3. United Kingdom: the constructed threat of cyber terrorism

Gareth Mott, *Kent University*

The Emergence of Political 'Cyberterrorism' Discourse in Britain

Although it has existed since the 1980s in a science fiction capacity[1], the term 'cyber terrorism' has not been conclusively defined either within academia or indeed amongst policymakers internationally[2]. There has been sustained debate as to what this term may mean and indeed whether we should refer to the term cyber terrorism at all. Nonetheless, cyber terrorism has been 'spoken into existence'[3]; it is a social construction of a threatening phenomenon, irrespective of legitimate claims that cyber terrorism has not yet occurred anywhere in the world[4]. This paper draws from – and builds upon – research and findings produced in the author's monograph, entitled *Constructing the Cyberterrorist: Critical Reflections on the UK Case*[5], in order to articulate the manner in which British political discourse and legislation has 'securitized' the threat of cyber terrorism. To securitize an issue is to discursively elevate it from a 'political' realm, instead transposing it into an exceptional 'security' realm in which extraordinary policies may be implemented or reinforced[6].

The UK is an interesting case study in relation to the construction of the threat of cyber terrorism, because the legislation under which incidences of cyber terrorism may be prosecuted pre-exists the discursive construction of the threat. Accordingly, such an activity would be prosecutable under the Terrorism Act 2000 in most instances, which, under Section (2)(e) of its definitions of terrorism includes attacks that are "designed seriously to interfere with or seriously disrupt an electronic system"[7]. An attack that may not fit the parameters of the Terrorism Act - for

[1] 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.

[2] 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; MacDonald, S, L Jarvis and S Lavis. (2019) "Cyberterrorism today? Findings from a follow-on survey of researchers", Studies in Conflict and Terrorism.

[3] 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.

[4] Kenney, M. (2015) "Cyberterrorism in a post-Stuxnet world", Orbis, Vol.59 No.1, pp.111-128.

[5] Mott, G. (2019) *Constructing the cyberterrorist: critical reflections on the UK case*, London: Routledge.

[6] Buzan, B, O Waever and J Wilde. (1998) *A new framework for analysis,* Boulder: Lynne Rienner.

[7] Legislation.gov.uk. (2000) *The Terrorism Act 2000,* chapter 11, www.legislation.gov.uk/ukpga/2000/11/contents, accessed on 7th March 2020; Walker, C. (2008) "Cyberterrorism: legal principle and the law in the United Kingdom", *Penn State Law Review*, Vol.110, pp.625-665.

instance, a serious or sustained attack perpetrated by a group not already included in the proscribed terrorist group list – could also be prosecutable under the Computer Misuse Act 1990[8]. However, it is important to stress that in British political discourse prior to 2010, the specific term 'cyber terrorism' was rarely, if ever, used. This status quo was perhaps indicative of the perception that whilst cyber terrorism was a distinct possibility, it was deemed improbable. In contrast, the perceived threat from nation-states – in particular China and Russia – was greater and therefore captured discussions around the protection of key British interests in cyberspace. In this vein, it was not surprising to find an excerpt from the 2009-2010 *Annual Report of the Intelligence and Security Committee*, which summarised part of a discussion with GCHQ representatives who, when questioned about the potential risk of cyber terrorism, dampened the threat on a relative basis[9].

This discursive political scene changed substantively in 2010. As has become standard protocol in the UK, the then-new British Coalition government published a new *National Security Strategy* and *Strategic Defence and Security Review*. By overtly listing the key threats facing the UK and ranking these according to their likelihood and their propensity for harm, these documents sought to be the public face of UK security priorities for the duration of the Coalition government. Collectively, these documents established – on a formal basis – the stature of cyber terrorism as a Tier One threat to the UK. 'Tier One' is a classification that the British government used to distinguish the threats to national security that – taking account of both likelihood and impact – were the highest priority. This *Strategy* specifically cited cyber terrorism as a serious threat to the UK. It detailed "cyber attack, including by other states, and by organized crime and terrorists" alongside 'international terrorism', 'international military crises', and 'major accidents or natural disasters' as a Tier One threat to British national security[10].

[8] Legislation.gov.uk. (1990) *The Computer Misuse Act 1990*, chapter 18, www.legislation.gov.uk/ukpga/19990/18/contents, accessed on 7th March 2020. The current maximum penalty under the CMA is ten years imprisonment and an unlimited fine. Breach of the Terrorism Act can receive a penalty of life imprisonment. Feasibly, in the context of the CMA, broader legislation can be applied, including the Homicide Act 1957 and Criminal Damage Act 1971, where harmful intent beyond the act of hacking can be evidenced.

