THE INTERNATIONAL
CENTRE FOR THE STUDY
OF RADICALISATION AND
POLITICAL VIOLENCE

ICSR

Countering Online Radicalisation
A Strategy for Action

A policy report published by the International Centre for the Study of Radicalisation and Political Violence (ICSR)

In partnership with the Community Security Trust

ABOUT THIS REPORT

The authors of this report are Tim Stevens and Dr. Peter R. Neumann. The research for this report could not have been undertaken without the kind and very generous support of:

The Community Security Trust, London
Rena Shulsky and Dr. Sami David, New York

The views expressed in this report do not necessarily reflect the opinions of any of the project's sponsors.

All URLs (web links) mentioned in this report were active on 28 January 2009.

ABOUT ICSR

The International Centre for the Study of Radicalisation and Political Violence (ICSR) is a unique partnership in which King's College London, the University of Pennsylvania, the Interdisciplinary Center Herzliya (Israel) and the Regional Center for Conflict Prevention Amman (Jordan) are equal stakeholders.

The aim and mission of ICSR is to bring together knowledge and leadership to counter the growth of radicalisation and political violence. For more information, please visit **www.icsr.info**.

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
138 – 142 Strand
London WC2R 1HH
United Kingdom
T. + 44 20 7848 2065
F. + 44 20 7848 2748
E. mail@icsr.info

Like all other ICSR publications, this report can be downloaded free of charge from the ICSR website at **www.icsr.info**.

Executive summary

Political extremists and terrorists are using the internet as an instrument for radicalisation and recruitment. This report – resulting from the first systematic effort to bring together industry, experts and government on the issue of online radicalisation – examines what can be done by governments, industry and civil society to counter their activities.

Most governments have focused on technical solutions, believing that removing or blocking radicalising material on the internet will solve the problem. Yet, this report shows that any strategy that relies on reducing the availability of content alone is bound to be crude, expensive and counterproductive. Radicalisation is largely a real-world phenomenon that cannot be dealt with simply by 'pulling the plug'.

The analogy with countering child sexual abuse on the internet is flawed, because much of the material involved in child sexual abuse is clearly illegal and there are no political constituencies which might be offended if repressive action is taken against it.

Any strategy that hopes to counter online radicalisation must aim to create an environment in which the production and consumption of such materials become not just more difficult in a technical sense but unacceptable as well as less desirable. Elements of this strategy include:

- Deterring the producers of extremist materials
- Empowering online communities to self-regulate
- Reducing the appeal of extremist messages
- Promoting positive messages

The report thus develops concrete proposals for action within each of the four strands:

- Deterring producers
  The *selective use of takedowns in conjunction with prosecutions would* signal that individuals engaged in online extremism are not beyond the law.
- Empowering online communities
  The *creation of an Internet Users Panel* in order to strengthen reporting mechanisms and complaints procedures would allow users to make their voices heard.
- Reducing the appeal
  More attention must be paid to media literacy, and a comprehensive approach in this area is badly needed.
- Promoting positive messages
  The *establishment of an independent start-up fund* would provide seed money for grassroots online projects aimed at countering extremism.

Efforts to counter online radicalisation must view new technologies and modes of interaction not as a threat but as an opportunity. Relying on government alone is not sufficient. It is vital to capitalise upon the potential contributions of all stakeholders, including internet companies and internet users.

Contents

Figures

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Abbreviations

ADL	Anti-Defamation League
AOL	America Online
BBC	British Broadcasting Corporation
BT	British Telecom
ELF	Earth Liberation Front
GPS	Global Positioning System
ICT	Information Communications Technology
INACH	International Network Against Cyberhate
ISP	Internet Service Provider
ISPA	Internet Services Providers Association
IP	Internet Protocol
IWF	Internet Watch Foundation
MI5	British Security Service
MNet	Media Awareness Network
NGO	Non-Governmental Organisation
URL	Uniform Resource Locator
SEO	Search Engine Optimisation
SHAC	Stop Huntingdon Animal Cruelty

1 Introduction

No other recent development is likely to be more profound in its long-term impact on global society than the information revolution and the rise of the internet. It is impossible to say how many websites there are, partly because the numbers are changing so quickly; a recent survey estimated that more than a million websites were added every month in 2008.[1] The search engine Google had indexed one trillion webpages by July 2008,[2] but – according to its own chief executive – it only captures a miniscule percentage of what is currently online.[3]

Nearly 70 per cent of British adults now use the internet every day, an impressive rate considering it was virtually unknown outside government, academia and the technology community only twenty years ago.[4] Britain is the most active online country in Europe, with each user spending nearly 35 hours online every month.[5] In fact, for young people in Britain, the internet has – for the first time – overtaken television as the 'most indispensable' medium.[6]

In an astonishingly short period of time, therefore, the internet has become an essential part of our lives. Nearly every group or social actor who plays a role in real life is represented online, and it should come as no surprise that political extremists and terrorists too have taken advantage of this new medium. This report deals with their activities and, especially, what can be done to limit their impact.

In doing so, the report focuses on online radicalisation and, more specifically, how governments and civil society can counter these activities within the framework of a liberal democratic society (for definitions of key terms, see Box 1). It does not discuss the operational use of the internet by terrorists nor the threat from cyber-terrorism (that is, terrorist attacks against computers or computer infrastructure).

Framing the argument

There have been many reports looking at the online activities of extremists, but most of their policy recommendations are either stating the obvious ('promote the activities of those who speak out against violent extremism')[7] or avoiding the tough questions altogether ('invoke the full force of the law where it makes most

[1] Netcraft, *Web Server Survey*, August 2008; available at http://news.netcraft.com/archives/2008/08/29/august_2008_web_server_survey.html).
[2] Jesse Alpert & Nissan Hajaj, 'We knew the web was big', *Official Google Blog*, 25 July 2008; available at http://googleblog.blogspot.com/2008/07/we-knew-web-was-big.html.
[3] Eric Schmidt, speech to Association of National Advertisers Annual Conference, 8 October 2005; available at http://ana blogs.com/conference/2005/10/google_ceo_eric.html.
[4] Office of National Statistics, *National Statistics Omnibus Survey*, 26 August 2008; available at http://www.statistics.gov.uk/pdfdir/iahi0808.pdf.
[5] comScore, *World Metrix*, June 2007; available at http://www.comscore.com/press/release.asp?press=1459.
[6] Ofcom, *The Communications Market 2008* (London: Ofcom, 2008); available at http://www.ofcom.org.ukresearch/cm/cmr08/keypoints/.
[7] J. Rami Mroz, *Countering Violent Extremism: Videopower and Cyberspace* (New York: EastWest Institute, February 2008); available at http://www.ewi.info/pdf/Videopower.pdf.

sense to do so').[8] Few have made an effort to address the dilemmas and questions that policymakers are faced with in responding to the extremist challenge.

At its core, the policy dilemma is neither new nor unprecedented. Democratic governments must respect and uphold individual rights to freedom of speech and expression even when people's views are distasteful and objectionable. At the same time, if democracy and its freedoms are to survive, governments must protect civil society from political extremists. They must counter ideas and activities that polarise communities, undermine the democratic process and lead to violence. The question is: how far can one go in protecting democracy without jeopardising the very liberties one wishes to protect?[9]

This question – 'how far can we go?' – is the key dilemma for any liberal state when confronted with 'subversion' and political violence, and has been central to many of the debates that have taken place in the years since the September 11, 2001 terrorist attacks against the United States. It also underlies the discussion about the potential use of *'negative' measures* aimed at denying access to information, in particular the materials published by political extremists. When considering removing websites, filtering or other forms of blocking content, democra tic governments have (rightly) been torn between wanting to protect society from harm whilst being conscious of the political backlash and loss of legitimacy that could result from attempts to limit free speech and censor the internet.

If one is to believe some of the participants in this debate, the solution is simple: the laws and conventions that apply to 'conventional' media (newspapers, radio, television, etc.) should also be used to regulate the internet. There is no reason at all – so the argument goes – that incitement to murder should be tolerated on the internet when it would be illegal in a newspaper or radio programme. In reality, though, most experts recognise that the enormous size of the internet as well as its decentralised nature and transnational reach make the implementation of this principle more difficult than it would be with conventional media. More fundamentally, the argument ignores the increasingly 'conversational' nature of the internet, with vast amounts of 'user-generated content',[10] web forums, instant messaging and other kinds of online material.

As a result, an important element of the debate about countering online radicalisation has been the discussion of *'positive' measures*; that is, ways in which extremists' political messages can be challenged and/or neutralised through alternative messages or other, more attractive forms of content that will reduce the extremists' 'audience share'. Here, the dilemma is not ethical but practical. What kinds of positive measures work? How can governments help, and at what point does their support become a hindrance?

[8] Frank J. Cilluffo and Gregory Saathoff, *NETworked Radicalization: A Counter-Strategy*, George Washington University Homeland Security Policy Institute and the University of Virginia Critical Incident Analysis Group, May 2007; available at http://www gwumc.edu/hspi/reports/NETworked Radicalization_A Counter Strategy.pdf.

[9] In the words of Paul Wilkinson: 'It is vital to understand that human rights protection is not an optional extra in the fight against terrorism; it is an *essential weapon* or *asset* in the protection of democracy" [original emphasis]. See Paul Wilkinson, *Terrorism versus Democracy: The Liberal State Response*, 2nd edn. (London & New York: Routledge, 2006), p.210.

[10] For a definition and discussion of user-generated content, see OECD, *Participative Web: User-Created Content*, Directorate for Science, Technology and Industry, 2007; available at http://www.oecd.org/dataoecd/57/14/38393115.pdf.

This report will show that the popular dichotomy between positive and negative measures – while useful in conceptualising the policy dilemma – provides only a limited range of options for dealing with online radicalisation. If the problem is to be dealt with comprehensively, it needs to be recognised that radicalisation is a 'virtual' phenomenon only in part, and that any attempt at countering it needs to be anchored in the 'real world'. Furthermore, even when focusing on cyberspace, it becomes obvious that there are a range of additional instruments and approaches which defy the negative/positive dichotomy: for example, deterring the producers of extremist materials; empowering online communities to self-regulate; and reducing the appeal of online extremism through education.

The report argues that a comprehensive strategy for countering online radicalisation will have to draw on all these instruments and approaches in order to be effective. The aim is to create an environment in which the production and consumption of such materials become not just more difficult in a technical sense but unacceptable as well as less desirable.

Scope

Before delving into the analysis, it is vital to explain what has been looked at – and what not. First, the primary focus of this report is the situation in the United Kingdom. Since the British Home Secretary declared that the internet was 'not a no-go area for government' at the ICSR launch conference in London in January 2008,[11] the question of what exactly government can and/or should do to counter radicalisation and recruitment online has preoccupied policymakers and experts. It is within this national political context that this report hopes to make a contribution. However, the analysis and conclusions will be of considerable interest beyond the British context. Nearly all Western democracies face the same dilemmas and tough questions. Even if political, legal, and societal conditions may differ in each case, it is hoped that many of the principles and ideas contained in this report will stimulate the debate in other countries.

Second, although Al Qaeda-inspired Islamist militants represented the most significant terrorist threat to the United Kingdom at the time of writing,[12] Islamist militants are not the only – or even the predominant – group of political extremists engaged in radicalisation and recruitment on the internet. Visitor numbers are notoriously difficult to verify, but some of the most popular Islamist militant web forums (for example, *Al Ekhlaas*, *Al Hesbah*, or *Al Boraq*)[13] are easily rivalled in popularity by white supremacist websites such as Stormfront.[14]

[11] Jacqui Smith, 'Keynote address', ICSR inaugural conference, King's College London, 17 January 2008; available at http://icsr.info/files/ICSR Remarks by Jacqui Smith.pdf.

[12] This seems to be the view of the Director General of the Security Service, expressed in a series of interviews in January 2009. See, for example, Michael Evans, 'MI5's spymaster Jonathan Evans comes out of the shadows', *The Times*, 7 January 2009.

[13] Al Ekhlaas and Al Boraq appear to be semi-permanently offline. See NEFA Foundation, 'Al Fajr Media Centre: Regarding the Closing of Several Jihad Web Forums', 29 September 2008; available at http://www.nefafoundation.org/miscellaneous/nefafajrforums1008.pdf. See also Ian Black, 'Cyber-attack theory as al-Qaida websites close', *The Guardian*, 22 October 2008.

[14] Stormfront was founded in 1995 by ex-Grand Wizard of the Ku Klux Klan, Don Black. As of January 2009, the web forum (http://www.stormfront.org/forum/) boasted over 150,000 members, of whom over 31,000 were noted as 'active'.

Single-issue groups such as environmentalist extremists and radical animal rights activists also have a strong web presence.[15]

All the conclusions and recommendations are meant to be applied to extremist groups across the board. Indeed, any governmental initiative – however well-conceived – that is seen to be directed solely at the Islamist end of the spectrum will risk being counter-productive.

Methodology and structure

The research which informs this report was carried out over a period of eight months, from June 2008 to early February 2009. Its approach is qualitative, with evidence based on a combination of primary and secondary sources.

The research began with an extensive review of the existing literature, including relevant academic publications on extremism, radicalisation and recruitment, as well as the internet, media and communication. Numerous policy reports, as well as summaries from roundtable discussions, seminars and workshops were consulted. In addition, the research team conducted nearly fifty semi-structured interviews with experts, members of civil society, industry and government. Needless to say, the process also involved looking at countless websites of extremists and those trying to counter them.

Moreover, the research team participated in a dozen international conferences dealing with the topic, and organised two one-day workshops at King's College London which brought together representatives from industry, government, media and civil society and engaged them in a systematic discussion about the issues dealt with in the report. In fact, it is believed that this is the first project which has brought all the stakeholders in the debate about online radicalisation to the table.

The structure of the report broadly follows the questions and dilemmas set out earlier in this chapter. Chapter 2 aims to provide a more sophisticated understanding of radicalisation and recruitment in the context of the internet. Chapter 3 assesses the effectiveness and potential implications of negative measures, which continue to occupy a prominent place in the public debate about how online radicalisation can and/or should be countered.

