions “to produce social and political actors authorised to speak and act”, in a process that acts to exclude and silence other forms of representation (Jackson 2007, 234). Within discourse, identities and political policies are inherently inter-linked. Identities are articulated as the justification for policies, and they themselves are also (re)produced through the discourses (Hansen, 2006, 19). The two discursive identities considered – faceless detractors and faceless guarantors of security – are discourses that have operated simultaneously within the May 2010 to July 2015 timeframe, and in some instances may be considered linked. Nevertheless, each discourse cannot be considered dependent upon the other; if one of the official discourses were to dissipate, or to change significantly, this would not necessarily impact on the other. Faceless guarantors of security could exist in the absence of faceless detractors of security and vice versa. The tenet that is revealing – and forms the focus of this article – is that they nevertheless exist simultaneously, and are reflected, by official documents and texts, with radically different vocabularies, symbols, labels and signifiers. Documents appearing in the period between May 2010 and July 2015 were sourced through key-word searches for ‘cyberterror’, ‘cyberterrorism’, and ‘surveillance’ on the gov.uk, publications.parliament.uk and yougov.co.uk websites. I commenced analysis with the premonition that both ‘faceless’ detractors and guarantors of security *may* exist as discursive constructions between this time period. Specifically, I was looking for official discussion and documentation of threatening cyberterrorists that appeared abstract and general, given that ambiguousness could be seen as feeding the ‘faceless’ narrative. Regarding the construction of ‘faceless guarantors’ of security, I sought discussion and documentation that held MI5 and the Government Communications Headquarters’ (GCHQ) remote and largely classified surveillance methods as necessary for national security. I was also interested to observe any dissent that may appear within official engagement with these two narratives, as this could indicate either a fractured securitisation, or a movement towards de-securitisation.

By reflecting on both the securitising moves and the audience’s reception to the discourse of a threatening terrorist Other in cyberspace, this article traces “the contours of the meta-narrative and the extent to which it has become normalised through society; and to allow an examination of the ways in which securitisations become routinised in everyday life” (ibid, 100). The article is consequently posited within the securitisation literature that focuses on “a more banal form of securitisation”, which “is less the creation of special measures in exceptional circumstances and more the introduction of mundane policies and practices, technologies of security" (Baker-Beall 2009, 203). These mundane – or routine – practices normalise the identities of the majority and isolate the 'alien' (Bigo 2008a, 108), instigated by 'managers of unease' in what has been termed by Didier Bigo as a 'ban-opticon' (2008b). Conceptualising security in this manner allows us to examine "a new generative space of struggles between security professionals that produce common interests, an identical program of truth and new forms of knowledge" (ibid, 24-25). As Jef Huysmans explains, we can conceive of a series of 'little security nothings', which "are highly significant, since it is they rather than exceptional speech acts that create the securitising process" (2011. 377).

Faceless Detractors of Security

In this case, a 'faceless detractor' of security is not necessarily literally taken to be without-a-face (although that may be the case in certain contexts, for instance a cyberterrorist attack initiated by pre-programmed software that awaited a signal or spammed attacks). Rather, the 'faceless' aspect derives from the likely spatial distance between the attacker and the target, and the inherent inability to actively 'see' the face of the attacker; in essence, the inability to confidently attribute an identity to the perpetrator. Of course, *Skype* video calls, and online avatars on forums and messaging services are cases where facelessness is relinquished, but ultimately the level of transparency that users of the internet choose to exhibit is a conscious decision. With accessible encryption technologies such as Virtual Private Network (VPN) services and Tor-enabled browsers, users of the world-wide-web – including individuals who wish to conduct malicious, security-detracting attacks – can choose to operate a 'faceless' online identity. The ability of these technologies to obfuscate the true Internet Protocol Address (IP address) of internet users has been a source of frustration for America's National Security Agency (NSA) and Britain's GCHQ (Ball, Schneier and Greenwald).

News and media reporting on threatening internet-mediated phenomena concerning not just cyberterrorism but also hacking more broadly, is saturated with accompanying imagery that obfuscates the identity of the attacker; for instance, foreboding hands behind a keyboard set against a dark background, a singular individual or a group of individuals wearing the 'Anonymous' Guy Fawkes mask, or green numbers or letters sprawling across a dark screen in the style of those seen in *The Matrix* (1999). In popular media, such as the CBS show, *CSI: Cyber* (2015), there is a tendency to represent the fibre-optic chasm between the victim and perpetrator as a black void with rapidly-moving, brightly-coloured lines, shapes and symbols. Through their facelessness, these threatening entities represent a 'known unknown'. It is known that they exist, but the aesthetic realism is incomplete. An internet-mediated cyberterrorist attack cannot be photographed and reproduced in the same way as, for instance, footage of the second plane striking the World Trade Center (Norfolk 2012). This stifles people's ability to *see* the face of evil, which is a prevalent societal demand concerning a plethora of perpetrators, whether they be Osama bin Laden, Josef Fritzel, Andrey Lugovoy, Samantha Lewthwaite, or 'Jihadi John', in a process that nullifies concern towards the victim and inflates the will to understand the perpetrator and to retrace their steps (Schinkel 2010, 129).

The existence of a threatening detractor of security in cyberspace is cited by the government. 'International terrorism affecting the UK or its interests' and 'Hostile attacks upon UK cyber space' form two of the four Tier One threats facing the UK, listed in the guiding document for security priorities, the *National Security Strategy* (Cabinet Office 2010, 27). Whilst cyberterrorism is only explicitly mentioned briefly in section 0.18, it would not be unfair to suggest that the two threats are linked in terms of ethos when either terrorism or cyber-attacks are discussed throughout the document; for instance in a similar vein to the way in which the symbiotic threats of narcotics and terrorism can be discursively inferred without necessarily resorting to terminology such as 'narco-terrorism' (Bjornehed 2004). The *Cyber Security Strategy* (Cabinet Office 2011) followed a similar theme. In this document, the term 'terrorism' was used in reference to terrorist *use* of the internet more broadly; for instance, propaganda, recruitment and financing, rather than attacks on critical infrastructure per se. However, the vulnerability of British critical infrastructure was still stressed.

