Chapter 2
Responding to Terrorism and Ideologies of Hate

Peter Lehr and Gilbert Ramsay

Introduction

The controversy around the film *The Innocence of Muslims*, manifesting itself in violent demonstrations and counter-demonstrations basically all around the world in September 2012 brought a debate into the open that has kept academics, policy makers and security officials busy for some years now: how to respond to terrorism, and to ideologies of hate? Many strategies have been suggested on how to combat 'them' and to win 'their' audiences' hearts and minds. This contribution aims to shed some light on the main conceptual issues around this question, commenting on 'modern' mass media (TV, radio, print press) first before discussing the dissemination of ideologies of hate in the 'post-modern' media (Internet, YouTube, twitter) and how to counter them (if possible at all), which seem to be the more pressing issues for reasons to be explained below. It will conclude with suggesting that responding may not be as urgent or necessary as it may look at first sight.

Newsmakers and Newsbreakers

There are many definitions of what terrorism is or is not, and all of them are contested. Many of them however point at the fact that terrorism usually aims at reaching an audience. Mark Juergensmeyer for example notes,

> Without being noticed, in fact, terrorism would not exist. The sheer act of killing does not create a terrorist act: murders and wilful assaults occur with such frequency in most societies that they are scarcely reported in the news media. What makes an act terrorism is that it terrifies. The acts to which we assign that label are deliberate events, bombings and

P. Lehr (✉) • G. Ramsay
Centre for the Study of Terrorism and Political Violence (CSTPV), University of St. Andrews, St. Andrews, Scotland
e-mail: pl17@st-andrews.ac.uk; gawr2@st-andrews.ac.uk

S.O. Wolf et al. (eds.), *The Merits of Regional Cooperation*,
DOI 10.1007/978-3-319-02234-5_2, © Springer International Publishing Switzerland 2014

> attacks performed at such places and times that they are calculated to be observed. Terrorism without its horrified witnesses would be as pointless as a play without an audience. Juergensmeyer (2003, p. 141)

Hence, as Brian Jenkins and others repeatedly pointed out, terrorism is theatre. But terrorism as such forms only the most visible tip of the extremist iceberg. There are those who are what is in legalese now called "aiding and abetting" terrorism, for example by helping terrorist groups to recruit new members by radicalising individuals susceptible to their particular message or cause. Including those *preachers of hate* in a rather expansive definition of terrorism – a definition that also covers the equally fuzzy terms 'radical' and 'extreme' by the way – raises many moral, practical and conceptual questions: for example, where exactly does freedom of speech end and the preaching of hate start? Or, where are the exact legal boundaries between 'radicals', 'extremists' and 'terrorists'? Nevertheless, most Western European countries have laws in place criminalising such acts – and quite rightly so: the cases of Abu Hamza al Masri in the UK and Mehtin Caplan (aka Caliph of Cologne) in Germany demonstrate that such individuals play a crucial role with regard to disseminating the terrorists' message. As the controversial film *The Innocence of Muslims* highlights, preachers of hate however do not necessarily need to directly address an audience that is physically present. Rather, modern ways of communication such as YouTube, Twitter, Skype and Facebook can be used for such purposes as well, the effect basically being the same. Notes Dr. Salah Beltagui of the Muslim Council of Scotland on the occasion of a peaceful rally against the anti-Muslim film in Glasgow on 29 September 2012:

> It is giving fuel to those who hate Muslims for some reason, to go on and do some silly activities. [. . .] We have had many attacks on mosques and things, especially after an event like this and a publication like this.[1]

It needs to be emphasised in this context that terrorism is primarily a communication strategy that depends on getting through to a target audience – which includes the terrorists' supporters and members (in order to increase their morale), a broader constituency sympathetic with the terrorists (in order to win over new recruits), the wider (potentially) international audience (in order to attract attention and sympathy for their cause), and, finally the self-defined enemy (in order to intimate and spread fear). Hence, disrupting the terrorists' communication channels and denying them any access to public space and public debate seems to be a good idea, at least at first glance. In the context of the UK and the IRA, Margaret Thatcher once famously demanded to starve them of the oxygen of public attention for this very reason. Faced by unanimous criticism from the British press pointing at the freedom of speech, she defended herself by adding that "in order to protect democracy, you sometimes have no choice but to use undemocratic means."