Building on this analysis, Chapters 4–7 contain a series of policy proposals based on the various instruments and approaches that could form part of a comprehensive strategy against online radicalisation: Chapter 4 addresses the question of how to deter the producers of extremist materials and delineates the idea of strategic prosecutions; Chapter 5 explores ways to empower online communities to self-regulate and proposes the creation of an Internet Users Panel; Chapter 6 examines what can be done to reduce the appeal of extremist messages and argues that media literacy needs to be strengthened; Chapter 7 returns to the idea of 'positive' measures and proposes the establishment of an independent start-up fund through which to support counter-extremist grassroots initiatives.

Chapter 8 sums up the findings and sets out the parameters of what is believed to be a balanced and comprehensive approach to countering online radicalisation.

[15] For a summary of Stop Huntingdon Animal Cruelty (SHAC)'s use of the internet in preparing and waging campaigns of violence, see David Kocieniewski, 'Six Animal Rights Activists Are Convicted of Terrorism', *New York Times*, 3 March 2006; available at http://www.nytimes.com/2006/03/03/nyregion/03animals.html?_r=1. For the use of the internet by the Earth Liberation Front (ELF), see Gary A. Ackerman, 'Beyond Arson? A Threat Assessment of the Earth Liberation Front', *Terrorism and Political Violence*, Vol.15, No.4 (2003), pp.143-170. For further background on 'ecoterrorist' activity and the internet, see Anti-Defamation League, 'Ecoterrorism: Extremism in the Animal Rights and Environmental Movements'; available at http://www.adl.org/learn/ext_us/Ecoterrorism.asp?LEARN_Cat=Extremism&LEARN_SubCat=Extremism_in_America&xpicked=4&item=eco.

BOX 1 Key terms & Definitions

CYBERSPACE Cyberspace is the total landscape of technology-mediated communication. This includes not only the internet and the World Wide Web but also mobile and fixed phone networks, satellite and cable television, radio, the Global Positioning System (GPS), air traffic control systems, military rocket guidance systems, sensor networks, etc. As more devices become interlinked through the processes of digital convergence, cyberspace is rapidly covering more of our physical world and channels of communication and expression. Importantly, cyberspace also includes the people that use these devices and networks.

THE INTERNET A subset of cyberspace, the internet is a system of interconnected computer networks. The internet is comprised of both hardware and software that facilitate data transfer across a network of networks, ranging from local to global in scale, and encompassing private, public, corporate, government and academic networks. Functioning primarily as a global data exchange system, it carries a wide range of resources such as email, instant messaging, file transfer, virtual worlds, peer-to-peer file sharing, and the World Wide Web.

THE WEB The World Wide Web (or, simply, web) is a more recent development than the internet, with its origins in the European academic community of the late 1980s. The web is one of the many services reliant on the internet. It consists of an assemblage of files (audio, video, text, and multimedia), each assigned an address, which are connected to one another through the formation of hyperlinks (more commonly, links). The contents of the web are (usually) accessed via the internet using software known as browsers.

USER-GENERATED CONTENT User-generated content (also user-created content) is an umbrella term referring to a wide range of online materials that are created by internet users themselves. User-generated content has blurred the distinction between the ‘producers’ and ‘consumers’ of information. It is thought to be behind the massive expansion of the internet in recent years, which now encompasses a wide variety of blogs, discussion and review sites, social networking sites, and video and photo sharing sites.

RADICALISATION Most of the definitions currently in circulation describe radicalisation as the process (or processes) whereby individuals or groups come to approve of and (ultimately) participate in the use of violence for political aims. Some authors refer to ‘violent radicalisation’ in order to emphasise the violent outcome and distinguish the process from non-violent forms of ‘radical’ thinking.

EXTREMISM Extremism can be used to refer to *political ideologies* that oppose a society’s core values and principles. In the context of liberal democracies this could be applied to any ideology that advocates racial or religious supremacy and/or opposes the core principles of democracy and universal human rights. The term can also be used to describe the *methods* through which political actors attempt to realise their aims, that is, by using means that ‘show disregard for the life, liberty, and human rights of others’.[16]

[16] Roger Scruton, *The Palgrave Macmillan Dictionary of Political Thought*, 3rd edn. (Basingstoke: Palgrave Macmillan, 2007).

2 Radicalisation and the Internet

In few other areas of policymaking is the need for a sound understanding of the problem more urgent than with online radicalisation. Though everyone uses the internet, most members of the public – including many policymakers and politicians – have only the most cursory idea of how it works. Awful things are said to happen on extremist websites and in internet chat rooms, but few are able to identify what exactly it is that causes so much concern. As a result, many of the policy proposals that are currently in circulation are either irrelevant or unworkable. It is essential, therefore, to begin the analysis by taking another look at the nature of the problem.

This chapter will set out the particular areas and functions that make the internet a problematic environment in relation to radicalisation. It will be shown that the internet can play a role in radicalisation, but that so far it has not been the principal driver of the process. Furthermore, it will be demonstrated that the process of radicalisation – even where it has a virtual dimension – remains rooted in the real world. Consequently, any strategy aimed at countering radicalisation on the internet needs to be part of a more comprehensive approach.

The role of the internet

Political extremists and those in the process of radicalisation use the internet for the same reasons, and in broadly the same manner, as the vast majority of the online public. It may be useful, therefore, to begin by looking at the principal ways in which the internet has revolutionised the world of communication:

- It has dramatically reduced the cost of communication, making the exchange and dissemination of information virtually free.
- It has enabled unlimited access to much of the world’s knowledge and begun to organise it in systematic fashion.
- It has made it easier to find people and create networks among like-minded individuals, across great distances and beyond national borders.
- It has lowered the threshold for engaging in ‘risky’ or ‘embarrassing’ behaviour because it helps to conceal users’ identities.

In many respects, these have been positive developments. The *New York Times* columnist Thomas Friedman claims that the internet has helped create ‘super-empowered individuals’ and predicts a renaissance of civic engagement.[17] Similarly, former US President Bill Clinton argues that, because of the internet, people can ‘do more public good than ever before’.[18] Indeed, there can be no question that the internet is a great educational resource; it facilitates cross-cultural exchange; it helps non-governmental and other organisations with

[17] Thomas L. Friedman, *The Lexus and the Olive Tree* (New York: Farrar, Straus and Giroux, 1999), pp. 13, 381

[18] ‘Remarks of former U.S. President Bill Clinton’, *Harvard University Gazette*, 6 June 2007; available at http://www.news.harvard.edu/gazette/2007/06.07/99-clinton.html.

small budgets to disseminate their ideas; it allows small businesses to sell their products worldwide; and it gives sufferers of rare diseases the opportunity to create support networks.

The difference between such benign uses of the internet and the activities of political extremists lies not primarily in their nature but, rather, in the content of the information that is being exchanged and the purposes for which it is used. Like other, less problematic non-governmental organisations (NGOs), extremist groups too appreciate the opportunity to disseminate their ideas at little or no cost; they take advantage of the vast amount of knowledge and information that is available online; they use the internet to maintain (virtual) networks and communities of like-minded individuals; and – perhaps not quite like conventional NGOs – they cherish the fact that the internet makes it difficult for their individual identities to be revealed.

A whole range of online activities, therefore, can be said to be relevant and beneficial to extremist organisations. Based on the research, there are three aspects of the internet which can be thought of as *particularly* problematic in the context of radicalisation and recruitment:

- The internet can be used by extremists to *illustrate and reinforce* ideological messages and/or narratives. Through the internet, potential recruits can gain near-instantaneous access to visually powerful video and imagery which appear to substantiate the extremists' political claims.
- The internet makes it easier to *join and integrate* into more formal organisations. It provides a comparatively risk-free way for potential recruits to find like-minded individuals and network amongst them, enabling them to reach beyond an isolated core group of conspirators.
- It creates a new social environment in which otherwise *unacceptable views and behaviour are normalised*. Surrounded by other radicals, the internet becomes a virtual 'echo chamber' in which the most extreme ideas and suggestions receive the most encouragement and support.

It seems obvious, then, that the internet can have a role in intensifying and accelerating radicalisation. In fact, one may argue that the internet is of particular benefit to marginal and/or illegal groups and movements, because it facilitates the formation of (virtual) communities which would be more 'risky', if not impossible, to establish in the real world. There can be no doubt, therefore, that the internet is problematic, but is it the problem?

The role of human interaction

Despite the problematic aspects highlighted in the previous section, there continues to be little evidence to support the contention that the internet plays a *dominant* role in the process of radicalisation. The case of Younis Tsouli, better known as 'Irhabi007' ('terrorist007'), who joined a number of popular web forums in early 2004 and quickly emerged as the undisputed superstar of 'jihadism online', received so much attention precisely because it represented an exception.[19]

Self-radicalisation and self-recruitment via the internet with little or no relation to the outside world rarely happens, and there is no reason to suppose that this situation will change in the near future.

The reason for the absence of self-radicalisation and self-recruitment online is that real-world social relationships continue to be pivotal. Many experts who have studied the problem have concluded that the internet can support and facilitate but never completely replace direct human contact and the ties of friendship and kinship through which intense personal loyalties form.[20] This chimes with the observations that were made in the course of an earlier research project which looked at recruitment for the Islamist militant movement in Europe.[21] None of the radicals or former radicals that were interviewed had been radicalised or recruited solely on the internet. A university imam from London explained why: 'Human contact is important because [radicalisation and recruitment] is all about who knows who. One guy knows a friend who knows a friend, and so on'.[22]

Similarly, an ongoing research project funded by the Economic and Social Research Council found that much of the jihadist web presence was about 'preaching to the choir'. While the internet provides a convenient platform for activists to renew their commitment and reach out to like-minded individuals elsewhere, it is largely ineffective when it comes to drawing in new recruits.[23]

From the extremists' perspective, the internet's failure to provide face-to-face human interaction nullifies many of its advantages. According to the social movement theorist Quintan Wiktorowicz, exceptionally 'risky' behaviours, such as engaging in violence or crime, always require social networks in order for the perceived cost/benefit calculation to tip in their favour. Involvement in violence needs to be preceded by a prolonged process of 'socialisation' in which perceptions of self-interest diminish and the value of group loyalties and personal ties increase.[24] This corresponds with the thrust of the argument made by the American academic Marc Sageman, who contends that, '[f]or the type of allegiance that the jihad demands, there is no evidence that the internet is persuasive enough by itself'.[25]

As the recent case of Hamaad Munshi shows, the processes of radicalisation and recruitment are anchored in the real world (see Box 2). It is unlikely that they can be understood or countered effectively if all the attention is exclusively focused on the portion which occurs online. Where radicalisation has a virtual component, that element needs to be seen as part of an iterative process through which events and developments in the real world are fed into cyberspace and vice versa. As a result, any policy aimed at tackling online radicalisation must account for and be embedded within a more comprehensive approach that reflects the real-world nature

[19] See SITE Institute, 'Irhabi 007 Unveiled: A Portrait of a Cyber-Terrorist', *SITE Report*, 2006; and Evan F. Kohlmann, 'The Real Online Terrorist Threat', *Foreign Affairs*, Vol.85, No.5 (2006), pp.115-124.

[20] See, for example, Marc Sageman, *Understanding Terror Networks* (Philadelphia, PA: Pennsylvania University Press, 2004), p. 163.

[21] Peter R. Neumann and Brooke Rogers, *Recruitment and Mobilisation for the Islamist Militant Movement in Europe*, ICSR, King's College London, on behalf of the European Commission Directorate-General for Justice, Freedom and Security, October 2008; available at http://www.icsr.info/files/ICSR EU Research Report_Proof 01.pdf.

[22] Abu Musa, interviewed August 2007.

[23] Andrew Hoskins, Ben O'Loughlin and Akil Awan, *Legitimising the Discourses of Radicalisation: Political Violence in the New Media Ecology. Interim Report*, ESRC New Security Challenges Programme.

[24] Quintan Wiktorowicz, 'Joining the Cause: Al Muhajiroun and Radical Islam', paper presented at 'The Roots of Islamic Radicalism' conference, Yale University, May 8-9 2004; available at http://www.yale.edu/polisci/info/conferences/Islamic Radicalism/papers/wiktorowicz-paper.pdf.

[25] Sageman, *Understanding Terror Networks*, p. 163.

of the problem. It is impossible, therefore, to solve the radicalisation problem by simply ‘pulling the plug’, and it is a serious mistake to believe that the problem would go away if only the internet could be cleaned up. Nevertheless, whatever potential might exist for such measures in countering online radicalisation will be explored in the next chapter.

BOX 2 CASE STUDY Hamaad Munshi

In September 2008, a sixteen-year-old teenager from Dewsbury, Hamaad Munshi, was found guilty of possessing materials that were likely to be used in acts of terrorism. Labelled ‘Britain’s youngest terrorist’ by the press,[26] Munshi collected instructions for making napalm, high explosives and suicide vests, and was a member of a British group of ‘online jihadists’ who regularly shared extremist videos and spent hours discussing their plans to travel to Pakistan and die as ‘martyrs’.

Much of Munshi’s extremist activism took place online, but his radicalisation had been initiated in the ‘real world’. Through a common friend, Munshi had met Aabid Khan at Dewsbury central mosque. Khan had attended a terrorist training camp in Pakistan and served as a recruiter for the Islamist militant movement in the Dewsbury area.[27] He also had a history of online jihadist activity and was closely connected to the ‘superstar’ of jihadism online, Younis Tsouli (‘terrorist007’), as well as a number of foiled bomb plotters in Sarajevo, Washington DC, and Toronto. Khan spotted Munshi’s knowledge of computers, and carefully groomed him to become a leading part of his online network.

As with Khan, whose real world contacts informed his online activities, Munshi’s radicalisation too was a combination of face-to-face interaction and virtual consolidation. His online communication with a closed network of like-minded and older individuals consumed much of his time and represented the defining feature of his extremist existence. But it was the early meetings with Khan and some of his friends that helped turn a boy interested in religion into a young man dedicated to killing ‘non-believers’.

