27 - Countering Terrorism via the Internet

Maura Conway and Clive Walker

Introduction

Terrorist and extremist movements have long employed every available mass communications technology. Examples range from the Irish Republican press in the nineteenth century,[1] Marighela's advice to his comrades in 1969 to use photocopiers to reproduce pamphlets and manifestos,[2] and Hizbollah's establishment of its Al Manar television station in the early 1990s,[3] through to the so-called 'Islamic State's' (IS) 'slickly' produced contemporary digital content.[4] For many years, scholars interested in the relationship between terrorism and media focused on the role of news media, particularly newspapers,[5] with terrorism often portrayed as involving the intentional manipulation of journalists. Terrestrial and satellite television has also directly impacted on terrorism,[6] with many terrorism spectaculars, including 9/11, appearing to be specifically choreographed for television.

The performative and propagandistic nature of terrorist acts is central to many of the wide variety of available definitions of terrorism. According to Schmid and De Graaf:

[1] See *R v John Mitchel* (1848) 6 StTr (NS) 599; *R v Charles Gavan Duffy* (1848) 2 StTr (NS) 795; *Martin v R* (1848) 3 Cox CC 318; *R v Grey* (1865) 10 Cox CC 184; *R v Sullivan and Pigott* (1868) 11 Cox CC 44.
[2] C Marighella, *Mini Manual of the Urban Guerrilla* (Abraham Guillen, Montreal 2002) 30.
[3] See B Saul and D Joyce, *International Approaches to the Regulation of al-Manar Television and Terrorism Related Content* (ACMA, Canberra 2010).
[4] See HJ Ingram, 'Three traits of the Islamic State's information warfare' 159 (6) *RUSI Journal* 4; J Klausen, 'Tweeting the Jihad: social media networks of western foreign fighters in Syria and Iraq' (2015) 38 *Studies in Conflict & Terrorism* 1.
[5] See M Conway, 'Introduction: Terrorism and contemporary mediascapes – reanimating research on media and terrorism' (2012) 5 *Critical Studies on Terrorism* 3.
[6] AP Schmid and J De Graaf, *Violence as Communication: Insurgent Terrorism and the Western News Media* (Sage, London 1982) 16; G Chaliand, *Terrorism: From Popular Struggle to Media Spectacle* (Saqi Books, London 1985) 13-14; BH Hoffman, *Inside Terrorism* (Columbia University Press, New York 1998) 136-137; SL Carruthers, *The Media at War* (MacMillan, Basingstoke 2000) 168.

> Terrorism cannot be understood only in terms of violence. It has to be understood primarily in terms of propaganda. Violence and propaganda have much in common. Violence aims at behaviour modification by coercion. Propaganda aims at the same through persuasion. Terrorism is a combination of the two.[7]

If the intention of terrorism is to induce terror, then it follows that the ultimate targets are the audience rather than direct victims.[8] Terrorism has, therefore, often been portrayed as a strategy of 'armed propaganda', calculated to generate maximum response amongst target audiences with the purpose of pressurising political leaders to accede to terrorists' demands.[9] Consequently, it is relatively unsurprising that governments have responded with robust legal restraints. Amongst the most prominent restrictions were those introduced in the Republic of Ireland (1976 – 1994) and the UK (1988 – 1994) arising from the Northern Ireland conflict and banning the broadcasts of Loyalist and Republican paramilitaries.[10]

The advent of the internet means that terrorists are no longer wholly reliant on the mass media to act as carriers and even intermediaries, because it affords otherwise unattainable prominence and meaning to their violence.[11] The internet now presents actors, whether mass movements or lone actors, with increased opportunities to globally propagate their own interpretations and messages.[12] A variety of other functions can be served by terrorist use of the internet, including information-gathering, planning, and even the commission of attacks usually through hacking and denial of service rather than the more spectacular catastrophes, such as aircraft falling from the sky through

[7] Schmid and De Graaf (n 6) 14. See also B de Graaf, *Evaluating Counterterrorism Performance* (Routledge, Abingdon 2011).
[8] Schmid and De Graaf (n 6) 15.
[9] M Stohl 'Demystifying the Mystery of International Terrorism' in CW Kegley (ed), *International Terrorism: Characteristics; Causes; Controls* (St Martin's, New York 1990) 93.
[10] See C Banwell, 'The courts' treatment of the broadcasting bans in Britain and the Republic of Ireland' (1995) 16 *Journal of Media Law & Practice* 21; S Kingston, 'Terrorism, the media, and the Northern Ireland conflict' (1995) 18 *Studies in Conflict & Terrorism* 203; J Horgan, 'Journalists and Censorship: a case history of the NUJ in Ireland and the broadcasting ban 1971-94' (2002) 3 *Journalism Studies* 377.
[11] See Carruthers (n 6) 170. These media roles sometimes resulted in threats of prosecution either for withholding information or for 'apology' of terrorism: C Walker, *Terrorism and the Law* (Oxford University Press, Oxford 2011) ch 8.
[12] See G Weimann, *New Terrorism and New Media* (Wilson Center, Washington DC 2014).

sabotaged air traffic control systems, that are often elaborated upon in media but have not materialised.[13]

In 1998, approximately half of the (then) 30 groups designated as 'Foreign Terrorist Organisations' under the US Antiterrorism and Effective Death Penalty Act of 1996 operated websites, including the Lebanese Hizbollah, the Sri Lankan Tamil Tigers, and others.[14] These early websites fulfilled largely a 'broadcast' function. Their content was tightly controlled by the terrorist organisations, and opportunities for interaction were negligible. By the next decade, online forums had become a popular format, especially amongst violent jihadis and allowed for much greater levels of interactivity.[15] Many forums remain active today, but jihadis and their online fans — 'jihobbyists'[16] — increasingly are having greater recourse to mainstream social media platforms.

IS and their online supporters have proven themselves to be prolific producers and disseminators of digital content.[17] IS does not have a single official website; instead 'official' IS online content emanates from several IS-affiliated content production entities or so-called 'media departments' (such as al-Furqan Media, al-Hayat Media Center) and is distributed via jihadi forums, but increasingly also via the major social media platforms and other content-hosting sites. In July 2014, the group released the first issue of its *Dabiq* magazine, similar in style to Al-Qa'ida in the Arabian Peninsula's *Inspire*.[18]

[13] See S Gordon and R Ford, 'Cyberterrorism?', (2002) 21 *Computers & Security* 636; G Weimann, 'Cyberterrorism: The Sum of All Fears?' (2005) 28 *Studies in Conflict & Terrorism* 129; PMS Sundaram and K Jaishankar, 'Cyberterrorism' in F Schmalleger and M Pittaro, *Crimes of the Internet* (Prentice Hall, Englewood Cliffs, New Jersey 2008).