Margaret 'Maggie' Thatcher's rather unsuccessful attempt to muzzle the press leads us to the following three ideal-type models on how modern mass media could

[1] As quoted in Sutton et al. (2012).

deal with terrorism, and, by extension, with preachers of hates peddling their ideologies of hate by fanning the proverbial flames:

The first option would be adopting a *laissez faire* approach which basically allows the media to cover terrorist events when and how it wants to, free of any code of conduct. This is, very obviously, not ideal as it would allow unscrupulous and irresponsible coverage to go unchecked. An example for that would be the Daily Mail's header of 4 July 2008 which, relating to the Glasgow Airport bombing, stated in bold letters "I kicked burning terrorist in balls."

The second option would be introducing some form of regulation or censorship to control the way that the media covers terrorist events – just as Maggie Thatcher tried to do. This is also unsatisfactory as it dangerously undermines the democratic values (i.e. a free press, right of free speech) that democratic governments are trying to protect. Therefore, neither a laissez faire approach or censorship are appropriate.

Instead, thirdly, a more suitable option might be a system of voluntary self-restraint on the part of the media.

This voluntary self-restraint includes the choice to not cover an incident, or to embargo it for a certain amount of time in order not to interfere with police operations. Recent controversies around the slightly embarrassing nude pictures of Prince Harry, followed by the even more embarrassing revealing pictures of the Duchess of Cambridge, demonstrated that voluntary self-restraint seems to work for quite a while – at least in the domestic British context. Here, it should also be noted that the first deployment of Prince Harry, or 'Captain Wales' as he is officially known, to Afghanistan was also kept under wraps for quite a while, until an Australian magazine finally 'broke the news' and everybody followed. Furthermore, in the case of Scottish NGO worker Linda Norgrove who was kidnapped by the Taliban, the press chose not to cover the story and to keep it out of the public space for fear that doing so would endanger negotiations, and, thus, the life of the hostage. Only when it was clear that the unfortunate NGO volunteer had been killed in a botched rescue operation, and that the next of kin had already been informed, the press went ahead and covered the event.

Voluntary self-restraint could also simply mean adopting guidelines for a responsible coverage of a terrorist event, or, by extension, an incident where a preacher of hate attempts to fan the flames. Again, the most recent example for the latter would be the incendiary and extremely crude *The Innocence of Muslims* 'documentary' on the Prophet by some American right-wingers. A list of criteria for responsible coverage of such events includes:

- No reliance on terrorists or authorities as sole sources.
- Balance the volume of news in the incident so that other news of the day will not be crowded out.
- Provide context, perspective, background, possible motivation of the terrorists, and causes of the incident.
- Do not disclose police or rescue plans.

- Do not use inflammatory catchwords or report rumours.
- Protect the lives of hostages by withholding their identity if disclosure will result in harm.
- Report terrorists' demands and deadlines but don't provide a platform for terrorists.
- Involve top management in tough decisions about coverage.
- Do not participate in incidents or serve as a negotiator.
- Respect the privacy of hostages and their families Schmid (undated).

Here, modern media can make best use of their so-called *gatekeeper role* to influence whether the story is published at all, and how it is received, and then discussed, in the public space: providing context and background, avoiding inflammatory words and pictures, plus airing the opinions of the various stake-holders including the aggrieved party helps to ensure a neutral reporting along the famous 'sine ira et studio' approach of Tacitus, and opens the door to a counter-narrative challenging the terrorists', or preachers of hate's, message. Mission accomplished, then – or not? Unfortunately, the answer to this admittedly rhetorical question is a resounding no: in the era of global modern mass media on the one hand, and Internet-based post-modern media on the other, the mission is not accomplishable at all.

First of all, as we already noted, in a time of 24/7, 365 media coverage, it is more than unlikely that all major media outlets will subscribe to this voluntary self-restraint: as the *Sun* demonstrated by the publication of Prince Harry's pictures, this is unenforceable even within the borders of the UK. How, then, enforcing this outside of the UK's borders, or extending it to non-Western global media outlets such as Al Jazeera or Al Arabiya?