[26] See for example, ‘Britain’s youngest terrorist, Hammaad Munshi, faces jail after guilty verdict’, *The Times*, 18 August 2008.
[27] Evan Kohlmann (2008), ‘Anatomy of a Modern Homegrown Terror Cell: Aabid Khan *et al* (Operation Praline)’, *NEFA Foundation report*, September 2008; available at http://www.nefafoundation.org/miscellaneous/nefaaabidkhan0908.pdf.

3 Negative measures

In recent years, policymakers not only in Britain but across the Western world have considered the possibility of denying internet users access to extremism-related content. The rationale seems to be that if access to such material is restricted, fewer people will be able to view it and consequently become radicalised. As the previous chapter demonstrated, the relationship between internet use and radicalisation is not as straightforward as the argument suggests. Still, the proposition that some or all of the content related to violent extremism on the internet can be made unavailable, and will therefore reduce extremist radicalisation, merits examination.

This chapter looks at the effectiveness of negative measures in countering online radicalisation. In doing so, it considers the various technical options that can be used to remove, filter or hide content and assesses their effectiveness. More important, it then discusses the wider implications of employing such measures in the context of a liberal democracy, focusing in particular on the United Kingdom.

What will be shown is that some of the positive experiences with filtering images of child sexual abuse are difficult to transfer to the area of violent radicalisation. Indeed, it will be concluded that the systematic, large-scale deployment of negative measures would be impractical, and even counterproductive: it would generate significant (and primarily political) costs whilst contributing little to the fight against violent extremism.

Technical options

Much of the debate about negative measures is highly technical, which has made it difficult for non-experts to follow and participate in the discussion.[28] For the benefit of the general reader, this section aims to describe the principles – not the technical details – behind different kinds of negative measures, and to evaluate their effectiveness in denying users access to extremism-related content. In general, the various tools that have been deployed by governments in recent years can be grouped into three categories: *removing* content from the web; restricting users’ access and controlling the exchange of information *(filtering)*; and manipulating search engine results, so that undesirable content becomes more difficult to find *(hiding)* (see Table 1). Each will be looked at in turn.

Removing

Removing websites is possible because all websites rely on two services to make their content available: a ‘hosting’ company which provides online storage, and a ‘domain name provider’ which supplies

[28] For technical background, see Steven J. Murdoch and Ross Anderson, ‘Tools and Technology of Internet Filtering’, in Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA. & London: MIT Press, 2008); see also Johnny Ryan, *Countering Militant Islamist Radicalisation on the Internet: A User Driven Strategy to Recover the Web* (Dublin: Institute of European Affairs, 2007).

the website addresses (or Uniform Resource Locators, URLs) through which the site can be accessed. Hence, if a government wishes to remove an unacceptable website, it instructs the hosting company to 'take down' its content or asks the domain name authority to deregister the relevant domain. Either way, the website becomes inaccessible and will, effectively, have been removed from the internet.

For this method to be effective, however, the service providers need to be located in the same jurisdiction as the government that wishes to remove a particular website. If the website is hosted outside that country, it will become difficult – if not impossible – for the government to exercise authority over the hosting company.[29] Likewise, unless the website has a country-specific top-level domain (for example, '.uk'), which is operated by a national registry,[30] governments have little power to request deregistration of a domain name. Even where hosting or domain name providers are located within a government's jurisdiction, website operators can simply move their site to one (or several) service providers outside that jurisdiction if they feel that they are being threatened with a takedown. Therefore, while government takedowns may be considered useful in disrupting and destabilising certain websites, they are unlikely to make them inaccessible for very long.

Another, albeit less conventional, form of 'removing' websites is the Denial of Service attack. Such attacks are fairly complex: they involve the 'hijacking' of large numbers of computers that are instructed to overload particular servers and/or networks with communication requests, so that certain websites become unable to respond to legitimate traffic. In spring 2007, for example, Estonia was the target of such an attack, which 'came close to shutting down the country's digital infrastructure'.[31]

Denial of Service attacks used to be associated only with 'hackers', but some governments have recently contemplated including this method in their arsenal of 'cyber attacks' against potential adversaries.[32] In the United Kingdom, Denial of Service attacks are illegal under the Police and Justice Act (2006).[33] Even if they were to be used in countering extremist websites, such sites are likely to resurface in a different location once the attack is over. Though undoubtedly effective, they are at best a temporary means of disruption.

Filtering

Filtering differs from removal in that, rather than attacking or disabling certain websites, it aims to control the flow of information between computers that are connected through the internet. This is possible because nearly all internet users (at least 95 per cent in the United Kingdom) are connected to the internet through a small number of so-called internet service providers (ISPs) – commercial companies such as British Telecom (BT), America Online (AOL) or Tiscali – which are located within a government's jurisdiction.[34] They represent the virtual 'bottlenecks' through which a society's internet usage can be controlled.

Even so, many of the filtering technologies that are currently in use are either too crude or too expensive to operate. Take, for example, *IP filtering*. All information on the internet comes in so-called packets which, along with the actual data, contain the internet protocol (IP) address of the computer and/or web host for which the information is destined. With IP filtering, if a user wants to access a website associated with a blacklisted IP address, the request will be intentionally dropped, making it impossible to view the website. Problems with this method of filtering arise because some web hosts – each with a single IP address – provide a variety of services or host many websites with different domain names, which means that all these acceptable services and sites will be blocked as well. While cheap and easy to implement, its propensity for 'overblocking' makes IP filtering a very crude method of interdicting banned material.

An alternative method is known as *content filtering* (sometimes also referred to as dynamic filtering). Rather than banning entire IP addresses, the content filtering software 'sniffs' each information packet for content that matches a list of blacklisted keywords. This is an expensive means of filtering, because it requires whole data streams to be reassembled when keywords are split between different packets. Furthermore, because many sites that contain blacklisted keywords may not be extremist at all – some, in fact, may be dedicated to *countering* extremist propaganda – governments would also have to maintain (and constantly update) a 'white list' of permitted sites against which any request for information would be compared.

Although China deploys content filtering on a grand scale,[35] the financial costs may be considered prohibitive in different national contexts. At a philosophical level, the idea that access to information is decided purely on the basis of 'automated judgement calls determined by software designers'[36] would probably be seen as unacceptable in most liberal democracies.

Filtering can also be performed through what is known as *domain name tampering*. Whenever users type in the domain name of a website they wish to access, a computer looks up the corresponding IP address to which the data package will be directed, which means that the computer could be instructed to drop requests for banned domain names at this point. The method is relatively inexpensive, but – like IP filtering – it will overblock acceptable sites that may be part

[29] For further discussion of these problems, see Raphael F. Perl, 'Terrorist Use of the Internet; Threat, Issues, and Options for International Co-operation', *Second International Forum on Information Security*, Garmisch-Partenkirchen, 7-10 April 2008; available at http://www.osce.org/documents/cio/2008/04/30594_en.pdf.

[30] In the UK, this registry is operated by Nominet (http://www.nic.uk/).

[31] Mark Landler and John Markoff, 'Digital Fears Emerge After Data Siege in Estonia', *The New York Times*, 29 May 2007; available at http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=1&pagewanted=all.

[32] Col. Charles W. Williamson III, 'Carpet bombing in cyberspace: Why America needs a military botnet', *Armed Forces Journal*, May 2008.

[33] 'UK bans denial of service attacks', *OUT-LAW News*, 9 November 2006; available at http://www.out-law.com/page-7462.

[34] ISPA, 'Memorandum', submitted as written evidence to the UK Parliament Select Committee on Culture, Media and Sport, March 2008; available at http://www.publications.parliament.uk/pa/cm200708/cmselect/cmcumeds/353/8031806.htm.

[35] See Greg Walton, *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China* (Montréal: International Centre for Human Rights and Democratic Development, 2001); available at http://www.dd-rd.ca/site/_PDF/publications/globalization/CGS_ENG.PDF. See also Richard Clayton, Steven J. Murdoch, and Robert N.M. Watson, 'Ignoring the Great Firewall of China', unpublished paper, 2006; available at http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf.

[36] Ryan, *Countering Militant Islamist Radicalisation*, p.92

of a larger domain, such as blogging platforms or discussion groups. It is also easy to circumvent if users know the IP addresses of the sites they hope to connect with.

A more refined method is *proxy filtering*. So-called proxy servers, which produce local copies of popular websites and are commonly deployed by internet service providers to save bandwidth, can be used to decide whether to allow requests for individual webpages. This avoids overblocking, but can be very expensive. If the system were to be rolled out across entire networks and internet service providers failed to make substantial investments in the required hardware, it could slow down internet traffic substantially.[37]

Often described as the best of all worlds, *hybrid IP and proxy filtering* is a practical response to the relative expense of proxy filtering and the significant overblocking which results from IP filtering. In the first instance, this system checks against a list of IP addresses, but does not block them immediately. Instead, all requests for 'problematic' IP addresses are channelled to a proxy server which inspects them for individual webpages and blocks them if required. The initial layer makes it possible for the vast majority of internet traffic to proceed without a full inspection, thus reducing the expense of straight proxy filtering, whilst the second layer helps to minimise the problems of overblocking. Hybrid IP and proxy filtering is the basis for the British Telecom Cleanfeed system for blocking child sexual abuse content (see Box 3).

Hybrid IP and proxy filtering seems to resolve the trade-off between cost and accuracy: it is neither too crude nor is it excessively expensive. Yet, like all other methods of filtering, it fails to capture dynamic content (for example, chat and instant messaging) and relies on blacklists of banned webpages, which – as will be shown in the second section of this chapter – raises all kinds of political questions.

Hiding

For most internet users, search engines such as Google are the principal entry points to the internet: they are vital tools for finding information and navigating around the internet. Whether a website is listed by a search engine, and – if so – what public page rank it has, can be critical in determining its success.[38] Conversely, if search engines are manipulated to drop certain webpages or rank them significantly lower than others, this could be the equivalent of hiding them from public view. Governments, therefore, may be tempted to interfere with the process whereby search engines produce their results in order to make extremism related websites less visible.

One way of doing so would be to engage in search engine filtering, so that certain webpages or requests for banned keywords are dropped. The best known example is that of China, where Google has been implicated in facilitating search engine filtering via its own products. The results returned by searching for banned keywords such as 'Free Tibet' on google.cn are very different from those on, say, google.co.uk. Indeed, not only are blacklisted sites omitted, but those supporting the Chinese government and its policies are returned instead.[39] Though technically feasible, it is highly unlikely that Western governments would consider pursuing this course of action.

Another method is to alter search engine results, so that appropriate sites appear higher than inappropriate ones. This would require either a form of search engine filtering or the systematic, illicit use of search engine optimisation (SEO). SEO describes a set of techniques that are used to boost or reduce a site's page rank. Legitimate – or 'white hat' – SEO tools are part of good web design and should not be regarded as 'negative'.[40] By contrast, unapproved – or 'black hat' – SEO techniques are widely frowned upon and, if discovered, will lead to sanctions by the search engine provider.[41]

In either case, the overall utility of using such methods may be limited. Extremist websites are not normally found via web searches on sites like Google, but because people are told about them in web forums, at schools, universities or community centres. Moreover, web searches for 'extremist' terms rarely produce the desired results. When searching for the word 'jihad', the first 100 hits returned by Google included 27 blogs of which 14 qualified as counter-jihad;[42] 19 news sites, including those of the BBC, *Time* magazine and the *Jerusalem Post*; 12 encyclopaedia entries and book reviews; and eight Islamic sites providing advice on the 'true' meaning of jihad. The remainder were a mixed bag of music, films, games and humour. Only one of the search results – the website *Jihad Unspun* – could be described as problematic, having been accused of posting controversial and pro-extremist videos.[43]

It should be evident from this small and imperfect experiment that tweaking the results for supposedly extremist terms would be largely ineffectual, not least because it is unlikely that any but the most callow wannabe terrorist would use a mainstream search engine to find banned material.

Implications

Some of the technical problems associated with deploying negative measures were described in the previous section. What should again be emphasised is that none of these measures can deal adequately with the increasingly important 'conversational' part of the internet: while it may be possible to remove, filter or hide content that is available from relatively static websites, large parts of the internet – chat rooms, instant messaging, virtual worlds and networking sites – are going to remain largely unaffected. Negative measures, therefore, are unlikely to be fully effective, and – as will be shown – their deployment generates wider costs.

[37] A figure of 87% in speed reduction was recently suggested by the Australian Communications and Media Authority. See ACMA, *Closed Environment Testing of ISP-Level Internet Content Filtering* (Belconnen, Melbourne & Sydney: ACMA, June 2008); available at http://www.acma.gov.au/webwr/_assets/main/lib310554/isp-level_internet_content_filtering_trial-report.pdf.

[38] Amy Langville and Carl Meyer, *Google's PageRank and beyond: the science of search engine rankings* (Princeton, NJ: Princeton University Press, 2006).

[39] OpenNet Initiative, 'Probing Chinese search engine filtering', *Bulletin*, No.5, 19 August 2004; available at http://opennet.net/bulletins/005.

[40] See for example Google's 'Webmaster Guidelines'; available at http://www.google.com/support/webmasters/bin/answer.py?hl=en&answer=35769.

[41] See SEO Black Hat website (http://seoblackhat.com/)

[42] See Toby Archer, 'Countering the counter-jihad', *RUSI Homeland Security and Resilience Monitor*, Vol.7, No.7 (2008), pp.7-11.