[14] For Hizbollah's internet presence, see M Conway, 'Cybercortical Warfare: Hizbollah's Internet Strategy' in S Oates, D Owen, and R Gibson (eds), *The Internet and Politics: Citizens, Voters and Activists* (Routledge, London 2005); an analysis of the LTTE's websites is contained in S Tekwani, 'The Tamil Diaspora, Tamil Militancy, and the Internet' in KC Ho, R Kluver, and KCC Yang (eds), *Asia.Com: Asia Encounters the Internet* (RoutledgeCurzon, London 2003). Comparative analysis is to be found in M Conway, 'Terrorist web sites' in P Seib (ed), *Media and Conflict in the Twenty-First Century* (Palgrave MacMillan, New York 2005).

[15] See K Damphouse, 'The dark side of the web' in F Schmalleger and M Pittaro, *Crimes of the Internet* (Prentice Hall, Englewood Cliffs, New Jersey 2008); AY Zelin, *The State of the Global Jihad Online* (New America Foundation, Washington DC 2012).

[16] J Brachman, *Global Jihadism: Theory and Practice* (Routledge, London 2009) 19. For Irish Republican sites, see R Frennett and MLR Smith, 'IRA 2.0' (2012) 24 *Terrorism & Political Violence* 375. For right-wing groups, see German Federal Office for the Protection of the Constitution, *Right-wing Extremists and their Internet Presence* (Cologne, 2013)

[17] See n 4.

[18] See AF Lemieux et al, 'Inspire Magazine' (2014) 26 *Terrorism & Political Violence* 354.

The 'slick' and 'glossy' nature of IS' online content and its resultant potential attractiveness to, and resonance with, discontented 'digital natives' (young people who have grown up with the internet) has become a source of official apprehension.[19] However, the relationship between consumption of extremist online content, such as that produced by IS, and the adoption of extremist ideology or of recruitment to terrorism remains unproven.[20] From the producer perspective, this impact is of increasing importance.[21] A particular alleged outcome that has received utmost attention is the role of online jihadi content influencing young people to travel to Syria as 'foreign fighters' and 'jihadi brides', which gives rise to trepidation about their role in the conflict zone and even more so regarding their capacity for future terrorism upon their return home.[22]

The remainder of this chapter is concerned with describing and analysing the responses to the foregoing extremist uses of the internet. Much of the following is therefore concerned with what is called 'content control': efforts on the part of stakeholders to regulate what sort of material is available on the internet, including the removal of 'objectionable' materials currently accessible and the erection of barriers to the uploading of such materials in the future. The latter so-called 'negative' measures may be contrasted with more 'positive' approaches.[23] 'Negative' measures describe all those approaches that advocate for, or result, in the deletion or restriction of violent extremist online content and/or the legal sanctioning of its online purveyors or users; 'positive' measures refer to those online initiatives that seek to make an impact through digital engagement and education.

[19] See for example, See EU Counter-Terrorism Coordinator in consultation with the Commission services and the EEAS, *Foreign Fighters and returnees* (16002/14, Brussels 2014) 2-3.
[20] See Home Affairs Committee, *Roots of violent radicalisation* (2010-12, HC 1446) para 38; I von Behr and others, *Radicalisation in the Digital Era* (RAND, Santa Monica 2013); D Rieger, L Frischlich and G Bente, *Propaganda 2.0: Psychological Effects of Right-wing and Islamic Extremist Internet Videos* (Luchterhand, Munich 2013); DC Benson, 'Why the internet is not increasing terrorism' (2014) 23 *Security Studies* 293.
[21] See D O'Callaghan and others 'An analysis of interactions within and between extreme right communities in social media' (2013) *Ubiquitous Social Media Analysis* 8329, 88; A Fisher and N Prucha, 'The Call-up: The Roots of a Resilient and Persistent Jihadist Presence on Twitter' (2014) 4(3) *CTX Journal* (Online).
[22] See UNSCR 2178 of 24 September 2014.
[23] For comprehensive strategic statements in regard to cybersecurity, see Cabinet Office, *Cyber security strategy of the United Kingdom: safety, security and resilience in cyberspace* (Cm 7642, 2009); Cabinet Office, *The UK cyber security strategy: protecting and promoting the UK in a digital world* (London 2011); Department of Homeland Security, *National Strategy to Secure Cyberspace* (Washington DC 2003); Executive Order 13636, Improving Critical Infrastructure Cybersecurity; T Legrand, 'The citadel and its sentinels' in T Chen, L Jarvis, and S Macdonald (eds), *Cyberterrorism* (Springer, Heidelberg 2014).

Content control issues in general

Both Article 19 of the UN's Universal Declaration of Human Rights 1948 and Article 10 of the ECHR identify freedom of expression and the right to seek, receive, and impart information (including from foreign countries)[24] as fundamental human rights. These grants of right also recognise, however, that freedom of expression is counter-balanced by state-imposed limitations for the sake of, *inter alia*, 'public order' (UNDHR, article 29) or 'national security, territorial integrity or public safety, for the prevention of disorder or crime' (ECHR, Article 10(2)). This dichotomous international regime, in conjunction with states' widely differing social, political, and religious contexts, added to the absence of any comprehensive international law definition of terrorism,[25] opens many possibilities for variant interpretations and levels of tolerance.[26] Uncertainties can also arise through differences between the 'real' and 'cyber' worlds. Existing rules about speech, promulgated for application in the real world, *can* be applied to the internet, as adopted in the EU for racist speech.[27] However, it is arguable that the internet requires specific legislation tailored to its specific characteristics which impart differences in terms of risk and legal attributes. The risk factors include quantity (the number, spread, and easy accessibility of messages) as well as quality (the intensity and instantaneity of messages and the facility for personal dialogue). The special legal attributes include the complexities of trans-jurisdictional impact, the potential for anonymity, and the technical expertise and specialist equipment required to gather evidence.[28] These risk factors and legal attributes become especially troubling when the effects of online extremism may prove so pernicious.