A POSTnote[1] published in September 2011, focusing specifically on cyber threats to British infrastructure, noted that "Cyber attacks have not caused physical disruption in the UK to date", and provided a brief overview of the different types of threat, as well as the common solutions to these threats (POST 2011, 1,3). A sober reflection on the perceived risk of death and bodily injury and physical asset damage to both large and small businesses was provided in the government document on insurance and the mitigation of cyber-risks. Figures four and five indicate that death and bodily injury were extremely unlikely (0.5-1%), as were physical damages to assets (1%-5% for large businesses, 0.5-1% for small businesses). In terms of projected severity, such attacks were noted as likely to impact annual profit, but unlikely to cause a balance sheet loss (Cabinet Office 2015a, 12-13). Overall, firms were portrayed as much more likely to experience more banal (although not benign) forms of cyber crime. Notably, 81% of large firms and 60% of small firms reported a cyber breach in 2014 (Cabinet Office 2015b), with another report suggesting that nearly 9 out of 10 large organisations suffered from some form of security breach, making breaches 'a near certainty' (Department for Business, Innovation and Skills 2015, 9). Small firms were believed to be vulnerable to the risk of assimilating 'myths'; particularly the assumption held by 22% of small firms, that they were less attractive cyber-attack targets compared to larger firms (Home Office

[1] A government report on research, including stakeholders and academia.

2015).

The terms ‘cyberterrorism’ and ‘cyberterrorist’ appear to have only appeared sporadically during the years for which searches were carried out. On 14 October 2010, Viscount Waverley stated that whilst “suicide bombings have been the weapon of choice in certain quarters, carefully targeted cyberattacks will be the weapon in tomorrow’s world” (Anderson 2010, column 693). On 7 February 2013, Mike Weatherley, Conservative MP for Hove expressed his concern that nuclear facilities needed to be protected from cyberterrorism, at an ‘unknown’ cost (2013, column 468). On 4 March 2014, Jim Shannon, DUP MP for Strangford stated that “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. column 811). On 3 December 2013, Margaret Richie, SDLP MP for South Down unhelpfully conflated cyber-bullying as a form of cyberterrorism (2013, column 824), although this is certainly noteworthy for demonstrating the flexibility with which policy-makers interpret cyberterrorism. Before standing down as MP for Sheffield Brightside and Hillsborough, David Blunkett gave an interview with the *Yorkshire Post*, in which he warned of the high level of threat entailed by cyberterrorism, suggesting that “now the threat is cyber. I strongly believe 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). Regardless, the engagement by MPs and Lords with the discourse of cyberterrorism appears markedly minimal, particularly when juxtaposed against the more prolific discussions and debates that have surrounded terrorism discourse more broadly.

It is worth reflecting on this apparent dearth of debate concerning cyberterrorism. On a general level, exploitation of technology for malicious purposes has certainly received parliamentary attention. If the key-word search is widened to include results for ‘hacking’, the quantity of returns exponentially increase; doubtless inflated by the *News International* phone hacking scandal (BBC 2014c). Given that cyberterrorism exists as a Tier One threat to national security, it is interesting that MPs and Lords have largely neither publicly spoken in support of its securitised status, nor publicly questioned it, particularly given the lack of cyberterrorist incident to-date. However, perhaps this is the prevailing reason for the lack of public discussion; the absence of an a priori cyberterrorist incident may inherently diminish expectations for the phenomenon to be discussed. Furthermore, as demonstrated by Margaret Richie’s comment, politicians do not necessarily agree on a common definition of what cyberterrorism *is*, thereby potentially diminishing a consensual confidence of definition that would otherwise facilitate a debate or discussion. The conflation of cyberterrorism with other threatening phenomena indicates that the securitisation of cyberterrorism represents an ‘incantation’ of an ambiguous phrase (Oren and Solomon 2015). There is a strong case to suggest that cyberterrorism represents what David Kertzer (1988) would term an 'empty signifier', wherein calls to (re)securitise the threat are themselves rooted in the lack of common consensus regarding what cyberterrorism is. The status of cyberterrorism as an 'empty signifier' is an ample environment for an underlying role of fantasy – symptomatic of the broader epistemological crisis of counterterrorism efforts (Jackson 2015, 41) – where the discourse, mediated by the differing interpretations both within securitising actors and the audience, maintains the securitised reality.

What is the perception of the public towards the threat of cyberterrorism? Here polls are indicative but by no means definitive. In a September 2014 Yougov poll, responding to a 'tick all that apply' question on serious threats to national security, 69% of respondents 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'; thus placing cyber-attacks below immigration (55%), yet above other responses such as 'resource competition' (30%) and 'climate change or extreme weather' (28%) (Rogers 2014). Of course, the nature of these questions means that they are open to interpretation; threatening acts of cyberterrorism could technically fit under the categories of both domestic and foreign terrorism, as well as cyber-attacks. When prompted to select just one of the responses, 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' (ibid). The latter response is interesting, and is perhaps, again, symptomatic of the lack of a cyber attack in the UK to-date, whereas conventional terrorist attacks against the UK possess a history spanning several generations. In an international 'tick all that apply' poll conducted in July 2015, one can observe a markedly similar depiction; wherein 66% of UK respondents were very concerned about ISIS, and 34% very concerned about cyber-attacks on governments, banks or corporations (PewResearchCenter 2015). Unlike in the previous poll, the question did not forwardly indicate the *severity* of the cyber-attack, which may have contributed to the percentage difference when compared to the Yougov poll noted above. The prevalence of terrorism as the most-cited threat in these polls is perhaps not surprising, indeed, much has been written on the saturation of information inciting and maintaining fear of terrorism in Western societies. As Charlotte Heath-Kelly notes, there is a:

> "compulsion to faith in the apocalypse in the repeated warnings we receive to be vigilant – to watch out for suspicious persons/packages/activities. We are constantly alerted to remember the coming apocalypse, and are constantly made insecure by the technologies which are supposed to protect us" (2012, 357).