[43] Criticism of the *Jihad Unspun* website (http://www.jihadunspun.com/index.php) is rife in the counter-jihad and right-wing blogosphere. See, for example, Bill Roggio, 'The Taliban Kidnap One of Their Own', *The Weekly Standard*, 14 November 2008; available at http://www.weeklystandard.com/weblogs/TWSFP/2008/11/the_taliban_one_of_thei_1.asp

The term ‘cost’ does not necessarily refer to financial costs, though there are obviously going to be financial implications. If filtering technology were to be made mandatory, internet service providers would have to invest in new hardware and software. More significantly, if user-generated content and other, more dynamic parts of the internet were to be included in any new regulatory regime, this would make it necessary for website operators to hire large numbers of people responsible for the proactive monitoring of these sites. Industry sources told us that the video sharing site YouTube alone would require several hundred additional employees.[44] It is impossible to say how realistic such numbers are, but given that at least ten hours of video are uploaded to YouTube every minute, it is reasonable to assume that the additional burden would be substantial.[45]

The implications of deploying negative measures, however, go far beyond the financial. As mentioned above, all types of filtering require blacklists of banned websites and keywords. These blacklists, however, can be ‘reverse engineered’, meaning that – however much a government tries to keep them secret – it will be near impossible to prevent them from ending up in the public domain.[46]

The consequences would be twofold. First, attention would be drawn to websites and content that have been judged to be undesirable. No filtering system is perfect, and there can be little doubt that, in the wake of its introduction, various methods for circumvention would circulate on blogs and in web forums. Against this background, the blacklists would come to serve as virtual guides to all the material ‘the government doesn’t want you to see’. Doubtless, some of the banned websites and their operators would gain kudos from being blacklisted, thereby negating the intention behind the decision to block them.

A second consequence would be for the blacklists to become the subject of public scrutiny and political debate. In the case of the Internet Watch Foundation (IWF) and the issue of child sexual abuse, this is significantly less problematic than with politically motivated extremism (see Box 4). Paedophiles do not have public support – they cannot count on sections of the population to be ambiguous, and no one feels ‘victimised’ as a result of their websites being banned. The issue of extremism, by contrast, is political, and the use of blacklists to prevent the public from viewing such materials is certain to generate widespread political controversy as well as numerous legal challenges.

Presently, this would be true in particular for Muslim communities. Muslims in the United Kingdom are overwhelmingly opposed to violence, yet there is a widespread perception that counterterrorism policy has unfairly targeted their communities. If the government’s blacklists were to contain mostly Islamist websites, this might serve to feed a sense of exclusion and create the impression that the government is restricting Muslims’ freedom of expression.[47] Even if such measures were considered useful, consistency of application would be essential, and policies applicable to Islamist extremism would have to be extended to the far right and other kinds of violent extremism more generally.

Given the political controversies that would result from the introduction of any type of filtering at the national level, it should come as no surprise that the British government has so far been reluctant to make such systems compulsory. Instead, it seems to have opted for a voluntary approach whereby it collaborates with companies that provide filtering and/or parental control software, helping them to fine-tune their products to include materials that are judged to be unlawful under current anti-terrorism legislation. The main targets of the scheme appear to be parents and schools as well as businesses wishing to restrict employees’ access to certain types of material.[48]

Whatever the merits of this new initiative, the British government’s waning enthusiasm for mandatory web filtering at the national network level indicates that the myriad problems that would result from such a course of action have come to be understood.[49] As will be shown in the following chapters, there are other, potentially more productive ways in which online radicalisation can be countered.

[44] Interviews, July-October 2008.

[45] YouTube Fact Sheet (http://uk.youtube.com/t/fact_sheet). See also Jeffrey Rosen, ‘Google’s Gatekeepers’, *The New York Times Magazine*, 28 November 2008.

[46] This ability to circumvent control mechanisms is part of a broader argument that many of these negative measures are relatively easy to bypass, given a modicum of technical ability, and are therefore no barrier to determined users. See Richard Clayton, ‘Memorandum’, submitted as written evidence to the UK Parliament Select Committee on Culture, Media and Sport, January 2008; available at http://www.parliament.the-stationery-office.co.uk/pa/cm200708/cmselect/cmcumeds/353/353we05.htm. Some organisations even provide free advice on how to do so. See, for example, Civisec, *Everyone’s Guide to By-Passing Internet Censorship: For Citizens Worldwide*, September 2007; available at http://www.civisec.org/sites/all/themes/civisec/guides/everyone’s-guide-english.pdf.

[47] A recent survey found that a majority of young British Muslims felt unable to discuss extremism and terrorism freely in the presence of authority figures, even in universities. See UK Youth Parliament, ‘9 out of 10 young people say they need to discuss terrorism and preventing violent extremism, according to new survey’, UKYP press release, 8 August 2008; available at http://www.ukyouthparliament.org.uk/newsroom_site/pages/news/2008/08_08_08_terrorismsurvey.html.

[48] Home Office, ‘Industry and government work together to tackle internet terror’, press release, 18 November 2008; available at http://press.homeoffice.gov.uk/press-releases/industry-and-government. Home Office officials subsequently clarified to us that they are “providing details of material judged to be unlawful under Section 3 of the Terrorism Act 2006 to companies that provide filtering and/or parental control software. The companies are under no obligation to include the material in their products but can use the material to enhance the protection their products often already offer against terrorist material.”

[49] Australian government plans to implement network level filtering have been the subject of much criticism and are unlikely now to proceed as planned. See, for example, Asher Moses, ‘Labor plan to censor internet in shreds’, *The Sydney Morning Herald*, 9 December 2008; available at http://www.smh.com.au/news/home/technology/labor-plan-to-censor-internet-in-shreds/2008/12/09/1228584820006.html.

TABLE 1 Negative measures: Overview

MEASURE	METHOD	ASSESSMENT
	Removing	
Takedowns	Government tells hosting company to 'take down' content of website.	Hosting company needs to be located in same jurisdiction.
Domain name deregistration	Government tells domain name provider to deregister domain name.	Top-level domain (e.g. '.uk') needs to be operated by national registry.
Denial of service attack	Overloading servers or networks with communication requests.	Illegal and, at best, a temporary means of disruption.
	Filtering	
Internet protocol (IP) filtering	Requests for blacklisted IP addresses are intentionally dropped.	Cheap, but blocks all services hosted by a web host ('overblocking').
Content filtering (dynamic filtering)	Filtering software 'sniffs' all information packets for blacklisted keywords.	Expensive. Also requires 'white listing' of permitted websites.
Domain name tampering	During IP 'look-up', requests for banned domain names are dropped.	Cheap, but problems with overblocking. Also, easy to circumvent.
Proxy filtering	Proxy filters decide whether to allow requests for individual webpages.	Expensive. May slow down traffic unless substantial investments are made.
Hybrid IP and proxy filtering	Combines IP and proxy filtering: proxy filtering only for blacklisted IP addresses.	Technically effective. But, like other methods, relies on blacklisting and fails to capture dynamic content.
	Hiding	
Search engine filtering	Search engines drop requests for certain webpages and keywords.	Requires active collaboration of search engine provider.
'Black hat' search engine optimisation (SEO)	Manipulating search engines to boost or reduce websites' page rank.	Widely frowned upon. Utility may be limited.

BOX 3 British Telecom and Cleanfeed

In June 2004, one of Britain's largest internet service providers, British Telecom (BT), deployed their Cleanfeed blocking system at network level. The aim of the technology was to prevent access – either deliberately or accidentally – to child sexual abuse images listed by the Internet Watch Foundation (IWF) as illegal (see Box 4).

Cleanfeed is a hybrid IP and proxy filtering system, which means that internet traffic is first examined to see if it is attempting to access an IP address in the IWF's database. If traffic falls foul of this blacklist, it will then be redirected to a proxy server inspecting the data packets to see if specific URLs on this blacklist are being requested. Banned items are returned with a 404 *(page not found)* response, while the rest of the traffic continues unhindered to its destination. This two-tier system both keeps costs down and reduces the potential 'overblocking' of legitimate web content.

Although the scheme continues to be criticised as 'censorship',[50] access to the material with which it currently deals – child sexual abuse images – is not considered a right and is almost universally illegal. What is of more concern is that the technology can be circumvented and reverse-engineered to reveal the identities of sites on the blacklists,[51] therefore negating much of the purpose of the system. Its inventor, Mike Galvin, admits that the system 'won't stop the hardened paedophile'.[52]

Even so, according to the Home Office, the partnership of the IWF and BT's Cleanfeed has reduced the proportion of all child sexual abuse websites that are hosted in the United Kingdom from 17 per cent in 1997 to 0.4 per cent in 2008.[53]

[50] This criticism has resurfaced recently during the furore over the accidental blocking of access to Wikipedia as a result of IWF actions. See, for example, Open Rights Group, 'IWF censors Wikipedia, chaos ensues', 8 December 2008; available at http://www.openrights-group.org/2008/12/08/iwf-censors-wikipedia-chaos-ensues/.

[51] Richard Clayton, 'Failures in a Hybrid Content Blocking System', unpublished paper, 2005; available at http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf.

[52] S.A. Mathieson, 'Back door to the black list', *The Guardian*, 26 May 2005; available at http://www.guardian.co.uk/technology/2005/may/26/onlinesupplement.

[53] Vernon Coaker, written answer on pornography and the internet, *Commons Hansard Parliamentary Debates*, 16 June 2008; available at http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm080616/text/80616w0011.htm#08061620000414.

BOX 4 The Internet Watch Foundation

Founded in 1996, the Internet Watch Foundation (IWF)[54] has been instrumental and successful in reducing access to child sexual abuse images online in the UK. Funded collaboratively by the internet industry, the European Union, and private contributions, the agency is independent of local and/or national government. Its budget totalled just over £1m in 2006-2007.[55]

continued overleaf

[54] IWF website (http://www.iwf.org.uk/).

[55] All data from the IWF, *2007 Annual and Charity Report*; available at http://www.internetwatch.org.uk/documents/20080417_iwf_annual_report_2007_(web).pdf.

continued

The IWF's remit is to minimise the availability of potentially illegal internet content related to (1) images of child abuse hosted anywhere; (2) criminally obscene activities hosted in Britain; and (3) incitement to racial hatred hosted in Britain.

The public face of the IWF is a 'hotline', which enables the public to report content that falls into these categories when found on websites, newsgroups, mobile services and other online environments. In 2007, the IWF processed 34,871 such reports. The IWF employs a grading system which determines whether material triggers 'notice and takedown' advisory alerts to web hosts and ISPs. In Britain, most of these companies – as members of the IWF – comply within a matter of hours.[56] The offending web addresses are also added to blacklists that inform web filtering technology, including British Telecom's Cleanfeed system (see Box 3).

In addition, the IWF reports foreign-hosted material to relevant national hotlines and law enforcement agencies. Success relies on the willingness or ability of foreign agencies to record, process, trace and act upon internet intelligence, which varies greatly. The IWF works with 30 other hotlines across the world, principally in Europe, North America and Australasia, but there are as yet no unified or truly co-operative transnational mechanisms to help combat what is a global problem.

Of publicly submitted reports in 2007, a mere 2.4 per cent of the total was content related to incitement to racial hatred. The reasons for the low rate of public reports are unclear, although lack of knowledge about the reporting mechanism, lack of concern, and low frequencies of offensive materials may all have played some part.

According to the IWF, of this content, 'little if any' was 'confirmed as potentially illegal by our analysts, and even less of it is hosted in the UK'.[57] The IWF states that suspected *terrorist* activity or material should be reported to the police's Anti-Terrorist Hotline and gives that phone number accordingly.

For the purpose of grading child sexual abuse images, the IWF uses a five-point scale established by the UK Sentencing Guidelines Council.[58] No such scale exists for grading incitement to racial hatred material, and adjudication on such issues would rely on context and be infinitely more complex than with images of child sexual abuse. Nevertheless, based on past prosecutions, the Home Office advisory does provide some guidance on what kind of internet material is 'potentially illegal under the incitement provisions'.[59]

[56] Unfortunately, this is not always the case, and a recent study suggests that takedown times for such material can actually be less than for material of financial, rather than moral, significance. See Tyler Moore and Richard Clayton, 'The Impact of Incentives on Notice and Take-down', *Seventh Workshop on the Economics of Information Security* (WEIS 2008), Dartmouth College, Hanover, New Hampshire, June 25–28 2008; available at http://www.cl.cam.ac.uk/~rnc1/takedown.pdf.
[57] IWF 2007 *Annual and Charity Report*, 'Trends'.
[58] Sentencing Guidelines Council, *Sexual Offences Act 2003: Definitive Guidelines*, April 2007, p.109; available at http://www.sentencing-guidelines.gov.uk/docs/82083-COI-SCG_final.pdf.
[59] Home Office, *Racially Inflammatory Material on the Internet*, February 2002; available at http://www.iwf.org.uk/documents/20041020_racially_inflammatory_material_on_the_internet.pdf.

4 Deterring Producers Strategic Prosecutions

As shown in the previous chapter, it is not realistic to expect all potentially radicalising content to be removed from the internet. Any attempt to do so would generate social and political costs that would far outweigh the benefits that might be gained from having certain materials removed, especially in the context of a liberal democracy.

For policymakers, the obvious question is: what can be done? This and the following three chapters will outline a set of concrete ideas which may help to counter online radicalisation. In conceiving these ideas, the aim was to move beyond a purely 'negative' approach and examine what options are available to create an environment in which the production and consumption of such materials become not just more difficult in a technical sense but unacceptable as well as less desirable. Not all the ideas presented are 'soft' and/or 'positive'. As this chapter will demonstrate, negative measures can play a constructive role, but it is essential that they be used in the context of a broader strategy.

This chapter proposes the selective use of takedowns in conjunction with other legal tools. Under this proposal, particularly offensive websites would be singled out, their websites taken down, and prosecutions brought against the individuals responsible. Doing so would convey the message that cyberspace is not beyond the law, that publishing certain materials is unacceptable in Britain, and that individuals engaged in producing and disseminating these materials might face prosecution. The aim is to end the current climate of impunity and deter British-based extremists from publishing clearly illegal and/or particularly hateful content.

Targeting individuals

Sections 3 and 4 of the Terrorism Act (2006) provide for the issuance of internet 'Notice and Takedown' procedures, which enable the government to instruct hosting companies or internet service providers to remove offending websites.