In the light of these problems, many countries have introduced internet-content legislation, most of it hastily promulgated in the wake of specific terrorist events, such as 9/11 and 7/7. There may be some tangible benefits in terms of resolving the boundaries of forbidden conduct. However, there

[24] See *Khurshid Mustafa and Tarzibachi v Sweden* App no 23883/06, 16 December 2008 and more generally *Társaság a Szabadságjogokért v Hungary* App no 37374/05, 14 April 2009.
[25] See Chapter 2 (Saul).
[26] For guides, see U Sieber, and PW Brunst, *Cyberterrorism* (Council of Europe, Strasbourg 2007); MC Golumbic, *Fighting Terror Online* (Springer, New York 2008); Home Office, *Safeguarding Online: Explaining the Risk Posed by Violent Extremism* (London 2009); Y Akdeniz, *Freedom of Expression on the Internet* (Council of Europe Publishing, Strasbourg 2010); UN Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* (Vienna 2012).
[27] See European Commission, *Proposal for a Council Framework Decision on Combating Racism and Xenophobia* (Brussels 2001) 6, 8.
[28] See generally Y Akdeniz, C Walker, and D Wall, *The Internet, Law and Society* (Longman, London 2000); I Spiecker genannt Döhmann, 'The Difference between Online and Offline Communication as a Factor in the Balancing of Interests with Freedom of Speech' in CP Walker and RL Weaver, *Free Speech in an Internet Era* (Carolina Academic Press, Durham, NC 2013).

are also criticisms in terms of a disproportionately blanket 'surveillance society'[29] affecting the rights of all and not just suspects,[30] the dubious efficacy of many provisions, and the absence of more innovative responses. Even the security authorities appear dissatisfied with the regime, and so, as revealed by Edward Snowden, they allegedly practice 'dataveillance' on a vast scale in ways which may transgress the boundaries of legality.[31]

'Negative' online measures

Successful use of the internet for violent radicalisation and other violent extremist purposes is based on the assumption that both users and audiences have access to the messages communicated via the internet and also can interact. States therefore believe they can constrain the effectiveness of these cyber-based strategies by limiting user and audience access, either by *ex ante* or *post hoc* censorship of content (such as by criminal law or take-down measures) or by control over internet infrastructure (such as by filters and firewalls), or by combination of the two. Some of these 'negative' internet-based counter-terrorism measures involve laws, and some involve voluntary codes or regulatory dialogue with communication service providers ('CSPs'). Illustrations of negative content control measures will be derived primarily from official state action in the US, the UK and the EU, though unofficial or unattributed cyber-attacks on jihadi and other extremist internet presences have also occurred, such as Internet Haganah.[32] In the wake of the January 2015 attacks in Paris, Anonymous launched 'Op Charlie Hebdo' with the purpose of disabling jihadi forums and social media accounts. They claimed their first victory in this effort via a tweet on 12 January announcing the takedown of the French-language jihadi forum, Ansar al-Haqq.

[29] See D Lyon, *Surveillance After September 11* (Polity, Cambridge 2005); Home Affairs Committee, *A Surveillance Society?* (2007–08 HC 58, and Government Reply, Cm 7449, 2008); House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State* (2008–09 HL 18, and Government Reply, Cm 7616, 2009); M Scheinin, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* (A/HRC/13/37, 2009); C Fuchs and others (eds), *Internet and Surveillance* (Routledge, New York 2011).

[30] See C Walker and Y Akdeniz, 'Anti-Terrorism laws and data retention: war is over?' in (2003) 54 *Northern Ireland Legal Quarterly* 159; *Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others*, 8 April 2014.

[31] See Chapter 10 (Macdonald). Key allegations were rejected in *Liberty v GCHQ* [2014] UKIPTrib 13_77-H.

[32] See G Weimann, *Terror on the Internet* (US Institute of Peace Press, Washington DC 2006) 199.

US negative measures

Controls over internet-based speech are especially contentious in the US context, where the First Amendment to the US Constitution prioritises freedom of expression, including the right to publish extreme and offensive materials.[33] Achieving a proper balance between content control and freedom of expression has therefore proven to be a considerable challenge, though the balance is still weighted in favour of expression compared to the stance in Europe.

It is for this reason that many extremist and terrorist websites have been hosted in the US. For example, in 1997, controversy erupted when it was revealed that the State University of New York (SUNY) at Binghamton was hosting the website of the Revolutionary Armed Forces of Colombia (FARC), and that a *Tupac Amaru* (MRTA) solidarity site was operating out of the University of California at San Diego (UCSD).[34] SUNY officials promptly shut down the FARC site. In San Diego, officials decided in favour of free speech, and the *Tupac Amaru* site remained in operation on UCSD's servers for some years. It was not illegal at that time to host such a site, even if a group was designated a 'Foreign Terrorist Organisation' by the US Department of State, as long as a site was not seeking financial contributions nor providing financial support to the group. This toleration persists even after 9/11. For instance, though listed in 2011 by the UN 1267 Committee and by the US as a Specially Designated Global Terrorist ('SDGT') under US Executive Order 13224, and proscribed in the UK in 2013,[35] Imarat Kavkaz (Caucasus Emirate) remains available on the internet through the sympathetic Kavkaz Centre (www.kavkazcenter.com) which is hosted by Cloudflare in the US.

The principal qualification to free speech since 9/11 has been the more aggressive usage of the anti-terrorist offences of material support.[36] First, 18 USC section 2339A, enacted in 1994,[37] addresses

[33] See *Brandenburg v Ohio* 395 US 444 (1969); *Hess v Indiana* 414 US 105 (1972); *RAV v St Paul* 505 US 377 (1992). The strength of the priority may have become less rigorous: T Healey, 'Brandenburg in time of terror' (2009) 84 *Notre Dame Law Review* 655. Compare for the UK, D Barnum, 'Indirect incitement and freedom of speech in Anglo-American law' [2006] *European Human Rights Law Review* 258.
[34] See M Conway, 'Terrorism and Internet governance: core issues' (2007) 3 *Disarmament Forum* 23.
[35] Terrorism Act 2000 (Proscribed Organisations) (Amendment) (no 2) Order 2013 SI 2013/3172.
[36] See RM Chesney, 'The sleeper scenario' (2005) *Harvard Journal on Legislation* 1 and 'Federal prosecution of terrorism related offences' (2007) 11 *Lewis & Clark Law Review* 851; D Cole, 'Terror financing, guilt by association and the paradigm of prevention in the "war on terror"' in A Bianchi and A Keller, *Counterterrorism* (Hart, Oxford 2008); J Ward, 'The root of all evil' (2008) 84 *Notre Dame Law Review* 471.
[37] Violent Crime Control and Law Enforcement Act 1994, PL 103-322 s 120005.

the provision directly or indirectly of financial or other material support or resources knowing or intending their use for terrorist activities as being forbidden by thirty-six listed offences. Proof of intent is required that the recipient is a terrorist group (even recklessness is not sufficient and certainly not negligence).[38] By 18 USC s 2339B,[39] it is an offence without any requirement of intent or belief as to the terrorist nature of the acts to be aided[40] to provide material support or resources (including to oneself) to a designated 'Foreign Terrorist Organization'[41] (Al-Qa'ida was listed in 1999). Title III of the USA PATRIOT Act, sections 803 to 815, also known as the International Money Laundering Abatement and Anti-Terrorist Financing Act 2001,[42] augmented sections 2339A and 2339B. It widened the notion of 'material support or resources' by including, for example, expert advice or assistance.