Drawing on the above discussion, perhaps the most remarkable aspect of the political discourse of cyberterrorism during the period May 2010 to July 2015 is the *lack* of representation, despite the phenomenon's status as a Tier One threat. Enshrined in its present securitised status by the *National Security Strategy*, the ambiguous nature of the threat of a potential cyberterrorist attack against the UK would appear to entrenched. This is not to suggest that the securitisation acts as a silencer of discussion in the political realm per se, rather, it is far more likely that the lack of an easily identifiable cyberterrorist incident to-date mitigates a will for general discussion, the scheduling of specific debates, or the direct attention of Special Committees. The marginal and infrequent attention given to cyberterrorism may suggest that the phenomenon need not necessarily be considered distinct from a monolithic threat of terrorism more broadly. However, it is nevertheless worth noting that this paucity of attention will have done little to alleviate the *facelessness* of the act of a terrorist using cyberspace to deliver an attack, nor contend the role of fantasy in the empty signifier underpinning this securitised discourse.

Faceless Guarantors of Security

A striking tenet of the constructed internet-mediated faceless detractors of security – of which cyberterrorists form one element – is that they exist simultaneously with the construction of faceless guarantors of security, for instance, GCHQ and MI5; both of which are British agencies that are legislated to conduct surveillance of the electronic communications and trails of British and foreign citizens. These agencies form part of a security apparatus that is in place to counter securitised threats, including cyberterrorism, amongst a myriad of others.

One would perhaps presume that a 'faceless guarantor' of security would be an oxymoron. Hille Koskela has written on the issue of faceless protectors in her gendered critique of urban CCTV surveillance, in which she suggests that the distance of the observation from the crime or maligned behaviour is problematic for intervention, and the 'facelessness' of the observer means that the observed is unable to form a perception concerning the reliability of their protection and the willingness-to-help in a harmful situation (2002, 267-268; see also Gray 2003, 326). There are few spheres in which one could say that being observed by a faceless figure is a *good* thing. Indeed, there is something inherently creepy and even voyeuristic in Google Chairman and CEO, Eric Scmidt's words: "With your permission you give us more information about you, your friends, and we can improve the quality of our searches … We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about" (2010). Julian Assange has repeatedly stated in televised interviews that "Google knows you better than you know yourself. Do you remember what you were searching for two days, three hours ago? Google does. It remembers. It knows you better than your mother" (2012). Applying weight to such statements is not facetious; indeed, it is known, and officially confirmed, that GCHQ is legally able to snoop on the use of Google by British citizens because the firm is based abroad (BBC 2014b).

How has the discourse of faceless guarantors of security been deliberated in the UK? Whilst this article is predominantly concerned with British government discourse following May 2010, it is certainly worth noting that the UK is exceptional in terms of the pre-existing relationship that has permeated between citizen and faceless authority, following the mass installation of CCTV cameras in the UK's urban spaces in the 1990s. Few states can claim to rival the UK's concentration of CCTV cameras, with The British Security Industry Association estimating that there are 4-5.9 million cameras in operation in the UK (BBC 2015). In the case of CCTV, this marked proliferation of an intrusive technology – which possesses disputed evidence of a meaningful impact on crime rates – has previously been termed the logic of the 'paranoia-of-the-watcher' (Holm 2009, 44); a resort to invasive technology on the basis of a *possibility* that it may assist in matters of state security. CCTV is not without flaws in its effectiveness; indeed, previous research has indicated that the operatives in the control rooms suffer from a human 'boredom factor', that leads them to leave the screens unattended for cigarette and toilet trips, to become engrossed in conversation with colleagues, and to read newspapers (Smith 2004).

The term 'faceless' in this instance denotes the from-afar (unless one resides in Cheltenham) nature of surveillance, as well as the literal facelessness of the transaction in question; wherein the discursive violence of 'watcher' and 'watched' is enacted. Through metadata analysis, the 'watched' is laid bare to see: where and when they have traveled, what they have purchased and the date of purchase, whom they have spoken to and when. With a relevant warrant – requested either for the individual 'watched' in question, or a bundled collection of targets – the content of those communications are also exposed. Consequently, this process represents a "technological vivisection, a digitised dismembering", as "the person is reduced to a transparency, like baggage, evacuated of vitality and materiality" (Amoore and Hall 2009, 452). Contrasting to this highly personalised transparency, the pervasiveness of news media imagery of the iconinic 'Doughnut', that houses some of GCHQ's operations, renders the facelessness of the watcher tangible in an aesthetic form. James Der Derian has previously linked security architecture to an aesthetic of the virtualisation and the disappearance of war, in which conventional warfare-based violence is supplanted with functional replacements such as terrorism, civil war, refugee and immigration war (1997; see also Virilio 1991). From the perspective of the watched, the watcher can therefore be considered a 'known unknown'; the public understands that the intelligence services exist, and that their digital trails may be surveilled, for instance via GCHQ's Tempora programme[2] (MacAskill et

[2] An operation that permits GCHQ to indiscriminately collect communications from fibre-optic cables, to watch the data live, or to store in databases.

al 2013). But, importantly, they do not know if their data will actually be used, or indeed how it will be used. This tenebrous uncertainty arguably stands as a technology of the panopticon (Foucault 1977). The faceless, abstract status of the intelligence services has, historically, been encouraged as the status quo by senior figures; for instance, as epitomised in the comments made by Sir Andrew Parker, the head of MI5, in 2013, when he stated that then-recent leaks concerning the methods of the intelligence services had been a 'gift' to terrorists (2013). Amidst the Snowden revelations, in which British intelligence services were implicated, defence officials sought to silence news media with a confidential D notice[3] (Halliday 2013). The webpage "How does an analyst catch a terrorist?" on GCHQ's website details a six-stage step-by-step walk-through of the process in which (using the case study of an overseas figure believed to be a potential Islamic State terrorist) an initial lead is investigated, leading to an identification and alert to MI5; although specific details such as the timeframe, technology or software used is characteristically absent (GCHQ 2015). With the intended purchase of Wynyard's *Persons of Interest* software[4] by British police forces (Harper 2015), the suggestion that the endeavour for counterterrorism is itself operating at degrees of fantasy, placing its foci on speculative futures – rather than present realities – appears to bear fruit (Frank 2015).