By itself, this instrument is clearly insufficient as a way of dealing with the problem of online radicalisation. Takedowns are a reactive measure, which means that by the time the takedown procedure is initiated, the material may have been viewed by large numbers of people. Furthermore, as shown in the previous chapter, the removal of a particular website does not guarantee that it will not appear elsewhere on the web, hosted by another company in a different jurisdiction. In the absence of regional or international law covering the material in question, this will nullify the government's efforts to make the website unavailable.

In addition to rarely achieving their desired technical outcome, takedowns suffer from another, even more obvious, flaw: they target content rather than the individuals responsible for producing and disseminating it. Even if a takedown is successful in removing a website or disrupting its operation, its creators and contributors are free to establish other websites from which the same material is available.

Takedowns, in other words, deal with the symptom, not its cause: they convey the message that publishers of illegal and/or unacceptable materials enjoy impunity as long as they ensure that their websites are hosted outside a government's jurisdiction. This, in fact, is what British neo-Nazis tended to assume until the recent conviction of Simon Sheppard and Steven Whittle (see Box 5).

Takedowns, therefore, should not be deployed on their own, nor should the government be under any illusion about their utility in removing material from the internet. Instead, they should be accompanied wherever possible by prosecution of the individuals responsible for producing, publishing and/or disseminating content that can be established as illegal in a court of law.

The advantage of focusing on individuals is that, by all accounts, the number of people involved in running extremist websites and forums is small when compared to the numbers they attract. Also, such individuals are often based in the same jurisdiction as their audience, and it will undoubtedly be more difficult for them to move to a different country than it is for their websites to be hosted in a different jurisdiction.[60]

Legal options

There is no lack of legal options that would allow successful prosecutions to be brought. Indeed, neither terrorism- nor internet-specific legislation may be necessary in order to charge and convict individuals who have been involved in the production and dissemination of radicalising materials. The Terrorism Act (2000) and Section 3 of the Terrorism Act (2006) make it clear that materials available on the internet should be considered as 'publications', and that – being 'published' – such content can in many cases be treated like print and broadcast media.

Among the established and tested legislation that can be used to bring prosecutions are provisions against 'soliciting murder', which is illegal under Section 4 of the Offences Against the Person Act (1861) and was part of the case against the radical preacher Abu Hamza, whose sermons were distributed on the internet.[61] It was also used against the former spokesman of the extremist group Al Muhajiroun, Umran Javed, who was prosecuted for his part in demonstrations during the Danish cartoons controversy.[62]

Although the legal offence of 'incitement to murder' was removed from the statute books in October 2008, the coming into force of the Serious Crime Act (2007) makes it illegal to encourage or assist crime, with incitement to murder now falling within the remit of this legislation. In addition, British murder laws are currently being reviewed, and it may well be that solicitation and incitement will be further defined as a result of the Law Commission's recommendations.[63]

Much of the material that is involved in online radicalisation can also be dealt with through laws proscribing racially or religiously motivated criminality. Incitement to racial hatred was first established as a criminal offence under the Race Relations Act (1976) and was bolstered under Sections 17-29 of the Public Order Act (1986). The latter applies only to racial groups 'in Great Britain', but the Anti-Terrorism, Crime and Security Act (2001) has extended this definition to groups abroad. Furthermore, the Criminal Justice and Public Order Act (1994) targets the publication of material that incites racial hatred; the Crime and Disorder Act (1998) prohibits racially aggravated harassment; and the Racial and Religious Act (2006) makes it illegal to threaten on the basis of religion.

Less is more

Whatever their legal basis, the use of strategic prosecutions in combating online extremism should be guided by the principle that 'less is more'. The purpose of this measure is not for all undesirable content to be removed from the web, which – as has been shown – is not possible. Rather, the objective is to signal to the public that publishing inciting and hateful materials on the internet is unacceptable in Britain and that – where such content is illegal – individuals might be prosecuted in a court of law. To achieve this goal, it may not be advisable to bring large numbers of prosecutions, but select a few, well-supported cases which help to communicate the government's intent and define the boundaries of what is acceptable.

One of the risks of bringing large numbers of prosecutions is that badly prepared (and ultimately unsuccessful) cases might be counterproductive in creating a body of case law that makes future prosecutions more difficult and allowing online extremists to claim that they are the innocent victims of government persecution.

Take, for example, the case of Samina Malik, whose conviction for 'possessing records likely to be used for terrorism' was recently overturned.[64] Malik, a twenty-three-year-old shop assistant from West London who called herself the 'Lyrical Terrorist', posted a number of poems on extremist websites in which she expressed a desire to

[60] In targeting individuals, a positive working relationship between law enforcement and the industry is essential because internet service providers are often the only party who can establish real-world identities of internet users. Unless they seek to obstruct reasonable requests or fail to provide information relevant to criminal investigations, government should therefore make it clear that it will not attempt to make internet companies liable for 'dissemination'.This helps to preserve the European legal status of ISPs as "mere conduits" for the exchange of information. See *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')*; available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML. This principle was adopted by the UK government in *The Electronic Commerce (EC Directive) Regulations 2002*; available at http://www.opsi.gov.uk/si/si2002/20022013.htm. Readers are also referred to *Godfrey v. Demon Internet Limited [1999] 4 All ER 342, [2001] QB 201 (QBD)*. See Yaman Akdeniz, 'Case analysis: Laurence Godfrey v. Demon Internet Limited', *Journal of Civil Liberties*, Vol. 4 No.2 (1999), pp.260-7.

[61] Crown Prosecution Service, 'Abu Hamza convicted of eleven charges', CPS press release, 7 February 2006; available at http://www.cps.gov.uk/news/pressreleases/archive/2006/105_06.html.

[62] Crown Prosecution Service, 'Cartoons protestors sentenced for soliciting murder', CPS press release, 18 July 2007; available at http://www.cps.gov.uk/news/pressreleases/archive/2007/145_07.html.

[63] Law Commission, 'Murder', updated 13 March 2008; available at http://www.lawcom.gov.uk/murder.htm.

[64] Crown Prosecution Service, 'CPS response to Samina Malik appeal', CPS press release, 17 June 2008; available at http://www.cps.gov.uk/news/pressreleases/143_08.html.

become a ‘martyr’ and voiced her support for beheadings. Although she was in contact with prominent figures in the British jihadist scene, Malik herself was a minor player and her writings had little impact on the wider extremist community. Her trial and acquittal, however, turned her into a ‘celebrity’ and resulted in the reprinting of her poems all over the internet. Most worrying, it communicated the message that expressing support for terrorism is acceptable after all.

Another reason for using the instrument of strategic prosecutions selectively is that doing so will make it easier to ensure consistency of application. As explained in the previous chapter, the principal problem with using negative measures lies not in their technical efficiency (or lack thereof), but in the potentially negative community impact. In the current climate, if the instrument of strategic prosecutions was to be used against just one section of the extremist spectrum at the expense of others, this might strengthen the perception – however unjustified – that ‘double standards’ are being applied. Accepting the principle that ‘less is more’ would enable governments to fine-tune their approach by balancing prosecutions against Islamist extremists with cases against white supremacists and other kinds of extremists. The government’s aim should be to communicate that not just one but *all* forms of incitement and online extremism are unacceptable in Britain.

Of course, strategic prosecutions alone will not solve the problem of online radicalisation. In fact, rather than focusing on governmental and/or administrative responses alone, it is vital to look at ways in which internet users can be empowered to confront online extremism, as discussed in the following chapter.

BOX 5 CASE STUDY
Simon Sheppard and Steven Whittle

Simon Sheppard and Steven Whittle are two well-known British neo-Nazis, who are currently seeking asylum in the United States after being convicted on several counts of publishing and distributing racially inflammatory material on the *Heretical Press* website run by Simon Sheppard.

Most of the charges that were brought against the two individuals related to offences defined in the Public Order Act (1986), which – evidently – could be used for materials published on the internet. According to lawyer Mari Reid of the Crown Prosecution Service, ‘People are entitled to hold racist or extreme opinions… What they are not entitled to do is to publish and distribute these opinions to the public in a threatening, abusive or insulting manner either intending to stir up racial hatred or in circumstances where it is likely racial hatred will be stirred up’.[65]

Sheppard and Whittle were likely to be given custodial sentences, and decided to skip bail in order to claim political asylum in the United States, where the Heretical Press website is hosted and continues to operate. At this point, it is unclear if and when they will return to the United Kingdom.

Despite the two men’s escape and the website’s continued operation, the trial and conviction of Sheppard and Whittle should be considered a success. It sent a strong signal to extremist groups that hosting websites outside the United Kingdom will not stop the authorities from taking legal action against their owners and contributors. According to the anti-fascist magazine *Searchlight:* ‘British Nazis had believed that if they hosted their racist ravings on US web servers they would be immune from prosecution. Sheppard’s conviction has undermined that confidence, sending shockwaves through British fascism’.[66]

[65] Quoted in Crown Prosecution Service, ‘Two guilty of inciting racial hatred against Jews’, CPS press release, 8 January 2009; available at http://www.cps.gov.uk/news/pressreleases/101_09.html.

[66] David Williams, ‘Holocaust deniers skip bail to claim asylum’, *Searchlight*, August 2008.

5 Empowering online communities
The internet users panel

Upon realising the limited ability of governments to police the internet, commentators often turn to industry, arguing that it is the internet service providers and big websites who need to 'keep their houses in order' and ensure that no unacceptable content is disseminated through their platforms. In shifting the responsibility from government to a small number of commercial companies, this line of reasoning fails to acknowledge the most natural and, in many ways, most promising resource for regulating content on the internet, namely internet users themselves. The proposal in this chapter is aimed at improving the mechanisms through which they can make their voices heard.

This chapter proposes the creation of an independent Internet Users Panel whose main objective is to strengthen the processes through which internet users can hold internet companies accountable for the content that is published on their platforms. The panel would be funded by the industry and could be charged with: raising awareness of reporting mechanisms for unacceptable content; monitoring companies' complaints procedures; highlighting best and worst practices; facilitating partnerships between internet companies and non-governmental organisations; and serving as an ombudsman of last resort. The underlying goal is to encourage and empower internet users to self-regulate the online communities of which they are part.

Regulating cyberspace?

Most file-sharing and social networking sites have internal reporting mechanisms which allow community members to flag offensive or potentially illegal content as well as material which contravenes the sites' own community guidelines.[67] When users report content, the sites adjudicate each case and remove the content if it breaches their internal policies, license agreements, or national or international law. These procedures operate on the principle that users police and shape their own online environments in conjunction with the platform providers. Although the vast majority of complaints are dealt with swiftly and positively these systems are imperfect in that – ultimately – users rely on internet companies' goodwill and have no recourse to an external body should companies fail to deal with complaints adequately, or do not respond at all.

Although the Code of Practice adopted by the Internet Services Providers Association (ISPA) addresses issues such as legality and decency – including the hosting of 'material inciting violence, cruelty or racial hatred'[68] – there clearly exists a gap in the regulatory mechanisms of the industry. Otelo, the telecommunications ombudsman, explicitly states that it will not deal with complaints

[67] See for example, YouTube's *Community Guidelines*; available at http://uk.youtube.com/t/community_guidelines.
[68] ISPA, 'ISPA Code of Practice', amended 3 July 2007; available at http://www.ispa.org.uk/about_us/page_16.html.

about ‘the content of Internet sites, calls, emails, or SMS (texts)’.[69] As a result, the only option available to users is to contact the police if they believe that such communications constitute harassment, fraud, slander, or any other criminal offence. Reporting an offensive or otherwise unacceptable website to the police, however, is something which most users will be reluctant to do. In fact, it is unlikely that the police would want to be involved in investigating offensive websites and settling disputes between users and internet companies.

In the absence of effective, user-driven mechanisms to regulate internet content, policymakers have become increasingly vocal in their demands for government regulation. For example, the House of Commons’ Culture, Media and Sport Select Committee recently recommended that the ‘proactive review of content should be standard practice for sites hosting user-generated content’. The committee also proposed

> *a tighter form of self-regulation under which the industry would speedily establish a self-regulatory body to draw up agreed minimum standards… monitor their effectiveness, publish performance statistics, and adjudicate on complaints.*[70]

Although government representatives have signalled that regulation of the internet is not a current priority, the calls for industry self-regulation by influential bodies such as the Select Committee on Culture, Media and Sport should be understood as a warning. It reminds the industry that government will step in unless more effective and transparent mechanisms for dealing with unacceptable and/or potentially illegal content are implemented.

Indeed, many observers believe that some degree of regulation for cyberspace is inevitable.[71] Shortly before leaving office in 2007, Prime Minister Tony Blair commented that ‘change [is] on its way. The regulatory framework at some point will need revision’.[72] The precise form of regulation, of course, has yet to be determined, but it would seem sensible for the industry to take the initiative in creating better mechanisms of self-regulation before government action is imposed upon them.

Empowering users

From the industry’s perspective, the prospect of regulation represents an opportunity as much as it constitutes a threat. Properly conceived, it may offer the chance to bring into existence new models of user-driven self-regulation, which could make expensive, heavy-handed attempts at regulating cyberspace unnecessary.

All successful instances of user-driven internet strategies have aimed to activate the collective wisdom and power of online communities. What they share is the idea of online communities as vast, living organisms, which – though consisting of innumerable cells – can be made to pull in the same direction. Nowhere is this more obvious than in the case of Wikipedia, the online encyclopaedia, whose 12 million entries have all been written by volunteers from across the world and can be edited by any registered user. Wikipedia has been criticised for inconsistencies and for being susceptible to acts of online vandalism, though academic studies have shown that such aberrations are usually corrected within minutes.[73] Indeed, the power of the user-driven model lies precisely in its ability to detect anomalies, self-correct and, over time, build collective institutional memory.

Though undoubtedly different in terms of aims and context, the idea of capitalising upon the collective power of internet users can also be applied to the challenge of dealing with undesirable content. The Internet Watch Foundation (see Chapter 4) draws on a similar model in that – instead of depending on large numbers of staff to ‘proactively’ screen the internet for images of child sexual abuse – it relies on internet users to report suspected incidents, which are investigated and judged by a small number of professionally trained researchers. Naturally, for this model to work, reporting mechanisms need to be well known among the online communities to which they are most relevant; mediation procedures need to be transparent; and responses have to be swift.