[9] Intelligence and Security Committee. (2010) *Intelligence and security committee annual report 2009-2010*, London: Stationary Office. The report 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 the greatest threat of electronic attack to the UK comes from state actors, with Russia and China continued to pose the greatest threat".

[10] 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. 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 interconnected world). The *Review* highlighted that "the risks emanating from cyberspace (including the internet, wider telecommunications

This particular construction of the cyber terrorist threat was reiterated in the UK's first *Cyber Security Strategy*, which overtly raised the fear that the risk of terrorist application of significant cyber weapons was escalating[11]. This document also expressly distinguished between the general terrorist usage of online services (which it acknowledged were widespread) and the specific act of cyber terrorism itself (which it acknowledged had not yet occurred). The constructed securitization of the threat of cyber terrorism in the UK was reaffirmed by the updated 2015 version of the *National Security Strategy* and the 2016 version of the *Cyber Security Strategy*[12]. It is therefore of note that these public facing security documents served two functions with respect to the debates around the threat of cyber terrorism in the UK. Firstly, the documents served to legitimize the discussion of cyber terrorism; this now became a bona fide part of discussions around British security in the contemporary networked era. Secondly, the documents also served to define the parameters of the debate by imposing a particular interpretation of what cyber terrorism is, and by process of elimination, what it is also therefore *not*. To be specific, the British construction of the threat of cyber terrorism is concerned with the potential use of cyber weapons by terrorist entities against critical national infrastructure. This is cogently distinguished from broader uses of online services by terrorist organizations.

Elevating the Threat

With the parameters of the securitization of cyber terrorism in place, between May 2010 and June 2016 – the tenure of the Cameron Coalition and Conservative

and computer systems) of one of the four Tier One risks to national security. These risks include… the actions of cyber terrorists … these threats… are likely to increase significantly over the next five to ten years as our dependence on cyberspace deepens".

[11] Cabinet Office. (2011) *The UK cyber security strategy: protecting and promoting the UK in a digital world*, London: Cabinet Office. The *Cyber Security Strategy* 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 a can 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".

[12] Cabinet Office. (2015) *National security strategy and strategic defence and security review 2015: a secure and prosperous United Kingdom*, London: Cabinet Office; Cabinet Office. (2016) *National cyber security strategy 2016-2021*, London: Cabinet Office. The 2015 version of the *National Security Strategy* re-affirmed that: "the range of cyber actors threatening the UK has grown. The threat is increasingly asymmetric and global … nonstate actors, including terrorists and cyber criminals can use easily available cyber tools and technology for destructive purposes", and that these threats were 'significant and varied', including: "cyber terrorism … and disruption of critical national infrastructure as it becomes more networked and dependent on technology data held overseas". The 2016 *Cyber Security Strategy* provided a measured assessment of the escalating threat: "terrorist groups continue to aspire to conduct damaging cyber activity against the UK and its interests. The current technical capability of terrorists is judged to be low … the current assessment is that physical, rather than cyber, terrorist attacks will remain the priority for terrorist groups for the immediate future … the potential for a number of skilled extremist lone actors to emerge will also increase, as will the risk that a terrorist organisation will seek to enlist an established insider. Terrorists will likely use any cyber capability to achieve the maximum effect possible. Thus, even a moderate increase in terrorist capability may constitute a significant threat to the UK and its interests".

governments – discourse at the political level in the UK proliferated with the term ‘cyber terrorism’ and derivates thereof[13]. Several key findings can be raised. Notably, in over 100 distinct instances in which the threat of cyber terrorism was raised by Ministers, MPs and peers both inside and outside of the Chambers, there was no dissent. No political figure disputed the perception that cyber terrorism was an increasing threat. In some instances, the specter of cyber terrorism was cast in dire terms. Delivering a public-facing speech to GCHQ in November 2015, then-Chancellor George Osborne stated that:

> “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 … the pace of innovation of cyber attack is breathtakingly fast”[14].

Broadly, there was a consensus view that cyber terrorism referred to hypothetical instances in which terrorist organizations attack critical infrastructure with cyber weapons; indeed, overt references to the *Strategy* and *Review* documents were widespread. Delivering a *Cyber Crime* speech in March 2013, James Brokenshire, then a Parliamentary Under-Secretary for the Home Office noted 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”[15].

In a similar vein, Baroness Neville-Jones, speaking during a *Tackling Online Jihad* conference as the Security Minister, informed her audience that there was a discernible 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”[16].