This year marked a partial lifting of the faceless veil, with the publishing of the report produced by the Intelligence and Security Committee of Parliament. For the first time, this document detailed the procedures that the intelligence services follow in order to conduct their surveillance, as well as the nature of the surveillance itself, and, whilst endorsing the necessity for the surveillance, the authors actively called for greater transparency; the lack of which, they stated, was against the public interest (ISCP 2015). Nevertheless, a key aspect of the information detailed in the document – the *scale* of surveillance, measured in searches and interceptions per day – was censored throughout the publicly-accessible version. This is a significant omission, that has the practical effect of denying the public, and representative figures (in essence, the participant audiences in involved in the securitisations justifying surveillance) the tools with which they could endorse or dispute the success and necessity of a sweeping online surveillance apparatus.

How has the issue of surveillance been conveyed in political statements? In November 2010, Theresa May, the Home Secretary, speaking in the context of the recently-published *National Security Strategy*, discussed the capabilities that the government would be seeking in order to combat the threat of terrorism. Whilst she stated the government's belief that no online service should be beyond the surveillance remit of the British intelligence agencies, she emphasised that

[3] A government notice that demands news editors refrain from publicising certain information, on the grounds of national security.

[4] Predictive software that analyses meta and content data against behavioural models, to determine the likelihood of individuals committing crimes or acts of terror.

capabilities should be proportionate, as “there is no value in security without liberty” (2010). In a CONTEST speech in July 2011, May spoke of the increasing use of online communication services by terrorists, and the necessity to continuously adapt the technology that the British counter-terrorism agencies have access to (2011). In November that year, David Cameron, citing ‘everyday’, ‘industrial-scale’ attempts to steal government secrets, emphasised the government’s £650 million towards improving British cyber defences, the requirement to ‘strike a balance’, and the need to avoid taking a ‘heavy handed’ approach (2011).

It is interesting that, during the tenure of the Coalition government, the respective leaderships of the Conservative and Liberal Democrat parties exhibited differing messages; whilst the Coalition necessarily had to produce unified policies, the discourse surrounding the issue of surveillance held notable nuances. For instance, in a speech in January 2011, Deputy Prime Minister Nick Clegg repeated the rhetoric of the threat posed by terrorism, but also warned that under the previous Labour government, legislation had been slipping into people’s lives, which, whilst increasingly perceived as mundane, was nevertheless chipping away at personal freedom; a process that, he claimed, represented the ‘real danger’ (2011). In a March 2014 speech at the Royal United Services Institute, entitled “Security and privacy in the internet age”, Clegg stated that:

> Privacy is integral to a free, fair and open society … the current framework assumes that the collection of bulk data is uncontroversial as long as arrangements for accessing it are suitably stringent. I don’t accept that … the public interest cannot be democratically determined behind closed doors. Decisions exercised in obscurity cannot be relied on to command public confidence when they come to light (2014).

In July that year, Cameron and Clegg gave a joint speech on the matter of the renewal of emergency legislation, which would ensure that communication firms could continue to retain rather than delete old data retrospectively, following a ruling by the European Court of Justice against a twelve-month retention of data for law enforcement purposes. In his speech, and the subsequent questions and answers section, Cameron repeatedly stressed the unquestionable need for the emergency exception legislation, based on his belief of the ‘real danger’ to the UK of not acting; whereas Clegg, whilst still acknowledging the present threats, took the opportunity to make – admittedly, probably political – swipes at the Conservatives for the so-called ‘Snooper’s Charter’ (which he had voted against), and stressed that the emergency legislation under discussion was temporary, and would require a full debate prior to its lapse at the end of 2016 (2014). Of course, this nuance could be symptomatic of political contention between the Conservative and Liberal Democrat elements of the Coalition. Indeed, it is of note that, in statements regarding surveillance and privacy, the Deputy Prime Minister did not dispute the securitised status of threats such as that emanating from domestic and international terrorism.

In a sense, this article is premature, as it is the debates surrounding the late 2016 deadline that will make possible either a discursive environment leading to legislation prioritising surveillance, or to legislation prioritising privacy. However, there were some sign-posts exhibited by Cabinet figures from the Conservative party both before and after the most recent general election. In January 2015, speaking to ITV News, Cameron made clear his intention to legislate consistently in favour of ensuring that, 'in extremis', no bona fide covert means of communication would be available to terrorists (Johnston 2015). The Prime Minister's usage of the term 'in extremis' when engaging with terrorism discourse arguably forms part of the linguistic tools that have been used to (re)securitise the threats that justify privacy and liberty diminishing practices. A similar signal was offered by Theresa May in an interview with the BBC in May 2015, in which she noted that increased surveillance powers were an example of legislation that had been blocked under the Coalition but would be pushed through in the Conservative government (Gayle 2015).

There is a marked paucity of dissent amongst the British public concerning the internet-mediated surveillance powers of the intelligence services. For instance, in a poll conducted in October 2013 – four months after the Edward Snowden revelations – 19% of respondents indicated that the intelligence services possessed too many powers, whereas 42% suggested that the balanced was 'about right', and 22% stated that the powers were insufficient (Dahlgreen 2013). In that same poll, 35% of respondents believed that the Snowden leaks were a 'good thing', whilst 43% believed that they were a 'bad thing'. However, in a poll conducted in April 2014, these figures were 46% 'good', 22% 'bad' and 31% 'don't know' (ibid; Jordan 2014). In a July 2014 poll, 83% of respondents noted that in practice, the security services probably have access to either 'almost everything', or a 'lot of' personal information about British citizens (Yougov 2014). In the same poll, when the question was posed normatively, 55% of respondents stated that the security services should have access to either almost everything, or a lot of personal information about normal people (ibid). In a January 2015 poll, which was commissioned shortly after the Parisian *Charlie Hebdo* attacks, 53% of respondents supported and 31% opposed the twelve-month data retention as outlined in the rejected 'Snooper's Charter'; furthermore, 63% of respondents trusted the intelligence serves to behave responsibly with information obtained via surveillance (Dahlgreen 2015). Civil liberties pressure groups such as Liberty and Big Brother Watch campaigned in the forum of a parliamentary committee earlier this year, against wide-ranging online surveillance powers, including bulk data collection, stating that even if it were categorically proven that data retention actively assisted the prevention of terrorist atrocities, the surveillance would not be justifiable because of the negative impact surveillance imparts on society (Parliament, 2015). Whilst this indicates that some dissent exists, such views cannot be considered to be held by the majority of the population, where a relative acceptance of mass surveillance prevails.