Though just a handful of speech-related prosecutions have arisen, free speech activists fail to be convinced that there is any clear and present danger of imminent harmful action.[43] In *US v Iqbal and Elahwal*,[44] Iqbal pleaded guilty to providing material support to Hizballah (also a designated Foreign Terrorist Organization) by operating a satellite television service known as HDTV Limited, which carried Al Manar and for which Iqbal was directly paid thousands of dollars by Al Manar. Next, in 2012, Tarek Mehanna, was sentenced to more than 17 years' imprisonment for conspiracy to provide material support to Al-Qa'ida, providing material support to terrorists (and conspiracy to do so), conspiracy to commit murder in a foreign country, conspiracy to make false statements to the FBI, and two counts of making false statements.[45] His internet-related material support arose from, among other things, translating and posting on the internet Al-Qa'ida recruitment videos and other documents, including some that encouraged violence against American military forces.

[38] But see *US v Lakhani* 480 F 3d 171 (2007).
[39] Antiterrorism and Effective Death Penalty Act 1996, PL 104-132, s 303.
[40] The Intelligence Reform and Terrorism Prevention Act 2004, PL 108-458, s 6603(c)(2) clarified that knowledge (but still not recklessness or negligence) is confined to the fact that the group is designated or has engaged in terrorism.
[41] 8 USC s 1189(a)(1), inserted by the Antiterrorism and Effective Death Penalty Act 1996, s 302 (see also 31 CFR s 597.101-901).
[42] PL 107-56.
[43] See *Brandenburg v Ohio* 395 US 444 (1969). Note also *32 County Sovereignty Committee v Department of State* 292 F 3d 797 (2002).
[44] (2008) USDC, SDNY.
[45] (2012) USDC, SDNY, cert den 547 US (2014). See N Abel, '*United States v. Mehanna*, The First Amendment, and Material Support in the War on Terror' (2013) 54 *Boston College Law Review* 711; GD Brown, 'Notes on a Terrorism Trial – Preventive Prosecution, "Material Support" and The Role of The Judge after *United States v. Mehanna*' (2012) 4 *Harvard National Security Journal* 1; EG Knox, 'Slippery Slope of Material Support Prosecutions: Social Media Support to Terrorists' (2014) 66 *Hastings Law Journal* 295.

The constitutionality of the material support offences was upheld by the US Supreme Court in 2010 against challenges based on free speech and vagueness in *Holder v Humanitarian Law Project*.[46] Chief Justice John G. Roberts Jr declared that for speech to qualify as material support for terrorism, it had to be 'expert advice or assistance' delivered 'in coordination with or under the control of' a designated foreign terrorist organization; 'independent advocacy' of a terror group's ideology, aims or methods is not a crime.[47] Justice Roberts underlined that 'under the material support statute, plaintiffs may say anything they wish on any topic' and pointed out that 'Congress has not sought to suppress ideas or opinions in the form of "pure political speech"'.[48] Despite these statements, the Mehanna conviction suggests that individuals can be convicted of terrorism offences on the basis of online speech acts with very tenuous links to notions of financing or support by deed.

A commitment to First Amendment rights is equally the reason put forward by major US social media companies, such as Facebook, Twitter, and YouTube, for their decisions to decline to censor some of the violent extremist content posted to their sites. US lawmakers have been amongst those exhorting Twitter and YouTube to cancel accounts they view as 'terrorist'.[49] In response, Twitter has adopted the mantra of being 'the free speech wing of the free speech party'[50] and has in the past refused requests from government officials, activist organizations, and concerned individuals to cancel the accounts of, amongst others, Lebanese Hezbollah, the Afghan Taliban, and Syria's violent Jihadi faction Jabhat al-Nusra. However, its policy began to shift in 2012 towards a more country-specific approach,[51] and, in January 2013, Twitter cancelled the account of Somalia's al-Shabab following the group tweeting photographs of the body of a French commando whom they had killed followed by explicit threats to execute Kenyan hostages they held.[52] In the event, al-

[46] 561 US 1 (2010). See P Marguiles, 'Advising Terrorism: Material Support, Safe Harbors, and Freedom of Speech' (2011-2012) 63 *Hastings Law Journal* 455; A Tomkins, 'Criminalizing Support for Terrorism: A Comparative Perspective' (2011) 6 *Duke Journal of Constitutional Law & Public Policy* 81; D Cole, 'The First Amendment's Borders: The Place of *Holder v. Humanitarian Law Project* in First Amendment Doctrine' (2012) 6 *Harvard Law & Policy Review* 148.
[47] *Ibid.* 18-20.
[48] *Ibid.* 20-21.
[49] See B Farmer, 'Congress calls on Twitter to block Taliban' *Daily Telegraph Online* (London, 25 December 2011); J Gettleman, 'As militants use Twitter, U.S. explores boundaries; Officials say government is examining options to close Al Shabab's account' *International Herald Tribune* (Paris, 21 December 2011) 3; Subcommittee on Counterterrorism and Intelligence of the Committee on Homeland Security House of Representatives, *Jihadist Use Of Social Media - How to Prevent Terrorism and Preserve Innovation* (Serial No 112-62, Washington DC, 6 December 2011).
[50] See E Barnett, 'Twitter chief: We will protect our users from Government' *Daily Telegraph Online* (London, 18 October 2011).
[51] See J Taylor, 'Twitter faces user backlash over move to censor messages' *Independent* (London, 28 January 2012) 10.
[52] See 'Twitter bars Islamists' account in English' *Daily Telegraph* (London, 26 January 2013) 18.

