Shooting the Messenger: Do Not Blame the Internet for Terrorism

Andrew Glazzard

The internet clearly matters to terrorists, but online content by itself rarely causes people to carry out terrorist attacks. Responses should therefore not be limited to the mass removal of terrorist content from online platforms.

Big tech, we are told, is failing in its moral and social duties to reduce the risk from terrorism. UK authorities, for example, have long asserted that internet platforms are 'the command-and-control networks of choice for terrorists'. More recently, Prime Minister Theresa May told last year's World Economic Forum that 'technology companies still need to do more in stepping up to their responsibilities for dealing with harmful and illegal online activity', including 'the spreading of terrorist and extremist content'. This view has been repeated so often it has become a truism, especially in the UK where politicians and security professionals seem united in their belief that social media and online propaganda not merely facilitate, but actually *cause* terrorism, and that Silicon Valley appears unwilling to do anything about it. But this view of the problem, and the solution, is worryingly simplistic. The relationships between threat, terrorist propaganda and media are complex, and there is no single, linear path from extremist media to violent action. It follows that responses that fail to do justice to this complexity are unlikely to succeed.

The 2018 report of the UK Parliament's Intelligence and Security Committee (ISC) on the five terrorist attacks in the UK in 2017 is a recent and clear expression of the 'not doing enough' thesis. According to the ISC, 'access to extremist material online is reported to have been a key factor in the Manchester Arena attack which killed 22 people', referring to a newspaper report that the attacker, Salman Abedi, used YouTube videos to learn how to make his explosive device. But although it is known that terrorists, like most people, use the internet to discover how to do things – Anders Bering Breivik is a notable example of a lone actor terrorist who taught himself bomb-making almost entirely online – it is the apparent capacity of social media to radicalise that causes most concern. In this respect, the ISC noted with some exasperation that 'little tangible progress has been made' by communication service providers (CSPs – here meaning internet companies) since the ISC raised this issue in its 2014 report on the murder by Islamist terrorists of Lee Rigby in Woolwich the previous year; 'efforts to persuade the CSPs to take action have appealed to their sense of corporate and social responsibility, and have achieved relatively little'. It is a damning verdict – damning, but wrong.

> *'Technology companies still need to do more in stepping up to their responsibilities for dealing with harmful and illegal online activity'*
>
> *- Theresa May*

In fact, big technology companies are removing vast quantities of terrorist and extremist content, especially since breakthroughs in machine learning have enabled processes to be automated and implemented at scale (Facebook's founder Mark Zuckerberg recently said that 99% of content removed from Facebook is detected automatically). Removal of terrorist content by YouTube, Facebook and Twitter dwarfs anything achieved by the Counter-Terrorism Internet Referral Unit (CTIRU) at Scotland Yard, or the similar unit at Europol. Confusingly, the ISC appears to acknowledge this, when it notes that the 300,000 items removed by the CTIRU in nine years was matched by Twitter in just six months. A glance at the transparency reports which are now published regularly by the social media companies shows that automated removal is happening on an industrial scale and so swiftly that content is often taken down before anyone has a chance to access it.

To take one platform as an example, in 2010 YouTube removed hundreds of videos featuring Anwar Al-Awlaki, the notorious leader of Al-Qa'ida in the Arabian Peninsula, after Roshonara Chaudhry, who was inspired by Al-Awlaki's online videos, was convicted of the attempted murder in London of Stephen Timms MP (Chaudhry is a rare example of an individual apparently driven to terrorism by consuming online content). Seven years later, YouTube removed a further 50,000 videos associated with Al-Awlaki. But even this is small-scale compared to what is now being done with machine-learning algorithms. In the three months from April to June 2018, YouTube removed nearly 7.8 million videos, of which over 6.8 million were detected automatically. Only a fraction of these will be terrorist videos (of which over 150,000 were removed in six months in 2017). But 98% of terrorist content removals were

Removal of terrorist content by YouTube, Facebook and Twitter dwarfs anything achieved by the Counter-Terrorism Internet Referral Unit (CTIRU) at Scotland Yard, or the similar unit at Europol. Confusingly, the ISC appears to acknowledge this, when it notes that the 300,000 items removed by the CTIRU in nine years was matched by Twitter in just six months. *Image courtesy of Wikimedia*

detected automatically, and half were removed within two hours.

The statistics are impressive, but the question remains as to whether content removal is effective in reducing the terrorist threat. There can be no doubt that terrorists invest a great deal of time and resources in propaganda. Indeed, propaganda is fundamental to terrorism – a tactic designed to create fear among an audience – by definition. It is no coincidence that the first wave of modern terrorism struck during an earlier information revolution in the 19th Century, when mass-market newspapers and expanding literacy gave terrorists a new medium to affect its audience. A century later, the growth of television gave terrorists an incentive to mount visually impressive 'spectacular' attacks involving aircraft, international sporting events or high-rise buildings. The 9/11 attacks signalled the zenith of spectacular terrorism, at a time when satellite television dominated the media landscape in the Middle East. During this period, what efforts were made to counter terrorist use of mainstream media in the West were limited at best and counter-productive at worst: democratic governments came to recognise there was little they could do to censor or control terrorist content.