It is apparent that, during the period scrutinised, the surveillance of citizen's activities in cyberspace conducted by MI5 and GCHQ was regarded within the official discourse as a means by which securitised threats to national security could be mitigated. Those speaking on behalf of the intelligence services have sought to humanise their agents by emphasising their ‘normal’ domestic lives (Lobban 2014), but the methods that they employ in their capacity as guarantors of security exist under a partially-lifted veil. The apparent recourse to faceless technologies and premeditative approaches towards anti-crime, and counter-terrorism in particular, perpetuates worst-case-scenario projections and appears symptomatic of a process elucidated by Bill Durodie (2007). In essence, a public increasingly fearful of threats (with the effect of becoming more complicit in accepting or endorsing a given securitisation) increasingly seeks state narratives of reassurance for relief from the reality of threats emanating from the human society around them. Largely classified systems such as the Tempora programme are themselves a form of fantasy in the sense that they can be considered faceless technologies. Were the systems to become transparent and publicly accountable (for instance, publication of the number of searches conducted against meta data over a given time period, or the number and context of terrorist incidents that have been prevented due to technological premeditation over a given time period), the successes and failures of the technologies would be contestable. In this discourse, the ’faceless’ tenet of such surveillance is held as a *strength* to be upheld and respected, rather than a flaw to be addressed.

Conclusion

In this article, I have sought to offer a critique of the construction of ‘faceless’ detractors and guarantors of security, exhibited in official British cyber security discourse. Whilst the discourse may not use the term ‘faceless’, the facelessness is implicit. In the case of cyberterrorism, as a phenomenon that detracts from security but has no pre-existing real-term case studies from which to draw, the facelessness is further *implicated* by a paucity of a political will to discuss and represent the issue in public space. As previously stated, this lack of discussion may simply be a reflection of two factors. First, the absence of a cyberterror attack during the period under consideration. Second, a minimal level of confidence amongst members of parliament concerning technical aspects involved in cyber-threats. However, a securitisation, whilst in certain contexts necessary for the security of the nation, remains an inherently undemocratic phenomenon. Where a securitisation cannot be justified, the issue that is securitised should be returned to the political realm.

For as long as anonymity and obfuscation serves as a central component of the counter-terrorism and counter-crime efforts of the British intelligence services, faceless guaranteeing of security will remain a core tenet. This is not to suggest that such a veil is a negative creed, and indeed, the opinion polls noted above indicate that the public have broad faith that the capabilities of the intelligence services are both just and conducted with due care. However, it is of marked interest that the discourses of both good and bad (guaranteeing and detracting) facelessness operate simultaneously. Privacy is held as something to be surrendered in the endeavour for national security. Furthermore, by their very nature, both the technologies that retract online privacy and the temorality of the usage of such technologies remain within a shroud that is reminiscent of the panoptic.

Given the automatic expiration of emergency surveillance legislation at the end of 2016, it would be highly beneficial for a mature, open discussion to occur regarding *both* the faceless detractors and guarantors of security in cyberspace. This process should involve various stakeholders, including, but not necessarily limited to, communications firms, small and large businesses, and the public. The free cost and free access *Open University* eight-week Cyber Security course may help promote a greater confidence for discussion in this regard. Whilst, admittedly, perceptions of cyberterrorism are inherently likely to change in the event of its occurrence, it would arguably be beneficial for a more comprehensive legal definition of cyberterrorism, which, at present, is represented in Section (2)(e) of the 2000 Terrorism Act, under attacks "designed seriously to interfere with or seriously to disrupt an electronic system" (National Archives 2000, 1). This dubiety is highly susceptible to subjective interpretation, and, without multinational institutional guidelines, has arguably served to ferment the widely differing interpretations regarding 'what cyberterrorism is', elucidated by 118 terrorism researchers in a recent international survey conducted by Lee Jarvis and Stuart MacDonald (2015).

There are several future avenues of research that could bear interesting results if scrutinised under the lens of 'facelessness'. For instance, another phenomenon warranting consideration is that of the UK's cyberwarfare program; in 2013 the UK became the first state to publicly acknowledge the existence of its cyberwarfare program (Hammond 2013), but detailed information is non-existent. Undoubtedly, there are also parallels that can be drawn between the concepts of faceless detractors and guarantors of security elucidated here concerning cyberspace that could also relate to the increasing use of armed and unarmed drones in a security capacity by nation-states, which, as Zulaika states, also represent "a further step in the sensorial distancing from the targeted enemy" (Zulaika 2014, 177), with the drone operators able to act potentially thousands of miles away from their attacked or surveilled targets.

Cyber-mediated facelessness is becoming an increasingly common aspect of our experience of contemporary society. Much of this facelessness is banal, for instance, a firm sending an email to prospective clients or a consumer e-shopping items for delivery to Amazon lockers, but there are instances where facelessness presents issues for security. Where such potential contention arises, it is right that there should be a discussion of legitimate and illegitimate facelessness, because, entailed within such discourse, is a reflection of what we consider to be legitimate and illegitimate violence.