Shabab reestablished their Twitter account, under a slightly different name, almost immediately, and Twitter was once again embroiled in controversy when the group live Tweeted their attack on the Westgate shopping mall in Nairobi, Kenya in September 2013.[53] Twitter appears to have shifted its position somewhat since, engaging in a wholesale cull of violent jihadi accounts from mid-2014 possibly, according to one analyst, at the behest of the US Government and almost certainly also influenced by the use of these accounts to spread images from and links to beheading videos.[54]

These verdicts by CSPs of life and death over social media accounts highlight the lack of transparency surrounding how decisions are taken as to which accounts are cancelled and why. Twitter have no detailed and publicly available guidelines on the matter but merely report on requests,[55] as does Google.[56] The Edward Snowden revelations also alleged on-going contacts with state agencies which have become embarrassing for CSPs.[57]

UK negative measures

Compared to the US, the UK anti-terrorism laws contain a more comprehensive catalogue of criminal offence and take-down measures, with less restraint in their application, though the results often remain controversial.[58]

Reflecting the pursuit of precursor crimes, the mainstay offences dealing with extremist materials on the internet are sections 57 and 58 of the Terrorism Act 2000. Section 57(1) is contravened by possession of an article in circumstances which give rise to a reasonable suspicion that the

[53] See H Alexander, 'Tweeting terrorism' *Daily Telegraph Online* (London, 22 September 2013).
[54] See D Friedman, 'Twitter kills ISIS accounts over threats, denies fiends propaganda win' *Daily News* (New York, 17 August 2014) 12.
[55] All content removal requests directed at Twitter are however posted on the Chilling Effects website at <http://www.chillingeffects.org> last accessed 20 January 2014.
[56] See <http://www.google.com/transparencyreport/removals/government/> last accessed 20 January 2014.
[57] They have proposed greater use of encryption in response: 'Yahoo joins Google in effort to protect users' emails from prying eyes' *Daily Telegraph Online* (London, 8 August 2014).
[58] See C Walker, 'Cyber-terrorism: Legal principle and the law in the United Kingdom' (2006) 110 Penn State Law Review 625; M Conway, 'Terrorism and the internet: new media, new threat?' (2006) 59 *Parliamentary Affairs*, 283; I Cram, *Terror and the War on Dissent - Freedom of Expression in the Age of Al-Qaeda*, (Springer, Berlin 2009); A Carlile and S Macdonald, 'The criminalisation of terrorist online preparatory acts' in T Chen, L Jarvis and S Macdonald (eds), *Cyberterrorism* (Springer, Heidelberg 2014); CP Walker, *The Anti-Terrorism Legislation* (3rd ed, Oxford University Press, Oxford 2014) chs 2, 6.

possession is for a purpose connected with terrorism. The articles possessed will often be lawful in themselves and even commonplace. Regarding multiple-use articles such as computer disks or cars, section 57(1) only requires 'a' purpose to be nefarious, not a main or sole purpose. In *R v Omar Altimini*,[59] computer materials held by a 'sleeper' contravened section 57. Recognizing possible overreach, section 57(2) offers a defence by proof on an evidentiary basis according to *R v Director of Public Prosecutions, ex parte Kebilene*[60] that possession of the article was not for a purpose connected with terrorism. The offence is highly valued by police and prosecutors. Since 2006, sentences have increased and include 12 years ('the top of the spectrum') for a vast collection of propaganda and instructional guides, observations of security at Manchester Airport, and musings about attacks.[61]

Even more relevant are the offences under section 58. Section 58(1) contains two variants of *actus reus*: collecting or making a record of information likely to be useful to terrorism or possessing a document or record containing information of that kind. A 'record' includes electronic formats (section 58(2)). The defendant must be aware of the nature of the contents.[62] However, the Crown is also not required to show that the defendant harboured a terrorist purpose. In *R v K*, the defendant, Khalid Khaliq, argued boldly that section 58 was insufficiently certain to comply with Article 7 of the European Convention. In response, the Court of Appeal sought to remedy any imprecision by reading in the requirement of a purpose useful to terrorism. Thus, the purpose of the information (rather than the possessor) is at stake — it intrinsically 'calls for an explanation'.[63] The information must be of an intrinsic kind which gives rise to a reasonable suspicion that it is likely to provide practical assistance to a person committing or preparing terrorism rather than simply encouraging the commission of terrorism. To illustrate, the A–Z of London could be useful to a terrorist in the location of a target, but that use would not fall within section 58 since that document does not intrinsically arouse suspicion.[64] In *R v Terence Roy Brown*, an internet seller of literature, such as *The Anarchist Cookbook*, which he admitted was useful to terrorists, was convicted even though he viewed his activities as a non-ideological business on which he paid taxes.[65] By section 58(3), it is a defence to prove a 'reasonable excuse'. Section 58 is commonly invoked against those who download and

[59] [2008] EWCA Crim 2829.
[60] [2000] 2 AC 326.
[61] *R v Sultan Muhammed and Aabid Hassain Khan* [2009] EWCA Crim 2653, para 13.
[62] *R v G and J* [2009] UKHL 13, paras 47, 48.
[63] See further *R v Samina Malik* [2008] EWCA Crim 185, para 14; *R v G and J* [2009] UKHL 13, paras 43, 44
[64] [2008] EWCA Crim 1450.
[65] [2011] EWCA Crim 2751, paras 17, 34.

disseminate extremist internet material. In *R v Khuram Shazad Iqbal*,[66] the defendant (aka 'Abu Irhaab') had used Facebook and Twitter to post links to 848 examples of extreme content (videos and articles) on the internet and was found with nine copies of the Al-Qa'ida magazine *Inspire* on his laptop.

There have been 76 charges under section 57 and 44 under section 58 from September 11, 2001 to 31 March 2013 (out of 375 under anti-terrorism legislation).[67] The main controversies surrounding these offences concern the equivocal nature of the actions involved and the switched burden of proof of reasonable excuse. Journalists and even scholars can in theory fall foul,[68] as can self-proclaimed freedom-fighters.[69] Despite the shifts in judicial interpretation which have occurred, the European Court of Human Rights in *Jobe v United Kingdom* rejected a complaint that section 58(3) had resulted in the application of a retrospective criminal penalty.[70]

Countering the ideology of terrorism is further addressed by offences against extremist speech and publications in sections 1 and 2 of the Terrorism Act 2006. These offences react not only to the July 2005 London bombings but also in some aspects to the Council of Europe Convention on the Prevention of Terrorism 2005.[71] The principal offence in section 1(1) relates to the publication of statements that are 'likely to be understood by some or all of the members of the public to whom it is published as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism' or specified offences which are referred to as 'Convention offences'. As for the *mens rea*, in section 1(2)(b), the publisher must either intend members of the public to be directly or indirectly encouraged or otherwise induced by the statement to commit, prepare, or instigate acts of terrorism or specified offences, or be subjectively reckless as to whether members of the public will be so directly or indirectly encouraged by the statement. The most controversial facet of the offence is 'indirect' encouragement. By sub-section (3), the indirect encouragement of terrorism includes a statement that 'glorifies' the commission or preparation of