But even more ominously, in the era of post-modern media and the Internet, defined by YouTube, Twitter or Facebook, today's terrorists are no longer restricted to just being the object of 'breaking news'. Instead, modern-day terrorists are able to interact with the outside world in a way that traditional media as the gate keepers of the information flow never offered. In a sense, the Internet is blurring the line between 'news makers' (i.e. those providing the newsworthy event) and 'news breakers' (i.e., those reporting this event). Thus, even if the traditional modern mass media as the gate keeper is slow to react, or reluctant to react at all, today's terrorists can use the Internet to broadcast their own news – in real time, if need be, and unfiltered. Writes Philip Bobbit,

> It took decades for Muslims in Africa and Asia to get upset about the plight of Arab Palestinians. Now Muslims react to events in Lebanon, Gaza, and Iraq while the events are under way, 'in real time.'[2]

The Internet and services such as YouTube or Blogger sites are quite indicative of how much the relationship between media and terrorists has changed over the last one-and-a-half centuries: Originally, terrorist groups were at the mercy of

[2] Bobbitt (2009, p. 63), with further references.

traditional media – first print, then, much later, radio, and eventually television – acting as a gate keeper, deciding which kind of information was passed on and which was not. Also, even if one takes the position that the media's role as a gate keeper is a bit over-emphasized in this context, terrorists were faced by the limits of technology, i.e. most of the times, there was quite a time lag between the event and its reception by the targeted audience – if the audience was not just meant to be immediate bystanders. The advent of internet-based media outlets, including YouTube and similar services, seems to be changing the balance: as the case of Al Zarqawi's notorious beheading videos shows, terrorist groups now seem to be able to create news by themselves, and to influence the way in which these events are received and interpreted by more traditional mass media – nowadays trawling the depths of the Internet in order to find something newsworthy. Now, Internet-savvy terrorist groups seem to be the gate keepers. As a result, traditional approaches to deal with terrorist events, or ideologies of hate, do not work as well as they worked (at least in theory) before the advent of the Internet. If we still intend to influence whether a terrorist-related story is published at all, and how it is received, and then discussed, in the public space, new strategies to deal with terrorism and its coverage/reporting on the Internet on the one hand and with extremism nurtured by ideologies of hate also via the Internet on the other obviously need to be developed. Here, we shall focus on responding to terrorists' instrumental use of the Internet, responding on terrorist propaganda on the Internet, and, finally, responding to radicalization on or via the Internet.

Responding to 'Instrumental' Internet Use by Terrorists

A fundamental problem with responding to terrorists using the Internet as a way of increasing operational efficiency is simply that, to quote former White House 'Cybersecurity Czar' Richard Clarke 'terrorists use the Internet just like everybody else'. Since the Internet plainly cannot detect terrorist intention when someone does, say, a Google search for information about, say, where to buy plant fertiliser in London, there are often few practical ways in which the usefulness of the Internet to terrorists could be reduced without reducing the usefulness to everybody else. A good example of this would come from the shootings that took place Mumbai in November 2008. It was reported at the time (although the claim was absent from the subsequent official report made by Indian authorities), that the terrorists used Google Earth to get detailed information about the layout of Mumbai. Because of this, there were suggestions that this service might be banned in India. But, apart from the inconvenience that this might bring, there were good reasons to think that there would be little to gain from this:

> The US satellite data which Google uses to produce this service is unclassified, and is also provided by competitors.[3] Indeed, ironically, not long after the talk of banning Google

[3] Gilbert Ramsay, CSTPV, conversation with Rob Painter, Google Head of Geolocation.

> Earth in India, there were also proposals to set up a more detailed satellite mapping service using Indian satellites.[4]

Since the terrorists presumably planned the operation in Pakistan, not India, they would not have been impeded by this move.

In any case, the terrorists were equipped with GPS, which would presumably have given them similar advantages.[5]

Some common sense measures have, however, been taken since 9/11 to reduce the amount of information of potential use to terrorists to be found on the websites of public entities in the US (and presumably other countries as well). Something similar holds true for any use terrorists might make of the Internet for the purpose of secure communication. Early on, the US government attempted to outlaw strong encryption (that is to say, scrambling a message so that it can be read only by a recipient with the ‘key’ to unscramble it), on the grounds that it was a military technology. Instead, they provided a relatively weak form of encryption (the DES standard) for commercial and civilian purposes, which allowed US government authorities access to messages encrypted in this way.