The IWF model may be difficult to transfer to online extremism, not least because the material is of a fundamentally different nature and the boundaries between what is illegal and what is merely offensive are consequently more difficult to define. Rather than suggesting the creation of a central authority akin to the IWF, the proposal is for individual online communities to form networks of self-regulation which – principally through active participation in reporting mechanisms and similar procedures – determine which content ought to be tolerated and what kinds of materials should be removed. While reporting mechanisms and complaints procedures are not generally considered the most exciting parts of the online experience, if fully embraced they are the most effective as well as most democratic way of countering online radicalisation.

Targeting process

The purpose of the proposed Internet Users Panel would be to promote and strengthen user-driven self-regulation. Instead of grading content like the IWF, the Panel’s primary objective would be to facilitate the process whereby users and internet companies *themselves* are defining what is acceptable to their respective communities.

In practical terms, much of the Panel’s work would be dedicated to encouraging the use of reporting mechanisms and complaints procedures, making sure that such instruments are available and easily accessible, and that the rules according to which

[69] Otelo, ‘Is there anything we cannot deal with?’; available at http://www.otelo.org.uk/pages/33whatwecan’thandle.php.

[70] House of Commons Culture, Media and Sport Committee, *Harmful content on the Internet and in video games*, Tenth Report of Session 2007-08, 22 July 2008; available at http://www.parliament.the-stationery-office.com/pa/cm200708/cmselect/cmcumeds/353/353.pdf.

[71] The best single volume on this subject is Andrew D. Murray, *The Regulation of Cyberspace: Control in the Online Environment* (Abingdon & New York: Routledge-Cavendish, 2007).

[72] Tony Blair, Speech to the Reuters news agency, 12 June 2007; available at http://www.telegraph.co.uk/news/uknews/1554286/Full-text-of-Blair’s-speech-on-politics-and-media.html.

[73] Fernanda B. Viégas, Martin Wattenberg, and Kushal Dave, ‘Studying Cooperation and Conflict between Authors with History Flow Visualizations’, *Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI), Vienna, Austria, April 24-29, 2004, pp.575–582; available at http://alumni.media.mit.edu/~fviegas/papers/history_flow.pdf.

they are administered are transparent and comprehensible. The Panel would also devote considerable attention to monitoring companies' performance, that is, whether they are taking complaints seriously, dedicating sufficient staff to deal with them, and adapting policies in response to users' concerns. The Panel could also highlight best and worst practices in the area – not shying away from 'naming and shaming' internet companies which have consistently failed to live up to good practice – and be involved in promoting positive partnerships, such as the recent collaboration between YouTube and the Anti-Defamation League (ADL) in the United States (see Box 6).

One of the Panel's functions would be to serve as ombudsman of last resort. Where a conflict between a user and an internet company cannot be resolved, the Panel would investigate. The Panel's adjudication would be based not on the content of the website or communication which gave rise to the complaint but whether the complaint was dealt with appropriately. The threshold for applying this mechanism would have to be fairly high in order to avoid overloading the Panel with individual complaints. Users would have to demonstrate that they have exhausted all other means of seeking redress. In turn, internet companies would agree to abide by the Panel's ruling.

The Panel would be funded by ISPA, whose members – comprising 95 per cent of the British internet market by volume – would sign up as 'affiliates', agreeing to consider the Panel's recommendations and guidelines as well as abiding by its rulings in individual cases. Though funded by the industry, the Panel would nevertheless be independent and draw its membership from a variety of stakeholder groups, including experts, internet users, and industry professionals. The government would have no direct role within the body, though it is hoped that a useful working relationship between the two parties could be developed. If successful, the aspiration would be for other countries to adopt the same model, so that – over time – international standards and best practices can emerge.

However effective this Panel and the mechanisms for user-driven self-regulation it hopes to promote, the battle against online radicalisation is not just about reducing the availability of extremist materials but also, and more important, about lessening their appeal. As part of this effort, the proposal in the following chapter aims to strengthen people's ability to judge the context and validity of online information.

BOX 6 YouTube and the Anti-Defamation League

In 2008, the world's largest video-sharing site, YouTube, came under repeated criticism for its hosting of a variety of content considered inappropriate or offensive, including materials that were considered extremist.[74] Although the site and its owner, Google, have operated a range of community procedures and complaints mechanisms for years, it was apparent that YouTube would need to re-examine these in order to deflect criticism and improve its user experience.

YouTube decided to reconfigure its internal reporting process and, in December 2008, launched its Abuse and Safety Center.[75] This new mechanism provides information on a variety of issues – for example, breaches of community guidelines, cyber-bullying, privacy, child sexual abuse, and hateful content – and makes it possible for users to report issues of concern to YouTube. In addition, every YouTube page has a link to the Center embedded within a menu at the bottom of the page.

Of particular relevance to the debate on radicalisation has been YouTube's partnership with the Anti-Defamation League (ADL).[76] The ADL was founded in the United States in 1913 in order 'to stop the defamation of the Jewish people and to secure justice and fair treatment to all'.[77] Throughout its history, the ADL has tackled all forms of bigotry and hatred, often bringing it into confrontation with, among others, the Ku Klux Klan, neo-Nazis, skinhead movements, the Christian Identity movement, and Holocaust deniers. Their more recent experience in tackling internet hate speech, especially as a member of the International Network Against Cyberhate (INACH),[78] has been directly drawn upon by YouTube in an attempt to improve its own efforts in this field.

[74] See, for example, US Senator Joe Lieberman's letter to YouTube. 'Lieberman Calls on Google to Take Down Terrorist Content', 19 May 2008; available at http://lieberman.senate.gov/newsroom/release.cfm?id=298006. Lieberman's actions resulted in YouTube voluntarily removing a number of Islamist videos, and a revision of its community guidelines. The British government expressed concerns over the glorification of knife crime, amongst other issues, which led to YouTube banning such videos in the UK. See BBC, 'YouTube bans some weapons footage', 17 September 2008; available at http://news.bbc.co.uk/1/hi/technology/7621013.stm.

[75] YouTube Abuse and Safety Center (http://help.youtube.com/support/youtube/bin/request.py?contact_type=abuse). Also 'Safety, education, and empowerment on YouTube', *Google Public Policy Blog*, 11 December 2008; available at http://googlepublicpolicy.blogspot.com/2008/12/safety-education-and-empowerment-on.html.

[76] Anti-Defamation League, 'YouTube Taps ADL As Partner In Fight Against Hate', 11 December 2008; available at http://www.adl.org/PresRele/Internet_75/5416_75.htm.

[77] ADL, 'About ADL'; available at http://www.adl.org/main_about_adl.asp.

[78] INACH website (http://www.inach.net/).

6 Reducing the Appeal
Strengthening Media Literacy

As demonstrated in previous chapters, the internet has democratised access to communication, blurred the distinction between producers and consumers, and – as a result – challenged the dominance of traditional producers, such as newspapers, radio and television. Some of these developments are unquestionably positive, but they have also raised important questions about how information ought to be processed and evaluated. In particular, the internet makes it far more difficult to assess the context, origins and credibility of information. In order to reduce the appeal of extremist messages, it is vital, therefore, to strengthen users' ability to evaluate online content critically, especially when they are children or young people. The aim, in other words, must be to improve 'media literacy', which Ofcom defines as 'the ability to access, understand and create communications in a variety of contexts'.[79]

This chapter argues that a comprehensive strategy is needed to improve young people's capacity to deal with extremist internet content critically. Most efforts at promoting media literacy have narrowly focused on issues related to child safety and sexual abuse. While important and useful, these initiatives can be applied to the problem of online radicalisation only in part. A systematic review should be conducted to determine what relevant stakeholders (in particular parents, teachers and internet companies) and institutions (especially schools) can contribute to strengthening media literacy as a means of countering online radicalisation.

Broadening the Scope

In Britain, most efforts to promote online media literacy have traditionally focused on protecting children from sexual abuse and pornography. Past and current efforts in this area have primarily been aimed at restricting access to inappropriate environments and shaping children's ability to cope with these experiences. Indeed, there is a plethora of state, commercial and civil society organisations and initiatives working to reduce the risks that are regarded as inherent in child online behaviour.[80]

Until recently, the same was not true of children's exposure to extremist content. In a speech on media literacy in 2004, then Culture Secretary Tessa Jowell made no mention of terrorism or extremism in the context of media literacy.[81] When Ofcom published a literature review on media literacy among children and young people in 2005,

[79] Ofcom, *Ofcom's Strategy and Priorities for the Promotion of Media Literacy: A Statement*, 2 November 2004; available at http://www.ofcom.org.uk/consult/condocs/strategymedialit/ml_statement/strat_prior_statement.pdf.

[80] Examples include the Child Exploitation and Online Protection Centre (CEOP); UK Council for Child Internet Safety (UKCCIS); the National Society for the Prevention of Cruelty to Children (NSPCC)'s *Inform* resource; and Crisp Thinking.

[81] Tessa Jowell, Speech to British Film Institute, UK Film Council, BBC & Channel Four Media Literacy Seminar, 27 January 2004; available at http://www.culture.gov.uk/reference_library/minister_speeches/2098.aspx.

neither terrorism nor extremism were mentioned as a risk.[82] (A single reference to 'hate speech' suggested that French children were more concerned by this than pornography, but went on to argue that they considered themselves more capable of dealing constructively with this material if they spent more time online rather than less.) In subsequent years – especially following the terrorist attacks in London in July 2005 – the issue of online extremism and how young people ought to deal with it has come to the fore, eclipsing all but paedophilia at the top of the child online protection agenda. In fact, as recently as January 2009, the Director General of the Security Service (MI5) told reporters that terrorists' use of the internet as an instrument for grooming vulnerable children was one of his organisation's main concerns.[83]

Nevertheless, most activities in the fields of media literacy and 'child online safety' generally continue to be seen through the prism of child sexual abuse – despite the clear differences between the two problems. Whereas prevention of child sexual abuse is mostly about protecting children from 'predators' in chat rooms and web forums, improving media literacy vis-à-vis online extremism must tackle a wider set of issues. In addition to teaching children to be careful about whom they meet in chat rooms, it has to equip them with the critical skills to question and compare sources of information; engage in independent online research; and evaluate text, audio and visual information which – though not always illegal – may nevertheless be inciting and hateful.

For media literacy to be effective in strengthening young people's defences against online radicalisation, it needs to be treated as a concern in its own right. Given the scope of the challenge, a comprehensive strategy is necessary in order to determine what institutions and actors can make a useful contribution and how these can be coordinated.

The Role of Schools

Although media literacy is not wholly a formal educational issue, it falls to schools to help children understand a wide range of interpretative issues. At Key Stages 1 and 2 (5-11 years), the emphasis in Information Communications Technology (ICT) teaching is on functional literacy, that is, 'finding things out' from a variety of digital sources.[84] Even at an early stage – through the cross-curricular use of ICT – children are encouraged to recover data from 'a variety of sources, selecting and synthesising the information… and developing an ability to question its accuracy, bias and plausibility'.[85] The emphasis on critical literacy increases in Key Stage 2 (7-11 years) where children are required to 'distinguish between fact and opinion [and] consider an argument critically'.[86] In the revised National Curriculum 2007, both English and ICT contain compulsory elements of critical literacy. In fact, whole sections of the English curriculum are devoted to 'Reading for Meaning' and 'Critical Understanding' in Key Stages 3 (11-14 years) and 4 (14-16 years) respectively.[87]

In theory, therefore, key functions of media literacy are being taught at all stages of a child's education. In addition, the Department for Children, Schools and Families recently published a toolkit titled *Learning Together to Be Safe*. It explicitly calls on teachers to raise awareness of online extremism and emphasises the importance of 'developing critical skills and managing harmful media and internet information'.[88]

In practice, however, it is unclear how evenly this advice is applied in British schools. Moreover, there appears to be little emphasis on the user-generated content that has been behind the massive expansion of the internet in recent years and the rise of sites like Facebook, YouTube, Flickr and MySpace. The government agency responsible for promoting the effective use of ICT in teaching, Becta, recently published a report which found that 'there is only limited use of Web 2.0 [that is, websites relying on user-generated content], and only a few embryonic signs of criticality, self-management and meta-cognitive reflection'.[89] Yet it is precisely this type of material that causes the greatest concern in relation to online extremism. Given that two Ofcom reviews have singled out 'the creation of online material' as holding the greatest potential for enhancing learners' understanding of the online environment,[90] a powerful case could be made for giving the teaching (and practice) of such technologies a greater role in the curriculum.

Overall, it seems obvious that a comprehensive review of all the relevant elements of the current curriculum would be helpful in allowing schools to firm up the commitment of energy and resources to equipping children with the appropriate tools to deal critically with the internet generally and extremist materials in particular.

Other stakeholders

If the proposed strategy is to be comprehensive, focusing on schools alone will not be sufficient. The other obvious place in which media literacy needs to be promoted is the family. Parents often – and incorrectly – assume that their children are 'digital natives',[91] and that it makes no sense to get involved in their online activities. Yet, the

[82] David Buckingham with Shaku Banaji, Andrew Burn, Diane Carr, Sue Cranmer and Rebekah Willett, *The Media Literacy of Children and Young People* (London: Ofcom, 2005); available at http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/ml_children.pdf.

[83] Michael Evans, 'MI5's spymaster Jonathan Evans comes out of the shadows', *The Times*, 7 January 2009.

[84] Department for Education & Skills and Qualifications & Curriculum Authority, *Information and Communication Technology (ICT) – Teacher's Guide: A scheme of work for key stages 1 and 2* (London: DfES & QCA, 2003); available at http://www.standards.dfes.gov.uk/schemes3/documents/ICT_Teachers-guideupdate.pdf.

[85] QCA, 'National Curriculum: General Teaching Requirements'; available at http://curriculum.qca.org.uk/key-stages-1-and-2/general-teaching-requirements/index.aspx.