[66] [2014] EWCA Crim 2650.
[67] Source: Home Office, *Operation of Police Powers under the Terrorism Act 2000 and Subsequent Legislation* (London, 2013) Tables A05a and b.
[68] See 'The case of Rizwaan Sabir' *The Guardian* (London, 15 September 2011) 11.
[69] See *R v Gul* [2013] UKSC 64 para 54 (prosecution under the TA 2000, s 2).
[70] App no 48278/09, 14 June 2011, para 31. Compare J Hodgson and V Tadros, V 'How to make a terrorist out of nothing' (2009) 72 *Modern Law Review* 984.
[71] ETS 196. See E Parker 'Implementation of the UK Terrorism Act 2006' (2007) 21 *Emory International Law Review* 711; E Barendt, 'Incitement to, and glorification of terrorism' in I Hare and J Weinstein (eds), *Extreme Speech and Democracy* (Oxford University Press, Oxford 2009); Walker (n 11) ch 8

acts of terrorism or specified offences (either in their actual commission or in principle) but only if members of the public could reasonably be expected to infer that what is being glorified in the statement is being glorified as conduct that should be 'emulated by them in existing circumstances'. 'Glorify' is partly defined in section 20(2) as including 'praise or celebration'. Having handled the originators of statements in section 1, section 2(1) deals with secondary dissemination. The offence may be committed by a 'terrorist publication' such as by electronic transmission. It is a defence under section 2(9) to show that the statement neither expressed the publisher's views nor had his endorsement. This defence can benefit 'all legitimate librarians, academics and booksellers'[72] (and broadcasters and bloggers) who may have examined the article but do not endorse its contents. There have been only 10 prosecutions up to 31 March 2013.[73] As with section 58, challenges on human rights grounds have been rejected.[74]

More purely preventive measures is section 3 which seeks to apply these offences in the context of unlawfully terrorist-related articles or records on the internet and to devise a short-circuit enforcement power. It was claimed that 'extremist' websites have proliferated,[75] and that communication technologies represent both an important terrorist target and logistical aid. Section 3(1) applies where the publication under section 1 or the dissemination under section 2 was produced electronically. The impugned materials are those which are 'unlawfully terrorism-related' under section 3(7). The short-circuit process under section 3(3) arises where a constable forms the opinion that material held on the system of the service provider is 'unlawfully terrorism-related'. A notice can be issued which requires the provider to arrange for the material to become unavailable to the public and also warns the provider that failure to comply with the notice within two working days[76] will result in the matter being regarded as being endorsed with consequent potential liability under sub-section (4). Critics argued that these restrictions on freedom of expression should engage a judicial officer at some stage so that the value of rights could be considered more explicitly than in the likely calculations of a commercial service provider. The government retort was that judicial process would cause undue delay in a 'fast moving world',[77] though the *Home Office Guidance on Notices Issued under Section 3 of the Terrorism Act 2006* does seek to confine the initiation of notices to expert officers of the Metropolitan Police Service Counter-Terrorist Command.

[72] Hansard (HL) vol 676, col 465 (5 December 2005), Baroness Scotland.
[73] Sources: Statistical bulletins of the Home Office and Northern Ireland Office.
[74] See *Iqbal v R* [2014] EWCA Crim 2650.
[75] Home Office, *Pursue, Prevent, Protect, Prepare: The United Kingdom's Strategy for Countering International Terrorism* (Cm 7547, 2009) para 5.14.
[76] S 3(2), (9).
[77] Hansard (HL) vol 676, col 677 (7 December 2005), Baroness Scotland.

By 15 January 2015, the removal of 72,000 web items (at an increasing rate per year) had been prompted, though how this figure relates to alerts is not revealed.[78] The potential operation of section 3 is curtailed by the impact of the Electronic Commerce Directive.[79] More importantly, section 3 is bypassed by responsive action by CSPs in response to informal police requests. Indeed, the Guidance suggests dialogue and that a 'voluntary approach' should be taken where the provider is not viewed as encouraging publication.[80] In consequence, section 3 has never been formally invoked. The public are also invited to sound an alert about extremism and terrorism via a government website which feeds into the Counter Terrorism Internet Referral Unit (CTIRU), launched by the Association of Chief Police Officers (ACPO) in 2010,[81] to encourage 'a civic challenge against material that [the public] find offensive, even if it is not illegal.'[82]

The shortcomings of these warning systems were highlighted by the head of Government Communications Headquarters ('GCHQ') and the UK Prime Minister in November 2014. The head of GCHQ, Robert Hannigan, stated that social media companies are 'the command-and-control networks of choice for terrorists', with some technology companies 'in denial' about the internet's misuse.[83] Following criticism also by the Prime Minister,[84] several UK operators (BT, Virgin, Sky, and TalkTalk) agreed to install public reporting buttons to flag terrorist material on their services whilst Facebook, Google, Yahoo, and Twitter agreed to mentor smaller internet companies on standards of content monitoring.

More difficult is to contend with overseas CSPs. No international system replicates these UK take-down measures elsewhere, despite the dangers recognised by the EU Framework Directive on Combating Terrorism.[85] Most extremist content is hosted by US-based CSPs. Their receptivity to self-censorship is lower than for European-based companies, as highlighted by the Intelligence and

[78] Home Affairs Committee, *The Roots of Violent Radicalisation* (2010–12, HC 1446) para 53. It called for a code of conduct for ISPs: para 59.
[79] 2000/31/EC. See Electronic Commerce (European Communities Directive) Regulations 2002, SI 2002/2013.
[80] Paras 20, 27, Annex C.
[81] <https://www.gov.uk/report-terrorism>, last accessed 20 January 2015. See M Blain, 'Terrorism trawlers' (2011) *Police Review* 20 May 20.
[82] Hansard (House of Commons) vol 591 col 332, 21 January 2015. For the chronology, see <https://wiki.openrightsgroup.org/wiki/Counter_Terrorism_Internet_Referral_Unit?>, last accessed 20 January 2015.
[83] R Hannigan, 'The web is a terrorist's command-and-control network of choice' *Financial Times* (London, 3 November 2014).
[84] P Wintour, 'UK ISPs to introduce jihadi and terror content reporting button' *The Guardian* 14 November.
[85] Council Framework Decision, 2008/919/JHA, para 4. Europol encourage police cooperation through the 'Check the Web' initiative: EU Council docs 9496/06, 16532/1/06, 8457/3/07.

Security Committee ('ISC') *Report on the intelligence relating to the murder of Fusilier Lee Rigby*.[86] One of the soldier's killers, Michael Adebowale, had several of his multiple social media internet accounts (later revealed by the media to be operated through Facebook) closed proactively without official request by the CSP using an automated process because, according to GCHQ, 'they hit triggers…related to their criteria for closing things down on the basis of terrorist content'.[87] Facebook also learned, on completion of a retrospective review of all his 11accounts,[88] that Adebowale had also discussed 'in the most explicit and emotive manner' over Facebook's instant messaging service his desire to murder a soldier.[89] The ISC was critical of monitoring procedures by CSPs,[90] though serial investigations by the Security Service were excused as sufficiently thorough, especially because, as pointed out even by GCHQ,[91] true intent can be very difficult to discern from online communications. Putting aside other relevant issues around data privacy, accountability for surveillance, the duty of care to users, and the economic efficiency, were social media companies to be obliged to proactively monitor and share all postings of a violent extremist nature with security authorities, the former would have little time or money for anything else and the latter would be deluged with information and likely rendered unable to function.