References

Aaviksoo, J. 2010. “Cyberattacks Against Estonia Raised Awareness of Cyberthreats”, *Defence Against Terrorism Review*, 3, 13-22

Abrahamsen, R. 2005. “Blair’s Africa: The Politics of Securitisation and Fear”, *Alternatives*, 30 (1), 55-81

Amoore, L and A Hall. 2009. “Taking People Apart: Digitised Dissection and the Body at the Border”, *Environment and Planning D: Society and Space,* 27 (3), 444-464

Andersen, R and F Moller. 2013. “Engaging the Limits of Visibility: Photography, Security and Surveillance”, *Security Dialogue*, 44 (3), 203-221

Anderson, J. 2010. *House of Lords*, 14 October, http://www.publications.parliament.uk/pa/ld201011/ldhansrd/text/101014-0003.htm

Assange, J. 2012. “Transcript: Interview with Julian Assange in the Ecuadorian Embassy”, *Wikileaks etc,* accessed 20 July 2015, http://wikileaksetc.blogspot.co.uk/2012/09/transcript-interview-with-julian.html

Baker-Beall, C. 2009. “The Discursive Construction of EU Counter-Terrorism Policy: Writing the ‘Migrant Other’, Securitisation and Control”, *Journal of Contemporary European Research,* 5 (2), 188-206

Ball, J., B Schneier and G Greenwald. 2013. “NSA and GCHQ Target Tor Network that Protects Anonymity of Web Users”, *Guardian*, 4 October, accessed 5 January 2016, http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption

BBC (British Broadcasting Company). 2014a. “Hack Attack Causes ‘Massive Damage’ at Steel Works’, 22 December, accessed 20 July 2015, http://www.bbc.co.uk/news/technology-30575104

BBC. 2014b. “Google and Facebook Can be Legally Intercepted, Says UK Spy Boss”, 17 June, accessed 20 July 2015, http://www.bbc.co.uk/news/technology-27887639

BBC. 2014c. “Phone-hacking Trial Explained”, 25 June, accessed 20 July 2015, http://www.bbc.co.uk/news/uk-24894403

Bendrath, R. 2003. “The American Cyber-angst and the Real World - Any Link?”, 49-73 in *Bombs and Bandwidth: The emerging relationship between IT and security,* ed. R Latham, New York: The New Press

Bigo, D. 2008a. “Security: A Field Left Fallow”, 93-114 in *Foucault on Politics, Security and War,* ed. M Dillon and A Neal, New York: Palgrave Macmillan

Bigo, D. 2008b. “Globalised (in)Security: The Field and the Ban-Opticon”, 10-48 in *Terror, Insecurity and Liberty, Illiberal Practices of Liberal Regimes after 9/11*, ed. D Bigo and A Tsoukala, New York: Routledge

Bjornehed, E. 2004. “Narco-Terrorism: The Merger of the War on Drugs and the War on Terror”, *Global Crime*, 6 (3-4), 305-324

Blunkett, D. 2015. “UK Not Ready for Cyber Terror Attacks – Blunkett”, *The Yorkshire Post*, 4 April, accessed 20 July 2015, http://www.yorkshirepost.co.uk/news/main-topics/politics/uk-not-ready-for-cyber-terror-attacks-blunkett-1-7192952

Brickey, J. 2012. “Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace”, *Combating Terrorism Center*, 23 August, accessed 20 July 2015, https://www.ctc.usma.edu/posts/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace

Buzan, B, J Wilde and O Waever. 1998. *Security: A New Framework for Analysis*, Boulder: Lynne Rienner

BSI (Federal Office for Information Security). 2014. *The Management of IT Security in Germany 2014*, Bonn: BSI

Cabinet Office. 2010. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, 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. *UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk,* London: Cabinet Office

Cabinet Office. 2015b. *2010 to 2015 Government Policy: Cyber Security*, accessed 20 July 2015, https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security

Cameron, D. 2011. “Prime Minister’s Speech on Cyberspace”, *Gov.uk*, 1 November, accessed 20 July 2015, https://www.gov.uk/government/news/prime-ministers-speech-on-cyberspace

Cameron, D and N Clegg. 2014. “PM and Deputy PM Speech on Emergency Security Legislation”, *Gov.uk*, accessed 20 July 2015, https://www.gov.uk/government/speeches/pm-and-deputy-pm-speech-on-emergency-security-legislation

Clegg, N. 2011. “Civil Liberties Speech: Deputy Prime Minister”, *Gov.uk*, 7 January, accessed 20 July 2015, https://www.gov.uk/government/speeches/civil-liberties-speech-deputy-prime-minister

Clegg, N. 2014. “Security and Privacy in the Internet Age”, *Gov.uk*, 4 March, accessed 20 July 2015, https://www.gov.uk/government/speeches/security-and-privacy-in-the-internet-age

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

Croft, S. 2012. *Securitising Islam: Identity and the Search for Security*, Cambridge: Cambridge University Press

Dahlgreen, W. 2013. “Little Appetite for Scaling Back Surveillance”, *Yougov*, accessed 20 July 2015, https://yougov.co.uk/news/2013/10/13/little-appetite-scaling-back-surveillance

Dahlgreen, W. 2015. “Broad Support for Increased Surveillance Powers”, *Yougov*, accessed 20 July 2015, https://yougov.co.uk/news/2015/01/18/more-surveillance-please-were-british

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*, accessed 20 July 2015, http://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm

Department for Business, Innovation and Skills. 2015. *Information Security Breaches Survey*, London: Department for Business, Innovation and Skills

Der Derian, J. 1997. “The Virtualisation of Violence and the Disappearance of War”, *Cultural Values*, 1 (2), 205-218

Durodie, B. 2007. “Fear and Terror in a Post-Political Age”, *Government and Opposition*, 42 (3), 427-450

Foucault, M. 1977. *Discipline and punish: The birth of the prison*, London: Penguin

Fildes, J. 2011. “Stuxnet Virus Targets and Spread Revealed”, *BBC News*, 15 February, accessed 20 July 2015, http://www.bbc.co.uk/news/technology-12465688