Some civil rights campaigners objected to that on the grounds that encryption methods can be produced by anyone with sufficient mathematical competence, and that it would therefore be absurd to consider them a military secret. If the civilian encryption made available was weak enough for the US authorities to crack, it was presumably weak enough for determined organised criminals to crack as well. To demonstrate this, the Electronic Frontier Foundation (a group which aims to protect civil liberties on the Internet) built a device for US$250,000 capable of cracking the existing DES standard for civilian strength encryption.[6] Since then, free and publicly available encryption such as PGP (pretty good privacy) is so strong as to be uncrackable with existing levels of computing power using ‘brute force’ methods (that is, essentially, applying every possible combination until one succeeds, as one might do for a combination lock). Subtler types of cryptanalysis exist, based on, for example, assessing statistical frequencies relating to the most common words in a language believed to be that of the message. It is not known for certain whether anyone is able to reliably break PGP encryption, however, the security technologist Bruce Schneier believes it to be unlikely. As he observes:

> Maybe someone, somewhere has cracked PGP and is keeping real quiet about. Yeah, and maybe pigs will really fly. Hackers and crackers like to brag, have to brag, have a compelling, deep-seated, pathological need to brag. Crypto cracking is hot news. Were someone, somewhere to crack PGP the news would spread faster than a bush fire in the dry season. Schneier (undated)

[4] Blakely (2009).

[5] A copy of the dossier of evidence on the attacks presented by India to Pakistan can be found online at: http://arunshanbhag.com/2009/01/07/terrorist-evidence/.

[6] See http://cryptome.org/jya/cracking-des/cracking-des.htm.

Naturally, then, terrorists and criminals, just like the world's overwhelming majority of innocent users have access, in principle at least, to strong encryption which governments can break only with the utmost difficulty, if at all.[7] It does not follow, however, that all terrorist communications are necessarily properly encrypted. Moreover, even if communications are properly encrypted, this does not defend them against other forms of interception – for example, if the inner circle is already penetrated by agents working to monitor the group, or if computers are 'bugged' with programmes such as key stroke loggers (which record the buttons pressed on a computer keyboard). Governments and intelligence agencies are naturally secretive about the extent to which they use such techniques. However, it is quite clear from terrorism cases in the UK such as the liquid bomb plot that suspected terrorists are often kept under a great deal of sophisticated surveillance. Indeed, there is perhaps some irony to the fact that it is precisely the old-fashioned techniques of infiltration, deception and skilled use of informants that the newest developments in Internet secrecy provide least defence against.

Officially, the ability of agencies in the UK to tap communications in real time is presently regulated by the *Regulation of Investigatory Powers Act* (RIPA). A European Union (EU) directive also mandates that Internet Service Provider companies must preserve a record of traffic data (that is information about which Internet addresses are contacting which, though not information about the actual contents of the communications) for up to 2 years.[8] This information can be accessed under court-issued warrant by law enforcement agencies. It has been reported that the British government wished to propose new legislation which would allow police and security services to access online traffic data unwarranted and in real time.[9] There has been a vociferous backlash to these proposals, but it remains unclear exactly what it is that the government actually intends to propose.

Responding to Terrorist Propaganda on the Internet: Public-Private Dialogues

To start with, it is a highly questionable whether the material placed on the Internet by terrorists groups ought to be responded to at all. Particularly where 'terrorist' web sites contain political information with not much in the way of incitement to violence, there is a good case that trying to remove such sites would, apart from being a violation of freedom of speech rights, be a propaganda own goal in its own

[7] See McClure (1998).

[8] See at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT.

[9] Booth (2012).

right.[10] Where terrorist material has clearly objectionable characteristics (for example, incitement of hate, information on bomb making etc.), states do sometimes try to find ways of removing it. However, this is generally easier said than done. First of all, as we shall explain in a moment, there are technical difficulties in legislating against cybercrime generally. Where these relate to issues of freedom of speech, difficulties are multiplied. Generally, European countries have a narrower interpretation of what is protected by the principle of freedom of speech than does the USA. For example, Germany, Austria and other European states outlaw the use of language and symbols expressing support for Nazism, while the USA does not. And, perhaps unsurprisingly, European countries in turn protect a far wider variety of speech than, say, Middle Eastern countries, Russia or China. Russia, for example, has long been trying to get the removal of the website *The Kavkaz Centre*, which is maintained by Islamist Chechen rebels. The site has generally been hosted in Scandinavian countries, although admittedly, it had to move from sever to server to remain (virtually) open. This relates to the difficulty of determining whether the Russian request be interpreted as an attempt to stifle political dissent, or legitimate concern over a ‘terrorist’ website.