[86] Department for Education & Employment and QCA, *English. The National Curriculum for England: Key stages 1-4* (London: DfEE & QCA, 1999); available at http://curriculum.qca.org.uk/uploads/English 1999 programme of study_tcm8-12054.pdf?return=/key-stages-1-and-2/subjects/english/keystage2/en2-reading/index.aspx.

[87] QCA, *The National Curriculum statutory requirements for key stages 3 and 4 from September 2008* (London: QCA, August 2007); available at https://orderline.qca.org.uk/gempdf/184721553X.pdf.

[88] Department of Children, Schools and Families, *Learning together to be safe: A toolkit to help schools contribute to the prevention of violent extremism*, October 2008; available at http://www.dcsf.gov.uk/publications/violentextremism/downloads/DCSF-Learning Together_bkmk.pdf.

[89] Rose Luckin, Kit Logan, Wilma Clark, Rebecca Graber, Martin Oliver & Adrian Mee, *Learners' use of Web 2.0 technologies in and out of school in Key Stages 3 and 4* (Coventry: Becta, July 2008); available at http://partners.becta.org.uk/upload-dir/downloads/page_documents/research/web2_technologies_ks3_4.pdf.

[90] Ofcom, op. cit., supra n.74. See also Sonia Livingstone, Elizabeth Van Couvering and Nancy Thumim, *Adult Media Literacy: A review of the research literature* (London: Ofcom, 2005); available at http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/aml.pdf.

[91] Marc Prensky, 'Digital Natives, Digital Immigrants', *On the Horizon*, Vol.9, No.5 (2001); available at http://www.marcprensky.com/writing/Prensky - Digital Natives, Digital Immigrants - Part1.pdf.

use of complex tools such as the internet does not necessarily imply fluency or sophistication. The Becta report, for example, noted that many children 'lack technical skills' and warns against overestimating children's familiarity with digital technologies. Therefore, rather than being content with installing filtering software on the home computer and hoping that this will prevent access to harmful content,[92] parents should be encouraged to take an active interest in the technologies that are used by their children and make an effort to learn to use them together.

Needless to say, only teachers should be required to undergo formal 'training' in media literacy, but non-technical advice on child internet safety issues – including online extremism – should be made available to parents via their children's schools. There may also be scope for a public information campaign which could be aimed at children, their parents, or indeed both. Drawing on past campaigns about public health and science issues, the academic Sonia Livingstone has outlined various ideas for such a campaign whose central theme would the education of children and adults to handle complex media environments.[93]

In addition to providing more sophisticated parental controls for their online platforms and devoting sufficient resources to 'moderating' user-generated content, internet companies can play a positive role in publicising online safety and media literacy issues. The European Association of Internet Service Providers, for example, provides a 'Safer Internet' section on their website with lively and illustrated guidance for children and families.[94] In turn, the UK Internet Services Providers Association (ISPA) makes it clear that it sees itself as having a role in 'educating communities'.[95] Such commitments should be drawn upon in maximising the impact of any new efforts and/or public information campaigns.

A promising model for how all these efforts by different stakeholders can be brought together and coordinated is the Canadian Media Awareness Network (see Box 7), which has become a virtual hub for all media literacy efforts – both private and public – in that country.

Of course, none of this is likely to produce immediate results. Yet, in the longer term, few other measures will be more important in undermining the appeal of extremist messages, which is why a comprehensive strategy with coordinated contributions from all stakeholders is so important. However, just as critical as making users 'immune' to extremist messages is the promotion of positive ones. This is what our final proposal aims to encourage.

[92] See Adam Thierer, *Parental Controls and Online Child Protection* (Washington, D.C.: Progress and Freedom Foundation, 2008); available at http://www.pff.org/parentalcontrols/Parental Controls & Online Child Protection [BVERSION 3.1].pdf. According to Ofcom, 90% of UK internet subscriptions come with options, often free, for the provision and installation of parent control software, although only 54% of parents used them. The Byron Review recommended greater visibility and promotion of these tools. See Tanya Byron, *Safer Children in a Digital World: The Report of the Byron Review* (London: Department for Children, Schools and Families, March 2008), pp.94-95; available at http://www.dcsf.gov.uk/byronreview/pdfs/Final Report Bookmarked.pdf.

[93] Sonia Livingstone, Presentation to the Westminster Media Forum on 'Implementing Media Literacy', October 2005; available at http://www.lse.ac.uk/collections/media@lse/pdf/SLstaff_page/Westminster Forum on Implementing Media Literacy Sonia Livingstone's talk.pdf.

[94] EuroISPA, 'Safer Internet' (http://www.euroispa.org/default.aspx?pid=14&sitelang=dutch).

[95] Interview, October 2008.

BOX 7 Media Awareness Network

The Media Awareness Network (MNet)[96] is a not-for-profit organisation established in Canada in 1996, whose aim is to promote media education and media literacy through critical thinking. It is funded by the Canadian government as well as individual and private sector donations.

The organisation grew out of an initiative on media violence but has since broadened its remit and now focuses much of its work on the internet. It addresses a wide range of issues and has launched several initiatives on the issue of online hate.[97]

MNet is engaged in research, but it also provides targeted resources for parents, teachers and young people, including lessons plans for teachers, online tutorials, quizzes and other educational games. It is perhaps the world's largest and most comprehensive resource for information in the area of media literacy.

The organisation has worked with numerous partners, including private sector corporations like Microsoft. This demonstrates how various stakeholders, actors and interests can be brought together without the need for legislation or direct government involvement. Indeed, MNet is perhaps the best example for the kind of comprehensive and coordinated approach that is needed to promote media literacy against online extremism.

[96] Media Awareness Network website (http://www.media-awareness.ca).

[97] MNet, 'Online Hate: An Introduction'; available at http://www.media-awareness.ca/english/issues/online_hate/index.cfm.

7 Promoting Positive Messages The Grassroots Start-Up Fund

One of the strands of the British government's recently published PREVENT strategy aims 'to increase the capacity of communities to challenge and resist violent extremists'.[98] The strategy builds on earlier government initiatives in the field, which examined 'how local communities themselves can be empowered to tackle extremist ideologies'.[99] Although the internet is mentioned at several points as a vehicle for extremist rhetoric, little consideration is given to ways in which communities can build resilience through the use of information technologies. As will be argued in this chapter, one such way is the systematic encouragement of internet-based initiatives created and maintained by communities independent of government.

This chapter proposes the creation of an independent fund to provide seed money for online initiatives aimed at countering extremism and extremist messages across Britain. The aim is to capitalise on the enthusiasm and goodwill of communities around the country who might be willing to invest time and commitment but need limited financial support in order to get their ideas 'on the net'. As in venture capital, this approach will make it possible to support a wide variety of projects, aimed at many different audiences, which have high potential but might otherwise be considered too unconventional or risky. Since the cost of failure is relatively small, the ones who succeed will more than compensate for the failure of others.

Independence

The first chapter of this report described the dilemma faced by many governments when attempting to promote positive messages through the internet: while wanting to help groups that are involved in countering extremism, they cannot be seen to be doing so for fear that this might compromise the groups' credibility and independence in the eyes of their audience.

In the current climate of conspiracy and paranoia, government sponsorship can be the 'kiss of death' for independent initiatives hoping to counter extremism. This could be seen in the context of the so-called Preventing Violent Extremism Pathfinder Fund, which was launched by government in 2006 to finance Muslim grassroots initiatives. As it turned out, not many groups were willing to take money from the government. Furthermore, the initiative's exclusive focus on Muslim communities was seen as divisive, with the result that those who would have most benefited from additional funding chose not to apply (see Box 8).

[98] Home Office, *The Prevent Strategy: A Guide for Local Partners in England – Stopping people becoming or supporting terrorists and violent extremists*, 3 June 2008; available at http://security.homeoffice.gov.uk/news-publications/publication-search/prevent-strategy/.

[99] Commission on Integration and Cohesion, *Our Shared Future*, report for Department for Communities and Local Government, 2006; available at http://www.integrationandcohesion.org.uk/~/media/assets/www.integrationandcohesion.org.uk/our_shared_future%20pdf.ashx.

In the present environment, it is extremely unlikely that online projects seen to be funded, controlled or otherwise ‘manipulated’ by government would have any credibility or legitimacy, and would consequently be of little use to anyone.[100] A vital pre-condition for any effort at promoting counter-extremism initiatives on the internet is therefore for the funding mechanism to be seen as independent. The best way to avoid accusations of meddling and manipulation would be for the government to set up a fund, which – if not equipped with an endowment – would receive a guarantee of long-term funding and be established as an independent foundation.

The fund’s mission would be to support British-based initiatives aimed at promoting political education, community cohesion and resilience with a particular view to countering violent extremism and its messages. It would not be aimed at Muslim communities exclusively, but the foundation could obviously decide to set different priorities from year to year. Whatever its precise structure and design, it would be vital for the organisation not to be run by government or to be governed by it, and to make sure that – within the broad remit of its charter and mission – it would be free to set its own priorities and take independent decisions.

Small grants

As pointed out in Chapter 2, the rise of the internet has dramatically reduced the cost of communication. Traditional newspapers and television stations are under increasing pressure precisely because new competitors have emerged which – in earlier periods – would have been unable to enter the market because of the huge investments needed for production and distribution. Some of the most successful commercial sites on the internet started as projects by students or other enthusiasts, initially relying mostly on the goodwill and commitment of those who decided to become involved. Some money might have been needed to get the project off the ground, but these tended to be small sums, often borrowed from parents or taken from savings.

Most of the government’s past initiatives in this area have ignored this lesson on how the internet has evolved. Rather than acting as the provider of seed money, giving limited amounts of money to the most promising projects, the government believed there could be a small number of websites which – if showered with money – would evolve into the predominant vehicles through which to take on violent extremism and its messages. By putting all its eggs into just a few baskets, however, the government not only ignored the logic of the internet, it also spent large amounts of public money without making any significant difference.

Take, for example, the *Radical Middle Way* website,[101] which grew out of the government’s consultations with Muslim community leaders in the wake of the July 2005 bombings[102] and has been supported with generous grants from the Home Office and the Foreign Office.[103] The site is well designed and provides a range of highly sophisticated and mostly well-intentioned content but the overall effectiveness of the initiative remains open to debate.[104]

It seems obvious, therefore, that giving small start-up grants – perhaps in the range of £5,000 to £10,000 – to a variety of different initiatives is a more promising strategy than hoping for a small number of well-funded projects to succeed. Doing so would make it possible to support a larger number and broader range of online activities, including those targeted at small demographics or segments of the community, as well as initiatives with a strictly local or regional focus. It would also make it easier to support unconventional projects – for example, those aimed at utilising new and emerging technologies – which might otherwise be considered too risky.

Evaluating success

One of the key functions of the proposed start-up fund would be to monitor the success of funded projects. In doing so, the immediate goal would be to make sure that money is spent wisely. Equally important, however, evaluating the success of one’s investments would provide vital information about what kinds of projects gain traction within certain communities, so that future funding decisions can be fine-tuned accordingly. For example, in the context of preventing Islamist militant radicalisation, rather than spending large amounts of money on static surveys about British Muslims’ use of the internet, the government (and other organisations) could use the data provided by the start-up fund as a dynamic source of information through which to follow emerging trends and/or confirm existing patterns.

Based on their performance, the recipients of start-up grants could apply for further funding. In deciding their eligibility, traffic volume should not be seen as the only indicator of success. This would be unfair to projects aimed at local audiences or smaller segments within certain communities, or those experimenting with new and emerging technologies. At the same time, it would still be important for such indicators to exist and be clearly defined, so that the start-up fund can cut support where projects clearly have not worked and instead use the money for other, more promising initiatives.

There can be no question that many of the projects that might receive support will be unsuccessful. This should come as no surprise. The internet, after all, is a hugely dynamic environment, and it is not at all clear why certain websites fail while others succeed. Even if it was possible to find an explanation, new technologies and modes of interaction might soon make it irrelevant.

It is precisely because there is not one recipe for success that a dynamic and adaptable funding instrument such as the proposed

[100] Although this is the case, the UN reports that of 34 member states consulted, 12 were pursuing internet-based programmes to combat its role in violent extremism. See United Nations Counter-Terrorism Implementation Task Force, *First Report of the Working Group on Radicalisation and Extremism that Lead to Terrorism: Inventory of State Programmes* (Geneva: United Nations, September 2008); available at http://www.un.org/terrorism/pdfs/Report o the Working Group – Workgroup 2.pdf.

[101] Radical Middle Way website (http://www.radicalmiddleway.co.uk)

[102] See Home Office, *‘Preventing Extremism Together’* working group reports: *August-October 2005* (London: Home Office, 2005); available at http://www.communities.gov.uk/documents/communities/pdf/152164.pdf.

[103] Radical Middle Way, ‘Supporters’ (http://www.radicalmiddleway.co.uk/partners_supporters.php).

[104] Radical Middle Way employee, Home Office seminar, October 2008.

start-up fund would be important and appropriate. Rather than being based on any given theory about what makes a website successful, the fund represents a never-ending exercise in empiricism, which – in some way – is exactly how the internet itself has become what it is today. If, of 50 funded projects, only one becomes a major portal for the community it aims to reach, the investment would have more than paid off.

Like all the other proposals included in this report, the start-up fund alone will not be effective in countering online radicalisation. It needs to be part of a wider, comprehensive strategy. What elements this strategy should entail will be described in the following chapter.