[13] After June 2016 there has been a marked decline in the use of the term ‘cyber terrorism’ and derivatives thereof; although this may be indicative of a relative dearth of parliamentary time available to consider this and other issues within proposed legislation and standing orders. Since June 2016 there have been five instances in which the threat of cyber terrorism has been raised in either Chamber. These instances adhered to the same structure of the discourse that preceded them.

[14] Osborne, G. (2015) “Chancellor’s speech to GCHQ on cyber security”, *Gov.uk*, 17 November, https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security, accessed on 14 April 2020.

[15] Home Office and Brokenshire, J. (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 14 April 2020.

[16] Neville-Jones, P. (2011) “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 14 April 2020.

Given that the threat of cyber terrorism targets technology, and is enabled by technology, one might expect to see references to the technology itself in the exhibited discourse of the threat. Significantly however, the political discourse was overwhelmingly interested in the *identity construct* of purported cyber terrorist actors, rather than the weapon systems themselves. The weapon systems were instead left in a neutral discursive space; the weapons themselves were neither good nor bad, and this evaluation revolved on the identity of the person or group deploying them[17].

This author proposes that the constructed (and legislated) threat of cyber terrorism may have some indirect implications for digital rights and/or civil liberties, specifically with regard to the narrowing of the available political debate. Whilst the UK government has intermittently exhibited discourse relating to restricting access to, or use of, widespread encryption technologies, in an effort to restrict their untrammeled use by extremist organizations and other criminals, this discourse has largely not amounted to significant change in policy making terms[18]. With respect to the 'non-cyber terrorism' parameters of the Terrorism Act 2000, there are documented instances in which this legislation has been used in an aggressive fashion that arguably disproportionately undermined the civil liberties of individuals, particularly with respect to the application of Schedule 7[19]. Polling of the British populace has typically exhibited distinct – and persistent – sentiment on these issues. This polling has indicated that the British public value 'security' over 'privacy' with respect to online matters, and, even in the wake of the 2013 Edward Snowden revelations (which were described by then-MI5 chief Andrew Parker as a 'gift' for terrorists), the public held the view that intelligence agencies should have *greater* access to surveillance powers[20]. This public sentiment provided a backdrop

[17] Mott, G. (2019) *Constructing the cyberterrorist*.

[18] Travis, A. (2017) "Call for encryption ban pits Rudd against industry and colleagues", *The Guardian*, 26th March, https://www.theguardian.com/technology/2017/mar/26/amber-rudd-battle-tech-firms-cabinet-whatsapp-david-davis, accessed on 7th March 2020.

[19] Bowcott, O. (2016) "Terrorism Act incompatible with human rights, court rules in David Miranda case", *The Guardian*, 19th January, https://www.theguardian.com/world/2016/jan/19/terrorism-act-incompatible-with-human-rights-court-rules-in-david-miranda-case, accessed on 7th March 2020. Schedule 7 enables the police to stop, examine and detain passengers at transportation hubs. Individuals may be detained for up to six hours, and reasonable suspicion is *not* necessary.

[20] Dahlgreen, W. (2013) "Little appetite for scaling back surveillance", *Yougov*, 13 October, https://yougov.co.uk/topics/politics/articles-reports/2013/10/13/little-appetite-scaling-back-surveillance, accessed on 14 April 2020; Dahlgreen, W. (2015) "Broad support for increased surveillance powers", *Yougov*, 18 January, https://yougov.co.uk/topics/politics/articles-reports/2015/01/18/more-surveillance-please-were-british, accessed on 14 April 2020; Faulconbridge, G. (2013) "MI5 chief warns Snowden data is a 'gift' for terrorists", *Reuters*, 8 October, https://uk.reuters.com/article/uk-usa-security-britain/mi5-chiefwarns-snowden-data-is-a-gift-for-terrorists-idUKBRE99711K20131008, accessed on 14 April 2020; Jordan, W. (2014) "Snowden revelations 'good for society'", *Yougov*, 18 April, https://yougov.co.uk/topics/politics/articles-reports/2014/04/18/reporting-nsa-revelations-good-society, accessed on 14 April 2020.

of support for the Investigatory Powers Act 2016, which consolidated and legitimized existing large-scale surveillance practices.