But those governments seem to see internet-based propaganda as more powerful, more dangerous, and more in need of regulation and control. So much so, in fact, that the UK government is trying to restrict access not only to the terrorists' own channels, but also material hosted on the research website jihadology.net, stating that it is 'reckless to publish terrorist propaganda online without safeguards to stop those vulnerable to radicalisation from seeing it'. As a result, what looks like a double standard has emerged. In February 2015, for example, Fox News in the US broadcast excerpts of one of the most notorious items of terrorist propaganda ever produced: the last moments of Moaz Al-Kasasbeh, a Jordanian fighter pilot captured by Daesh (also known as the Islamic State of Iraq and Syria, ISIS) who was held in a cage and burned to death. To this day, Fox News continues to host the entire 22-minute video on its website – content which would undoubtedly have been removed by YouTube or Facebook. Similarly, the murder of Lee Rigby on 22 March 2013 featured a remarkable and disturbing item of propaganda, in which one of the killers, Michael Adebolajo, with blood on his hands and holding what appears to be a murder weapon, allowed himself to be filmed by a bystander while he delivered a justification for Rigby's murder. The resulting video was broadcast within hours by ITV News, and subsequently by the BBC and SkyNews. The media regulator Ofcom received nearly 700 complaints about the video, but ruled that broadcasting it was in the public interest. While Ofcom is independent of government, this still raises the following question: why is hosting a terrorist video on a television news channel considered to be a public good, but hosting it on a social media platform is considered a threat to public safety?

A further example is even more instructive. The ISC report on the 2017 attacks unwittingly acknowledges a double standard in its discussion of the case of Darren Osborne, convicted of a fatal attack outside the Muslim Welfare Centre in North London on 19 June 2017. Scotland Yard's Deputy Assistant Commissioner Neil Basu told the ISC that Osborne had been influenced by the BBC drama documentary *Three Girls*, noting that 'there is a wider society debate about some of the material out there and the effect that that … is having on people who want to commit these acts'. But the ISC stopped short of calling on the BBC, or any traditional media outlet, to take action on content that is either produced by active terrorists or which has the potential to radicalise new ones.

Did Osborne kill because of a television programme? Only a psychological study could determine this reliably, but there is enough in the academic literature on terrorism to support the hypothesis that the drama may have been a trigger factor in the chaotic life of a 'loner and a functioning alcoholic' who had threatened to kill himself and had been prescribed medication for anxiety and depression. The literature also states abundantly that terrorists vary enormously in their motivations and pathways to violence, that extreme ideas (however they are received or mediated) do not necessarily lead to extremist actions and violence, and that real-world social networks appear to be much more significant in recruitment and radicalisation to terrorism than internet content. In other words, internet content may enable or contribute to terrorist threats – it would be surprising if it did not – but it does not create or cause them. This means that using content removal as the primary means of preventing radicalisation is simply hitting the wrong target.

A broader view is also needed because terrorists use the internet for more than just disseminating propaganda. As the Breivik and Abedi cases show, it is an information source – for everything from bombmaking to reconnaissance. Internet technologies are used by terrorists to communicate, to manage and transfer funds, and to facilitate travel, and so it makes little sense for governments to focus on content removal to the exclusion of all else. For example, it is clear that too little attention is paid to the importance of communication in the aftermath of a terrorist attack: terrorist attacks are a means to an end, and that end is to engender fear. Therefore, what happens in the media after an attack is just as important as the attack itself, and there is evidence that the authorities have sometimes left the field open, allowing hostile forces to amplify the effect of attacks. Russian disinformation networks, for example, have been at work in shaping responses to the 2017 attacks in the UK, using fake accounts (so-called 'sock puppets') and invented over-reactions to provoke division and polarisation – all apparently uncontested by the UK authorities.

> *In the three months from April to June 2018, YouTube removed nearly 7.8 million videos, of which over 6.8 million were detected automatically*

While content removal will and probably should continue on an industrial scale, there are other things which can, should and are already being done. Technology companies have been experimenting with ways of making problematic content less appealing, less prominent, and substituting competing or benign material. The so-called Redirect method, for example, pioneered by Jigsaw (a Google company) with the British NGO Moonshot CVE, aims to reach 'those who are actively looking for extremist content and connections. Rather than create new content and counter-narratives, [their] approach tries to divert young people off the path to extremism using pre-existing YouTube content and targeted advertising'. Facebook, meanwhile, is grappling with what it calls 'borderline content', with Zuckerberg highlighting research which shows that 'no matter where we draw the lines for what is allowed, as a piece of content gets close to that line, people will engage with it more on average'. Facebook's emerging solution is to find ways to reduce distribution of borderline content, to remove the incentive for creating it in the first place. This is prompted primarily by the need to reduce 'clickbait' and disinformation, but has obvious application to the spread of legal but problematic extremist content.

As society works its way towards a legislative and regulatory accommodation between technology and safety, between availability and restriction, and between public goods and private profits, it is important to recognise the role that the technology industry has in protecting security. But it is also important not to exaggerate that role, and we do ourselves no favours if we focus our response too narrowly on content removal or cast big tech as a scapegoat. The internet does not cause terrorism, and Google and Facebook on their own will not stop it, no matter how much pressure is applied.

Andrew Glazzard
Andrew is the Director of the National Security Studies research programme at RUSI.

The author is project director of the Global Research Network on Terrorism and Technology, a research network supported by the Global Internet Forum for Counter-Terrorism, a consortium of technology companies led by Facebook, Google, Microsoft and Twitter. The views expressed in this article are the author's, and do not represent the views of RUSI or any other institution.