Countries have responded to this predicament in different ways. In some, such as China and Saudi Arabia, relatively efficient ‘filtering’ systems are in place. Content which the regime does not want is simply removed as it enters a relatively small number of monitored points of connection between national and global computer networks and is not accessible within the country. Of course, the efficiency of filtering systems depends on the efficiency of the humans who tell the computers what to filter for. For example, one of the authors who works on e-jihad has been informed that filtering against pornography in Saudi Arabia can be circumvented simply by searching in languages other than Arabic or English. Perhaps unsurprisingly, many Saudi men have acquired an extensive erotic vocabulary in languages such as French, Italian, and even German!

In the Europe Union and in North America, filtering is increasingly used against material such as child pornography – primarily because decisions to remove such content are rarely contested in court. But there has been a general unwillingness to take filtering further. This may be partly because of shortcomings in the technology. But it is also more difficult for countries where there is significant ‘rule of law’ to act in this way – must each new instance of potentially removable content be scrutinised by a court? Instead, such countries have attempted a number of other approaches. In France, the state took Yahoo to court for offering for auction to French citizens Nazi memorabilia which were illegal for sale in France. Yahoo argued that it could not possibly prevent French citizens from buying items which, after all, it was not physically selling in French territory. After demonstrating to the court that Yahoo could use geolocation software to explicitly deny certain items to computer users in France, the French state won its case. As a result, Yahoo

[10] So the conclusion of Weimann and Tsfati (2002). Readers should also note that the manuscript was finalized before whistleblower Edward Snowden brought the US NSA’s ‘Prism’ and the British GCHQ’s ‘Tempora’ programs to the general public’s attention.

'voluntarily' removed all such items for sale everywhere. In a less successful case, the German government attempted to shut down a far right website hosted in the USA. Its attempt provoked such outrage that, in defence of the principle of freedom of speech, even a number of American universities volunteered to host the site. In recent years, European countries have increasingly been turning to 'non legislative' approaches: urging hosts to voluntarily remove material which violates codes of conduct, rather than resort to legal measures. An example of this would be the European Union's recent 'clean IT' initiative. Despite insisting that much of the 'terrorist' content available on the Internet is specifically illegal, this strategy proposes addressing the issue by means of 'having a variety of stakeholders identify general principles and best practices, and start a permanent public-private dialogue', rather than by specific legal sanctions or technical attempts at Web filtering.

The issue of Internet censorship has been given new relevance by the outcry over legislation proposed in the United States such as the *Stop Online Piracy Act* or SOPA. While SOPA was directed against copyright infringement, it envisaged broad enforcement mechanisms (such as requiring search engines to remove links to whole sites hosting offending content) which, in principle could have been extended to other forms of illegal content as well. At the time of writing, SOPA has been withdrawn by its sponsors due to massive industry and public opposition, but alternative legislation may raise similar concerns.

Responding to Radicalisation into Terrorism on the Internet

The notion of 'radicalisation on the Internet' is problematic, not least because of the difficulties inherent in the concept of radicalization itself, but also because of the difficulties in determining in what senses this radicalization is an online issue. If radicalization 'on the Internet' is about the dissemination of illegal content, then it falls under the (rather haphazard) attempts of governments to restrict this content as outlined in the section above. If, on the other hand, it is about the emergence of genuine criminal conspiracies, then it falls under 'instrumental use' in the section before.