However, with respect to the use of the legislation against instances of 'terroristic' electronic interference, there are few cases to speak of[21] and it would be difficult to categorically argue that the particular British construction of the threat of cyber terrorism has served to restrict digital rights or civil liberties. In contrast, as the annual UK's *Cyber Security Breaches Survey* routinely highlights, broader profit-driven hacking directly or indirectly impacting UK organizations is prolific, to the extent that many attacks are not reported and not investigated[22]. There is, of course, widespread political-level discourse in the UK concerning the threat of generic profit-driven cybercrime. It is notable, however, that the 'cyber terrorism' discourse in the UK appears to have operated on a standalone basis, separate to 'cybercrime' or indeed 'terrorism' more broadly construed. This author suggests that the construction of the threat of cyber terrorism in the UK is pre-emptive in the sense that it articulates the real possibility of terrorist usage of cyber weapons against critical national infrastructure. The discourse is also self-reflective (although not self-critical), in that it insulates itself against exhibiting limited shelf life by exclaiming that the threat of cyber terrorism is increasing over time. The constructed threat is therefore reflective of the Rumsfeldian[23] logic: the absence of evidence is not the evidence of absence.

Conclusion

This is not to say that the constructed threat does not have significant implications for freedom of debate and dissemination of knowledge in the UK. It is of note that the UK political discourse left the cyber weaponry itself in a neutral space; focusing instead on the 'bad' actors who may or may not deploy them. This has important ramifications in terms of legitimizing particular practices and also in silencing

[21] In May 2017, British media outlets reported the successful prosecution of a 'cyber terrorist', Samata Ullah. 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 in Kenya about online anonymity. *The Times* and the *Evening Standard* labelled him a 'new and dangerous breed of terrorist', a 'cyber terrorist'; *The Sun* labelled him a 'James Bond Jihadi'. However, Ullah did not conduct any known cyberattacks per se. See Simpson, J and D Gardham. (2017) "ISIS hacker who hid terror files on cufflinks is jailed", *The Times*, 3 May, www.thetimes.co.uk/article/isis-hacker-who-hid-terror-fileson-cufflinks-is-jailed-t8008sqph, accessed on 7th March 2020; Mitchell, J. (2017) "Jailed: cyberterrorist Samata Ullah who used James Bond-style cufflinks to hide ISIS propaganda", *Evening Standard*, 2nd May, www.standard.co.uk/news/uk/jailed-cyberterrorist-samata-ullah-who-used-james-bondstyled-cufflinks-tohide-isis-propaganda-a3528451.html, accessed on 7th March 2020; 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*, 2nd May, www.thesun.co.uk/news/3459144/james-bond-jihadi-samata-ullah-who-used-cybercufflinks-to-hide-isis-data-and-was-branded-new-breed-of-terrorist-is-caged/, accessed on 7th March 2020.
[22] Department for Digital, Culture, Media and Sport. (2019) *Cyber Security Breaches Survey 2019*, London: Department for Digital, Culture, Media and Sport.
[23] Rumsfeld, D. (2002) "Press conference by US Secretary of Defence, Donald Rumsfeld", *NATO*, 7th June, https://www.nato.int/docu/speech/2002/s020606g.htm, accessed on 7th March 2020.

debates that might otherwise be warranted. The UK was one of the first countries in the world to recognize that it rigorously develops a cyber offensive arsenal[24], but we have not had a public facing debate about the rationale and proportionality of these weapon systems. Cyber weapons are unlike any other weapon system. They do not weigh anything, they can be disseminated at the speed of light, they can be replicated with very little cost. They can also leak, to potentially devastating effect[25]. By ‘securitizing’ the threat of cyber terrorism, the UK political discourse arguably serves to legitimize UK state-oriented cyber weapon practices, whilst at the same time avoiding public-facing scrutiny of, and debate around, the weapon systems themselves. As British society becomes increasingly networked, with IT systems penetrating deeper into both the national economy and our daily lives, we may reach a point at which the (tacit) avoidance of a rational and mature public forum around the implications of cyber weapons becomes untenable.

[24] Blitz, J. (2013) “UK becomes first state to admit to offensive cyber attack capability”, *Financial Times*, 29th September, https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de, accessed on 7th March 2020.

[25] In April 2017, 300mb of cyber exploits for legacy Windows operating systems that had been developed by the National Security Agency (NSA) were released by the ‘Shadow Brokers’, who had been drip-feeding a cache of exploits for the preceding eight months. ‘Eternalblue’, a worm, was part of this cache and would later be re-purposed for the ‘Wannacry’ ransomware attack that affected thousands of organisations in the summer of 2017. See Goodin, D. (2017) “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 7th March 2020; Graham, C. (2017) “NHS cyber attack: everything you need to know about ‘biggest ransomware’ offensive in history”, *The Telegraph*, www.telegraph.co.uk/news/2017/ 05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/, accessed on 7th March 2020.