European initiatives

Because of US constitutional distaste for restrictions on freedom of expression, the UN has achieved few tangible results in this field and most activity has arisen within Europe. Key international legal instruments addressing content have emanated from the Council of Europe - not only the Convention on the Prevention of Terrorism 2005 mentioned earlier but also the Convention on Cybercrime 2001 and the Additional Protocol 2002.[92] The Protocol specifies various types of hate speech that should be prohibited on the internet, including racist and xenophobic materials, justification of genocide, and crimes against humanity.

[86] (2014-15 HC 795).
[87] *Ibid.*, para 384.
[88] *Ibid.*, para 390.
[89] *Ibid.*, para 384.
[90] *Ibid.*, para 389.
[91] *Ibid.*, para 393.
[92] ETS 185, 189. The US has signed the former but not the latter on First Amendment grounds. 24 member states have ratified (not including the UK).

The Organization for Security and Co-operation in Europe ('OSCE') is active in this field also. Its Sofia Ministerial Council decided in 2004 that 'participating States will exchange information on the use of the Internet for terrorist purposes and identify possible strategies to combat this threat, while ensuring respect for international human rights obligations and standards, including those concerning the rights to privacy and freedom of opinion and expression'.[93] A follow-up decision from the OSCE's Brussels Ministerial Council in 2006 invited participating states to 'increase their monitoring of websites of terrorist/violent extremist organizations and their supporters and to invigorate their exchange of information.'[94] Since that time, numerous OSCE events have aired various policy views addressing internet content control, though no new rules have been instituted as a result of these discussions.[95]

As regards the European Union, terrorist uses of the internet and the risks posed by them have not been the subject of serious attention by its policymakers until quite recently because it is viewed as a relatively new issue and because the gestation of EU policy occurs at a glacial pace.[96] In fact, the EU has worked on formulating harmonised policy on combating terrorist use of the internet since 2006. Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism required state action to criminalise incitement of terrorism via the internet, including 'public provocation to commit a terrorist offence', as well as the use of the internet for recruitment for terrorism and training for terrorism. Though the UK had passed such legislation in 2006, other countries were thus prompted to take action.[97]

Other initiatives undertaken by the EU include 'Check the Web', which was launched in 2007 and allows states to pool data on terrorist propaganda and internet chatter at the European Police Office (Europol).[98] The EU Commission also funded a project titled CleanIT[99] to initiate 'a structured public-private dialogue between government representatives, academics, Internet industry, Internet

[93] OSCE Ministerial Council, Sofia, 2004, *Decision No. 3/04: Combating the Use of the Internet for Terrorist Purposes*.
[94] OSCE Ministerial Council, Brussels, 2006, *Decision No. 7/06: Countering the Use of the Internet for Terrorist Purposes*.
[95] See OSCE, 'Expert Workshop on Combating the Use of the Internet for Terrorist Purposes' (Vienna, 13–14 October 2005); OSCE-Council of Europe, 'Expert Workshop on Preventing Terrorism: Fighting Incitement and Related Terrorist Activities' (Vienna, 19–20 October 2006).
[96] J Argomaniz, 'European Union responses to terrorist use of the Internet' (2014) *Cooperation and Conflict* (Online) 5.
[97] See F Galli and A Weyembergh, *EU Counter-terrorism Offences: What impact on national legislation and case-law?* (University of Brussels, Brussels 2012).
[98] See Article 36 *Committee, Council Conclusions on cooperation to combat terrorist use of the Internet ('Check the Web')* (8457/3/07 REV 3, 2007).
[99] See <http://cleanitproject.eu/>, last accessed 20 January 2015.

users and non-governmental organisations in the European Union' on 'Reducing terrorist use of the Internet'. Its final product was a report on conditions for action, plus best practices .[100] It has been argued that the real value of the CleanIT project resided in the fact that 'it has turned the spotlight on a wider problem: the [European] Commission's reliance on industry solutions to address problems that are badly defined by policymakers from the very beginning'.[101]

Large-scale technologically-facilitated blocking and unattributed take-downs

Discussion up to now has focused largely on legislated or voluntary content removals. In addition, states are not technologically impotent when faced with terrorists seeking to use the internet, especially not powerful states with large defence budgets and advanced technological capabilities. Thus, states can seek to constrain the effectiveness of these cyber-based strategies by limiting user and audience access to online platforms through control of the internet infrastructure. The common element for governmental filtering is generally an index of websites that citizens are blocked from accessing. If a website appears on this list, access can be blocked. Filtering of content is carried out in many countries, such as China, Iran, Saudi Arabia, and Singapore, and in some cases, CSPs are pressured to apply blocks. In the final week of December 2014, for example, the government of India instituted a block on 32 major websites including software code repository Github, video streaming sites Vimeo and Dailymotion, the Internet Archive, and many others, on the basis of their hosting what Arvind Gupta, head of Information Technology for India's ruling Bharatiya Janata Party, called 'Anti India content from ISIS'. Five sites (weebly.com, vimeo.com, Pastebin, dailymotion.com and gist.github.com) were unblocked after agreeing to remove 'Anti-India' content.[102]

Finally, in terms of 'negative' measures, an even more drastic content control approach is to use cyber-attack methods. Today there are between two and five so-called 'top tier' jihadi forums.[103] Forums are considered 'top tier' that receive new and authentic content for distribution from Al-Qa'ida's Al-Sahab media production outlet and other important producers. These forums are thus

[100] *Reducing Terrorist Uses of the Internet* (The Hague, 2013).
[101] Argomaniz (n 106) p 11.
[102] S Panigrahi, 'Indian Netizens Criticize Online Censorship of 'Jihadi' Content' <http://globalvoicesonline.org/2015/01/06/indian-netizens-criticize-online-censorship-of-jihadi-content/>, last accessed 20 January 2015.
[103] AY Zelin, *The State of Global Jihad Online* (New America Foundation, Washington DC 2013) 2.

the subject of fairly routine attacks that can result in their being offline for days, weeks, or even months.[104] It is not known what or who is responsible for these outages, but many assume they are the work of one or more states' intelligence agencies. Such attack strategies have been criticised by those who argue that violent extremist online forums and other violent extremist cyberspaces can serve as valuable providers of open source intelligence for states' intelligence agencies.[105]

'Positive' Online Measures

Generally less contentious are 'positive' online counter-terrorism measures that employ online engagement and outreach rather than content controls to stem the encouragement of violence. Most contemporary such campaigns focus upon social media which target youth, since they are believed to be particularly vulnerable to violent online political extremist rhetoric. This work is often undertaken by non-governmental organizations and individual activists, including young people themselves; although some such campaigns have also been undertaken by state agencies.