Frank, M. 2015. “Conjuring up the Next Attack: The Future-Orientedness of Terror and the Counterterrorist Imagination”, *Critical Studies on Terrorism*, 8 (1), 90-109

Gad, U and K Petersen. 2011. “Concepts of Politics and Securitisation Studies”, *Security Dialogue*, 42 (4-5), 315-328

Gayle, D. 2015. “Theresa May to Revive Her ‘Snooper’s Charter’ Now Lib Dem Brakes Are Off”, 9 May, accessed 20 July 2015, http://www.theguardian.com/politics/2015/may/09/theresa-may-revive-snoopers-charter-lib-dem-brakes-off-privacy-election

GCHQ (Government Communications Headquarters). 2015. “How Does an Analyst Catch a Terrorist?”, accessed 20 July 2015, http://www.gchq.gov.uk/what_we_do/how_does_an_analyst_catch_a_terrorist/Pages/index.aspx

Gordon, S and R Ford. 2002. “Cyberterrorism?”, *Computers and Security*, 21 (7), 636-647

Gray, M. 2003. “Urban Surveillance and Panopticism: Will We Recognise the Facial Recognition Society?”, *Surveillance and Society*, 1 (3), 314-330

Halliday, J. 2013. “MoD Serves News Outlets with D Notice over Surveillance Leaks”, *Guardian*, 17 June, accessed 20 July 2015, http://www.theguardian.com/world/2013/jun/17/defence-d-bbc-media-censor-surveillance-security

Hammond, P. 2013. “New Cyber Reserve Unit Created”, *Gov.uk*, 29 September, accessed 20 July 2015, https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit

Hansen, L. 2006. *Security as Practice: Discourse Analysis and the Bosnian War*, Abingdon: Routledge

Harper, T. 2015. “Theives Beware: Police IT May Predict Crime”, *Sunday Times*, 7 June, accessed 5 January 2016, http://www.thesundaytimes.co.uk/sto/news/uk_news/Society/article1565712.ece

Heath-Kelly, C. 2012. “Can We Laugh Yet? Reading Post-9/11 Counterterrorism Policy as Magical Realism and Opening a Third-Space of Resistance”, *European Journal on Criminal Policy and Research*, 18 (4), 343-360

Hellberg, U. 2011. *Securitisation as a Modern Strategy of Constructing Identity: 'Negative Proof Identity in the European Union*, Malmo: Malmo University

Herschinger, E. 2011. *Constructing Global Enemies: Hegemony and Identity in International Discourses on Terrorism and Drug Prohibition*, New York: Taylor and Francis

Holm, N. 2009. "Conspiracy Theorising Surveillance: Considering Modalities of Paranoia and Conspiracy in Surveillance Studies, *Surveillance and Society*, 7 (1), 36-48

Home Office. 2015. "Cyber Security 'Myths' Putting a Third of SME Revenue at Risk", accessed 20 July 2015, https://www.gov.uk/government/news/cyber-security-myths-putting-a-third-of-sme-revenue-at-risk

Hua, J and S Bapna. 2012. "The Economic Impact of Cyber Terrorism", *Journal of Strategic Information Systems*, 22 (2), 175-186

Huysmans, J. 2011. "What's in an Act? On Security Speech Acts and Little Security Nothings", *Security Dialogue*, 42 (4-5), 371-383

Intelligence and Security Committee of Parliament. 2015. *Privacy and Security: A Modern and Transparent Legal Framework*, Stationery Office: London

Iqbal, M. 2004. "Defining Cyberterrorism", *Journal of Computer Information Law*, 22, 397-408

Jackson, R. 2007. "An Analysis of EU Counterterrorism Discourse Post-September 11", *Cambridge Review of International Affairs*, 20 (2), 233-247

Jackson, R. 2015. "The Epistemological Crisis of Counterterrorism", *Critical Studies on Terrorism*, 8 (1), 33-54

Jarvis, L and S MacDonald. 2015. "What is Cyberterrorism? Findings From a Survey of Researchers", *Terrorism and Political Violence*, 27, 657-678

Jarvis, L, S MacDonald and A Whiting. 2015. "Constructing Cyberterrrorism as a Security Threat: a Study of International News Media Coverage", *Perspectives on Terrorism*, 9 (1), 60-75

Johnston, I. 2015. "David Cameron Pledges New 'Snooper' Charter' if He Wins General Election", 12 January, http://www.independent.co.uk/news/uk/politics/david-cameron-pledges-new-snoopers-charter-if-he-wins-election-9971379.html, accessed on 20.07.2015

Jones, A. 2005. "Cyber Terrorism: Fact or Fiction", *Computer Fraud and Security*, (6), 47-48

Jordan, W. 2014. "Snowen Revelations 'Good for Society'", *Yougov*, accessed 20 July 2015, https://yougov.co.uk/news/2014/04/18/reporting-nsa-revelations-good-society

Kertzer, D. 1988. *Ritual, Politics and Power*, New Haven: Yale University Press

Koskela, H. 2002. "Video Surveillance, Gender, and the Safety of Public Urban Space: 'Peeping Tom' Goes High Tech?", *Urban Geography*, 23 (3), pp.257-278

Lerner, J and D Keltner. 2000. "Beyond Valence: Toward a Model of Emotion-specific Influences on Judgement and Choice", *Cognition and Emotion*, 14 (4), 473-493

Lerner, J and D Keltner. 2001. "Fear, Anger, and Risk", *Journal of Personality and Social Psychology*, 81 (1), 146-159

Libicki, M. 2007. *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge: Cambridge University Press

Lobban, I. 2014. "Sir Iain Lobban's Valedictory Speech – as Delivered", *GCHQ*, 21 October, accessed 20 July 2015, http://www.gchq.gov.uk/press_and_media/speeches/Pages/Iain-Lobban-valedictory-speech-as-delivered.aspx

MacAskill, E, J Borger, N Hopkins, N Davies and J Ball. 2013. "GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications", *Guardian*, 21 June, accessed 20 July 2015, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Matthews, A and C MacLeod. 1986. "Discrimination of Threat Cues Without Awareness in Anxiety States", *Journal of Abnormal Psychology*, 95, 131-138