There has, however, been a fashion in counterterrorism thinking which holds that it is necessary not only to respond to 'violent extremism' as something located discursively within content, or to extremist violence as something located in the material world, but to violent radicalization as a process arising, presumptively, from the interaction between certain sorts of online content and particular individuals.[11] As a result, there has been quite an extensive interest in the possibility of using the Internet as a medium for disseminating a 'counter-narrative' with the aim

[11] It is worth observing that there is considerable uncertainty about the importance of the Internet in processes of radicalization into terrorism. In a systematic review of the literature, Wikstrom and Bouhana have argued that the medium seems to play a surprisingly limited role. See Bouhana and Wikström (2011).

of disrupting and mitigating the supposed effects of violent extremist discourse online. For example, in 2010 the National Counterterrorism Coordinator of the Netherlands published an edited volume on ‘Countering Violent Extremist Narratives’, while in January 2011, the United Nations Counter Terrorism Implementation Task Force held a conference in Riyadh on the subject of ‘Use of the Internet to Counter the Appeal of Extremist Violence’.[12] In the UK, a dedicated unit of the Home Office, the *Research, Information and Communication Unit* (RICU) has been established with a similar purpose.

Quite apart from normative concerns about whether government ought to be playing a role in, in effect, telling people what to think, there is very little evidence at present to determine whether online counter-narrative strategies are likely to be effective, and indeed there is at least a good possibility that they may be counter-productive. In trying to develop strategies for counter-narrative online, governments find themselves on the horns of a dilemma. One option is to ‘go online’ in an official capacity in order to respond directly to their detractors. In this case, given that the people the government is trying to reach are almost by definition unlikely to consider the government a credible source, the effectiveness of the approach seems limited. An example of this difficulty is provided by the case of the US Department of State ‘Digital Outreach Team’. This special, multilingual unit is dedicated to the task of entering Web forums in order to ‘explain US foreign policy and counter misinformation’. An assessment of the effectiveness of the initiative by Lina Khatib suggests that the team struggles with a generally very hostile reception which tends to overload its capacity to respond effectively, potentially creating the impression that it cannot Khatib et al. (2011). There is also the problem of what happens if government agents are seen to be engaging online with ‘terrorists’.

Governments can obviate some of these difficulties by concentrating instead on mobilizing civil society and partners to create their own online ‘counter-narratives’. But if the government is seen to be directly involved in this, it risks undermining the credibility and authority of these partners and thereby undermining the very rationale for engaging with them in the first place. As Olivier Roy has opined regarding attempts by governments to oppose the specific issue of Islamist extremism: ‘to promote ‘good Islam’ through governmental means is to give the kiss of death to liberal Muslim thinkers’ Roy (2008). This has led some writers on the subject of countering online radicalization to call for very broad based initiatives aimed at strengthening citizenship education and civic values. However, as worthy as such initiatives sound, the ability of such measures to have a significant impact on the dissemination of radical views (which, after all, represent dissent from the mainstream by definition) is far from obvious.

[12] On the latter, see http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_riyadh_conference_summary_recommendations.pdf.

Conclusion: Civil Liberties Versus Security

To discuss the need to counter terrorism online presumes that terrorism has a meaningful online presence. As we stated above, the Internet affords new kinds of political action, bypassing the traditional media's gate-keeper function – some of it criminal. It also helps to amplify the mediated impacts of terrorism, and to complicate the cultural effects of the phenomenon by opening up all manner of different niches within which the meanings of particular terrorist acts can be constructed. But whether these processes really serve to complete a cycle of violence is uncertain.

Within Western countries, there has neither been an epidemic of successful mass casualty bombings, nor of devastating cyber-attacks on critical infrastructure. Even if we concern ourselves more generally with violence perpetuated by those groups against which the so-called 'war on terror' has been waged it does not seem that the production of megabytes of radical data has correlated with the production of corpses. The Taliban today, for example, are incomparably more 'wired' than the Vietcong were, but so far they have killed only about 8 % as many American soldiers.[13] It might, therefore, make more sense if policies aimed at addressing the role of the Internet in terrorism focused on the issues as they actually are. This could entail maintaining a modest focus on ensuring that the current reticence among potential terrorists about using the Internet as a means to organise is not reversed, combined with attempts to address issues of online radicalisation not with a view to preventing violence but rather to preventing the mutual suspicion and hostility that fear of terrorism engenders as an ill in its own right.

[13] According to US national archives, 58,193 Americans died in the Vietnam War, of which 47,406 were killed as a direct result of hostilities. So far, the US Defense Department reports that 4,422 US soldiers have died as a result of Operation Enduring Freedom (whether 'in action' or for 'non-hostile' reasons).