Within the realm of state interventions, shortly after 11 September 2001, the UK domestic Security Service (MI5) took the unprecedented step of posting an appeal for information about potential terrorists on dissident Arab websites.[106] The message, in Arabic, was placed on sites that the authorities knew were accessed by extremists, including Islah.org, a Saudi Arabian opposition site, and Qoqaz.com, a Chechen site that advocated jihad. MI5 were hopeful of eliciting information from persons on the margins of extremist groups or communities who were sufficiently shocked by the events of 11 September 2001 to want to contact the agency. The agency had intended to post the message on a further 15 sites known to be accessed by radicals, but many of these were shut down by the FBI in the aftermath of the attacks. Later, in 2007, the UK Home Office established the Research Information and Communications Unit ('RICU') as a cross-departmental strategic communications body based at its Office for Security and Counter-terrorism; RICU seeks to

[104] *Ibid.*, 9.
[105] J Lasker, 'Watchdogs Sniff Out Terror Sites' *Wired News* 25 February 2005 <http://www.wired.com/news/privacy/0,1848,66708,00.html>; W McCants, Testimony, US House of Representatives, Subcommittee on Counterterrorism and Intelligence, 'Jihadist use of social media: how to prevent terrorism and preserve innovation,' 6 December 2011 <http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20McCants.pdf>; Zelin (n 116); MR Torres Soriano, 'The vulnerabilities of online terrorism' (2012) 35 *Studies in Conflict & Terrorism* 263.
[106] See M Conway, 'Terrorist Use of the Internet and the Challenges of Governing Cyberspace' in M Dunn, V Mauer, and F Krishna-Hensel (eds), *Power and Security in the Information Age* (Ashgate, London 2007).

coordinate government communication activities to counter violent extremism while promoting inter-community relations.[107]

Another 'positive' government agency initiative is the US State Department's Centre for Strategic Counterterrorism Communications' ('CSCC') 'Think Again Turn Away' social media campaign. The CSCC was established in 2010, 'to coordinate, orient, and inform government-wide foreign communications activities targeted against terrorism and violent extremism, particularly al-Qaeda, and its affiliates and adherents…The Digital Outreach Team actively and openly engages in Arabic, Urdu, Punjabi, and Somali to counter terrorist propaganda and misinformation about the United States across a wide variety of interactive digital environments that had previously been ceded to extremists'.[108] The CSCC is both praised and vilified for 'Think Again Turn Away,' an English language social media campaign that commenced in December 2013, whose mission is described on its Facebook page as 'to expose the facts about terrorists and their propaganda'. In addition to its Facebook presence, the campaign is also active on Ask.fm, Google+, Tumblr, Twitter, and YouTube where it disseminates content that addresses the same grievances as those in extremist content, including in some instances creating 'mash-ups' of IS content and re-circulating it. Many commentators view the CSCC's online activity as a drop in the ocean compared to the likes of IS, but as essentially harmless; others describe CSCC activity as 'embarrassing' and 'ineffective'.[109]

In 2012, the EU established its Radicalisation Awareness Network ('RAN') under Directorate General Home Affairs to dissuade people from participating in violent extremism and terrorism or to persuade them to separate themselves from such ideas and methods in the first place.[110] The RAN is composed of eight working groups—composed of researchers, activists, and CVE practitioners (to name a few) — one of which, RAN@, is tasked with 'develop[ing] frontline partnerships around the collation, creation, and dissemination of counter-[violent extremist] and alternative-narratives through the Internet and social media'. Other RAN working groups have also discussed using the internet to reach out to publics; RAN Voices of Victims of Terrorism has, for example, expressed a desire to have the voices of terrorism victims amplified via the internet and social media.

[107] See <https://www.counterextremism.org/download_file/106/134/413/>, accessed 20 January 2015.
[108] <http://www.state.gov/r/cscc/>, accessed 20 January 2014.
[109] R Katz, 'The State Department's Twitter War with ISIS Is Embarrassing' *Time Magazine* (New York, 16 September 2014) (<http://time.com/3387065/isis-twitter-war-state-department/>).
[110] See < http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/index_en.htm >, last accessed 20 January 2014.

Finally, private actors have challenged violent jihadism online. Some are heavily backed by government,[111] but others have been initiated by individuals and non-governmental organizations. Their denunciations or alternative interpretations have taken many different forms, ranging from online video and other online responses denouncing violent extremism by scholars[112] and imams to wide-ranging multimedia campaigns such as 'My Jihad',[113] from ordinary individuals uploading videos to YouTube to more general macro-level positive messaging about Islam targeted at children and youth such as Naif al-Mutawa's comic and animated series, 'The 99'.[114] A particularly interesting example is Abdullah-X, a series of online animated shorts developed by a former extremist, which received support from RAN@ and Google.[115] The developer's status as a former extremist probably lends the project greater credibility than some of those described earlier, and the site may be more accessible and appealing to youth than most state-sponsored campaigns.

Conclusion

Given that the internet is part of the infrastructure of contemporary everyday life in the same way as supermarkets and motorways, it is misguided to make responsiblity on the internet for the aberrant terrorist usage of a small minority or to require that they should treat everyone as an equal risk and potential suspect. Nevertheless, even with the price being paid by extensive criminal offences, intrusion into free speech activities, and the running of new bureaucracies and programmes of funding, one can feel assured that not all terrorism will be averted. The acculturalization of immigrant communities in Western values and lifestyles will prove very difficult owing to the perceived shallowness of those lifestyles and the hypocrisy in the official adherence to proclaimed values. It is also difficult to compete in the market place of ideas against the narratives of jihadism which speak in simplistic, hedonistic, and graphic language not available to official spokespersons. As a result, the dismal prospect is that, no matter how much the state strives to counter international terrorism, current emanations of violent extremism will take generations to assuage.

[111] Probably best known (and highly controversial) is the Quilliam Foundation, <http://www.quilliamfoundation.org/>, last accessed, 20 January 2015.
[112] In March 2010, for example, Sufi Shakyh Dr. Muhammad Tahir-ul-Qadri issued a 600-page 'fatwa' (i.e. a religious ruling) in English and Urdu condemning terrorism, which has an accompanying website at http://www.fatwaonterrorism.com.
[113] See 'My Jihad' website at http://myjihad.org/.
[114] *The 99's* accompanying Website is at http://www.the99.org/.
[115] The Abdullah-X YouTube channel is https://www.youtube.com/user/abdullahx.