May, T. 2010. "Terrorism: Home Secretary's Speech on the Response to the Terrorist Threat", *Gov.uk*, 3 November, accessed 20 July 2015, https://www.gov.uk/government/speeches/terrorism-home-secretarys-speech-on-the-response-to-the-terrorist-threat

May, T. 2011. "Terrorism: Home Secretary's CONTEST speech", *Gov.uk*, 12 July, accessed 20 July 2015, https://www.gov.uk/government/speeches/terrorism-home-secretarys-contest-speech

McDonald, M. 2008. "Securitisation and the Construction of Security", *European Journal of International Relations*, 14 (4), 563-587

Mitchell, W. 2011. *Cloning Terror: The War of Images, 9/11 to the Present*, Chicago: University of Chicago Press

National Archives. 2000. *The Terrorist Act 2000*, Chapter 11, accessed 20 July 2015, http://www.legislation.gov.uk/ukpga/2000/11/contents

Norfolk, S. 2012. “Simon Norfolk in conversation with Andrew Hoskins”, Open Eye Gallery, Liverpool, 3 May, see A Hoskins. 2014. “A New Memory of War”, 179-191 in *Journalism and Memory*, ed. B Zelizer and K Tenenboim-Weinblatt, Basingstoke: Palgrave Macmillan

O’ Connor, T. 2011. “Cyberterrorism”, *Megalinks in Criminal Justice*, accessed 20 July 2015, http://www.drtomoconnor.com/3400/3400lect06a.htm

OED (Oxford English Dictionary). 2015. “Violence”, accessed 20 July 2015, http://www.oxforddictionaries.com/definition/english/violence

O’Loughlin, B. 2011. “Images as Weapons of War: Representation, Mediation and Interpretation”, *Review of International Studies*, 37 (1), 71-91

Oren, I and T Solomon. 2015. “WMD, WMD, WMD: Securitisation Through Ritualised Incantation of Ambiguous Phrases”, *Review of International Studies*, 41, 313-336

Parker, A. 2013. “MI5 chief: GCHQ Surveillance Plays Vital Role in Fight Against Terrorism”, *Guardian*, 9 October, accessed 20 July 2015, http://www.theguardian.com/uk-news/2013/oct/08/gchq-surveillance-new-mi5-chief

Parliament. 2015. “Oral Answers to Questions”, *House of Commons*, 16 March, accessed 20 July 2015, http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm150316/debtext/150316-0001.htm#1503165000004

Pew Research Center. 2015. *Climate Change Seen as Top Global Threat*, Washington: Pew Research Center

POST. 2011. *POSTnote: Cyber Security in the UK*, London: POST

Prensky, M. 2001. “Digital Natives, Digital Immigrants: Part 1”, *On the Horizon*, 9 (5), 1-6

Ritchie, M. 2013. *House of Commons*, 3 December, accessed 20 July 2015, http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131203/debtext/131203-0002.htm

Rogers, J. 2014. “Report on British Attitudes to Defence, Security and the Armed Forces”, *Yougov*, accessed 20 July 2015, https://yougov.co.uk/news/2014/10/25/report-british-attitudes-defence-security-and-arme

Schinkel, W. 2010. *Aspects of Violence: A critical theory*, Basingstoke: Palgrave Macmillan

Schmidt, E. 2010. “Google’s CEO: ’The Laws are Written by Lobbyists”, *The Atlantic*, 1 October, accessed 20 July 2015, http://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/#video

Sheldon, J. 2012. “State of the Art: Attackers and Targets in Cyberspace”, *Journal of Military and Strategy Studies*, 14 (2), 1-19

Shannon, J. 2014. *House of Commons*, 4 March, accessed 20 July 2015, http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm140304/debtext/140304-0002.htm

Slouka, M. 1995. *War of the Worlds: Cyberspace and the High-tech Assault on Reality*, New York: BasicBooks

Smith, G. 2004. “Behind the Screens: Examining Constructions of Deviance and Informal Practices among CCTV Control Room Operations in the UK”, *Surveillance and Society*, 2 (2-3), 376-395

Smith, T. 2001. “Hacker Jailed for Revenge Sewage Attacks”, *The Register*, accessed 20 July 2015, http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage

Solomon, T. 2009. “Social Logics and Normalisation in the War on Terror”, *Millennium: Journal of International Studies*, 38 (2), 269-294

Taliharm, A. 2010. “Cyberterrorism: in Theory or in Practice?”, *Defence Against Terrorism Review*, 3 (2), 59-74

Tapscott, D. 1998. *Growing Up Digital: The Rise of the Net Generation*, New York: McGraw-Hill

Virilio, P. 1991. Interview, *Art and Philosophy*, Milan: Giancarlo Politi Editore

Waever, O. 1989. *Security, the Speech Act: Analysing the Politics of a Word*, Working Paper 19, Copenhagen: Center for Peace and Conflict Research

Waever, O. 1995. “Securitisation and Desecuritisation”, 46-86 in *On Security*, ed. R Lipschutz, New York: Columbia University

Waever, O. 2010. *Taking Stock of a Research Programme: Revisions and Restatements of Securitisation Theory*, paper presented at the Annual Convention of the International Studies Association, New Orleans, 17-20th February

Walker, C. 2006. “Cyber-Terrorism: Legal Principle and Law in the United Kingdom”, *Penn State Law Review*, 110 (3), 625-665

Weatherley, M. 2013. *House of Commons*, 7 February, accessed 20 July 2015, http://www.publications.parliament.uk/pa/cm201213/cmhansrd/cm130207/debtext/130207-0002.htm

Weimann, G. 2005. “Cyberterrorism: The Sum of All Fears?”, *Studies in Conflict and Terrorism*, 28, 129-149

Yougov. 2014. *Yougov Survey Results*, 10-11 July, accessed 20 July 2015, http://d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/fx9mis4jz9/InternalResults_140711_data_information_access_security_W.pdf