BOX 8 The Preventing Violent Extremism Pathfinder Fund

Launched in October 2006, the Department for Communities and Local Government's Preventing Violent Extremism Pathfinder Fund is an instrument for supporting local authorities in developing their own programmes to tackle violent extremism. The Fund boosts the PREVENT element of the government's national counter-terrorism framework by involving local authorities and giving them responsibility for initiating and sponsoring local projects.[105] The original budget was set at £5m for the 2007/8 financial year, later revised to £6m, with a total of at least £70m to be distributed over a three-year period.[106]

In 2007/8, money was made available to a range of community projects in England, including a project in Haringey linking Tottenham Hotspur Football Club with local Muslim youth organisations; a Muslim youth and adult education programme in Barking and Dagenham; the 'Black Country Imams' scheme providing training to domestic clerics; and several other initiatives aimed at promoting positive Muslim self-awareness, community resilience, and civic participation.[107] The amount spent on projects varied widely from several hundred pounds to over £75,000.[108] The efficacy of these projects remains to be seen, as projects were charged with their own monitoring and evaluation activities. To avoid questionable activities from being sponsored, further mechanisms of due diligence will have to be introduced in future.

The Fund has attracted public suspicion and disquiet as well as constructive criticism.[109] Problems with disbursing monies from the Fund – recently highlighted in a BBC radio documentary – suggest that it has not been easy to find groups or individuals willing or able to undertake community projects under the scheme.[110] One of its principal failings has been its exclusive focus on Muslim communities, which – in the eyes of many British Muslims – seemed to suggest that their communities are 'the problem'.[111] More generally, in the current political environment, government-funded schemes are automatically perceived as tainted by government and find it difficult – if not impossible – to derive legitimacy, credibility and, by extension, effectiveness in fulfilling their aims.

[105] Department for Communities and Local Government, *Preventing Violent Extremism Pathfinder Fund: Guidance Note for Government Offices and Local Authorities in England* (London: CLG, February 2007); available at http://www.communities.gov.uk/documents/communities/pdf/320330.pdf.

[106] A figure confirmed in Parliament by Under-Secretary of State Parmjit Dhanda on 29 November 2007; available at http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm071129/text/71129w0028.htm.

[107] Department for Communities and Local Government, *Preventing violent extremism pathfinder fund 2007/08*: *Case studies* (London: CLG, April 2007); available at http://www.communities.gov.uk/documents/communities/pdf/324967.pdf.

[108] Department for Communities and Local Government, *Preventing Violent Extremism Pathfinder Fund 2007/2008* (London: CLG, December 2008); available at http://www.communities.gov.uk/documents/communities/pdf/1092863.pdf.

[109] Audit Commission & HM's Inspectors of Constabulary, *Preventing Violent Extremism: Learning and Development Exercise – Report to the Home Office and Communities and Local Government* (London: Audit Commission, October 2008); available at http://www.audit-commission.gov.uk/prevent/downloads/prevent.pdf.

[110] BBC, transcript of Radio 4's *File on 4*, 'Violent Extremism', first broadcast 18 November 2008; transcript available at http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/18_11_08_fo4_extreme.pdf.

[111] See, for example, Reading Muslim PVE Crisis Group website, http://pvecrisisgroup.com/. This feeling has been compounded by the incorporation of National Indicator 35 (NI35) – 'Building resilience to violent extremism' – into local authority outcome assessments. See Department for Communities & Local Government, *National Indicators for Local Authorities and Local Authority Partnerships: Handbook of Definitions*, revised edn. (London: CLG, May 2008); available at http://www.communities.gov.uk/documents/localgovernment/pdf/735112.pdf.

8 Conclusion

This report has examined what governments, industry and civil society can do to counter online radicalisation. Traditionally, most governments have focused on identifying technical solutions, believing that if somehow radicalising material can be removed from the web or made unavailable for viewing, the problem will go away. Yet, as this report has shown, any strategy that relies on reducing the availability of content alone is bound to be crude, expensive and counterproductive.

The comparison with efforts to counter child sexual abuse on the internet is flawed, because much of the material involved in child sexual abuse is clearly illegal and there are no political constituencies which might be offended if repressive action is taken against it. Child sexual abuse is not a free speech issue, whereas radical political propaganda is.

Any strategy hoping to counter online radicalisation must aim to create an environment in which the production and consumption of such materials become not just more difficult in a technical sense but unacceptable as well as less desirable. This includes:

- *Deterring producers of extremist materials and creating a more hostile environment for extremist messages.* We propose the selective use of takedowns in conjunction with prosecutions as a means of signalling that cyberspace is not beyond the law, and that individuals involved in the production and dissemination of extremist materials might face prosecution.

- *Empowering online communities to self-regulate and enforce their own standards of what is considered acceptable.* We recommend the creation of an Internet Users Panel that would strengthen reporting mechanisms and complaints procedures, thereby enabling internet users to be more effective in 'policing' the online communities to which they belong.

- *Reducing the appeal of extremist messages.* We argue that more attention should be paid to media literacy as a way of strengthening young people's 'defences' against extremist messages. A comprehensive review of existing approaches will be necessary to ensure that measures for countering online hate are appropriately considered and all stakeholders' contributions are maximised.

- *Promoting positive messages.* We propose the establishment of an independent start-up fund for grassroots initiatives to provide seed money for online projects aimed at countering extremist messages. The aim is to create a mechanism through which communities' goodwill and enthusiasm can be translated into concrete and positive action without compromising their integrity and credibility.

The report also emphasises that – instead of relying on government alone – it is vital to capitalise upon the contributions of all stakeholders, including internet companies and internet users.

Throughout the process of consultation, the research team encountered a tremendous amount of interest and goodwill. The internet industry, for example, may have concerns about heavy-handed government regulation, but it seems quite ready to make a positive contribution where this is possible and constructive. Such expressions of intent should be actively drawn upon in constructing a truly comprehensive strategy.

The same is true for evolving technologies and modes of interaction. The rise of user-generated content, for example, is often seen as a danger, because much of the material involved in online radicalisation is made available in this way. Yet, as has been shown, not only is user-generated content here to stay, if properly understood it can become a powerful force in countering radicalisation.

The recommendations put forward in this report are not meant to be the only good ideas supporting a strategy for countering online radicalisation. They are certain to be overtaken by the rapid development of the internet, with the advent of new applications and technologies likely to produce entirely new challenges in the near future.

Whatever the approach taken, any new strategy ought to reflect the fact that radicalisation is a real-world phenomenon that occurs not just in cyberspace but in communities across the country, and whose consequences are not confined to cyberspace but can be a matter of life and death.

Acknowledgements

Many individuals have helped us in shaping the ideas in this report. Particularly important were Mike Whine and Dave Rich at the Community Security Trust, who facilitated many contacts and provided sound advice.

Among the many people who took some of their time to speak to us or participate in one of our workshops were: Burhan Ali, Toby Archer, Matt Armstrong, Akil Awan, Abdul Haqq Baker, Chip Berlet, David Bhowmik, Neville Bolt, Ian Brown, Camille de Stempel, Maura Conway, Steven R. Corman, Yusuf Desai, Nick Fielding, Chiara Fonio, Gerry Gable, Frank Gardner, Mark Goldberg, Lorraine Grieve, Nigel Hawthorn, Evan F. Kohlmann, Mina al-Lami, Laura Leets, Nick Lowles, David Macnaghten, Will McCants, Tariq Modood, Cian Murphy, Yassin Musharbash, Mehmood Naqshbandi, Ben O'Loughlin, John Ozimek, Raffaello Pantucci, Gilbert Ramsay, Eric Randolph, Steve Rigby, Johnny Ryan, Rehan Shiraz, Stephen Tankel, Steve Tatham, Marisa Urgo, Richard Warnes, Noel Warr, Aaron Weisburd, and Victoria Withington.

We also wish to thank all the participants and collaborators who requested not to be named.

This project was the first to bring together industry, experts and governments on the issue of online radicalisation. We are grateful for the cooperation we received from the Internet Services Providers Association and many of its members, the Internet Watch Foundation, and the British government, civil service, law enforcement, and security services. In addition, the report draws on discussions with members of the governments of Austria, Canada, Finland, France, Germany, Ireland, Israel, Italy, Norway, Romania, Sweden, Switzerland, and the United States of America.

At ICSR, numerous people were involved in assisting the project, including Andreas Berg, Charlie Burnard, Ryan Evans, Vanessa Haas, Eelco Kessels, Elettra Pauletto, Katie Rothman, Terra Robinson and Kacie Yood. We should also mention the important role played by two of our trustees, John Sacher and Henry Sweetbaum, in allowing us to draw on their expertise in the technology sector and promoting the project on both sides of the Atlantic. We would also like to thank Steven Hirth, a member of our development committee and a true friend of ICSR.

Finally, we wish to thank Rena Shulsky and Dr. Sami David as well as the Community Security Trust, whose generosity and outstanding commitment to the public good made it possible to carry out this important piece of research.

Needless to say, while we are deeply grateful for all the support, any and all mistakes in this report are the authors' alone.

Further reading

Books, articles and policy reports

- Robert D. Atkinson and Daniel D. Castro, *Digital Quality of Life: Understanding the Personal and Social Benefits of the Information Technology Revolution* (Washington, DC: The Information Technology and Innovation Foundation, October 2008); available at http://www.itif.org/filesDQOL.pdf.
- Akil N. Awan, 'Virtual jihadist media: Function, legitimacy and radicalizing efficacy', *European Journal of Cultural Studies*, Vol.10, No.3 (2007), pp. 389-408.
- Tore Bjørgo (ed.), *Root Causes of Terrorism: Myths, realities and ways forward* (London & New York: Routledge, 2005).
- Tore Bjørgo and John Horgan (eds.), *Leaving Terrorism Behind: Individual and collective disengagement*, (London & New York: Routledge, 2009).
- James Brandon, *Virtual Caliphate: Islamic extremists and their websites* (London: Centre for Social Cohesion, January 2008).
- Ian Brown, 'Internet censorship: be careful what you ask for', *OSCE (Media Regulation on the Internet)*, forthcoming 2009; available at http://ssrn.com/abstract=1026597.
- David Buckingham with Shaku Banaji, Andrew Burn, Diane Carr, Sue Cranmer and Rebekah Willett, *The Media Literacy of Children and Young People* (London: Ofcom, 2005); available at http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/ml_children.pdf.
- Tanya Byron, *Safer Children in a Digital World: The Report of the Byron Review* (London: Department for Children, Schools and Families, March 2008); available at http://www.dcsf.gov.uk/byronreview/pdfs/Final Report Bookmarked.pdf.
- Frank J. Cilluffo and Gregory Saathoff, *NETworked Radicalization: A Counter-Strategy* (George Washington University Homeland Security Policy Institute and the University of Virginia Critical Incident Analysis Group, May 2007); available at http://www.gwumc.edu/hspi/reports/NETworked Radicalization_A Counter Strategy.pdf.
- Steven R. Corman, Angela Trethewey and H.L. Goodall, Jr. (eds.), *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism* (New York: Peter Lang, 2008).
- Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA & London: MIT Press, 2008).
- Jan Fernback, 'There is a there there: Notes toward a definition of cybercommunity', in Steve Jones (ed.), *Doing Internet Research: Critical issues and methods for examining the Net* (London: Sage Publications, 1999), pp.203-220.
- Boaz Ganor, *The Counter-Terrorism Puzzle: A Guide for Decision Makers* (New Brunswick, NJ & London: Transaction Publishers, 2005).
- Boaz Ganor, Katharina Von Knop and Carlos Duarte (eds.), *Hypermedia Seduction for Terrorist Recruiting*, NATO Science for Peace and Security Series E: Human and Societal Dynamics, Vol.25 (Amsterdam: IOS Press).
- Gordon Graham, *The Internet: A Philosophical Enquiry* (London & New York: Routledge, 1999).

- Home Office, *Countering International Terrorism: The United Kingdom's Strategy*, July 2006; available at http://www.official-documents.gov.uk/document/cm68/6888/6888.pdf.
- Home Office, *The Prevent Strategy: A Guide for Local Partners in England – Stopping people becoming or supporting terrorists and violent extremists*, June 2008; available at http://security.homeoffice.gov.uk/news-publications/publication-search/prevent-strategy/.
- House of Commons Culture, Media and Sport Committee, *Harmful content on the Internet and in video games*, Tenth Report of Session 2007-08, July 2008; available at http://www.parliament.the-stationery-office.com/pa/cm200708/cmselect/cmcumeds/353/353.pdf.
- Adam Joinson, Katelyn McKenna, Tom Postmes and Ulf-Dietrich Reips (eds.), *The Oxford Handbook of Internet Psychology* (Oxford: Oxford University Press, 2007).
- Daniel Kimmage, *The Al-Qaeda Media Nexus: The Virtual Network Behind the Global Message* (Radio Free Europe/Radio Liberty Special Report, March 2008); available at http://docs.rferl.org/en-US/AQ_Media_Nexus.pdf.
- Evan F. Kohlmann, 'Anatomy of a Modern Homegrown Terror Cell: Aabid Khan *et al*. (Operation Praline)' *NEFA Foundation Special Report*, September 2008; available at http://www.nefafoundation.org/miscellaneous/nefaaabidkhan0908.pdf.
- Sonia Livingstone, 'Media Literacy and the Challenge of New Information and Communication Technologies', *The Communication Review*, Vol.7 (2004), pp.3-14.
- Sonia Livingstone, Elizabeth Van Couvering and Nancy Thumim, *Adult Media Literacy: A review of the research literature* (London: Ofcom, 2005); available at http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/aml.pdf.
- J. Rami Mroz, *Countering Violent Extremism: Videopower and Cyberspace* (New York: EastWest Institute, 2008); available at http://www.ewi.info/pdf/Videopower.pdf.
- Andrew D. Murray, *The Regulation of Cyberspace: Control in the Online Environment* (Abingdon & New York: Routledge-Cavendish, 2007).
- National Coordinator for Counterterrorism, *Jihadis and the Internet* (The Hague: NCTb, 2007); available at http://english.nctb.nl/Images/Jihadis and the Internet_tcm51-52881.pdf?cp=51&cs=7365.
- Peter R. Neumann and Brooke Rogers, *Recruitment and Mobilisation for the Islamist Militant Movement in Europe* (ICSR, King's College London, on behalf of the European Commission Directorate-General for Justice, Freedom and Security, October 2008); available at http://www.icsr.info/files/ICSR EU Research Report_Proof 01.pdf.
- D. Elaine Pressman, *Countering Radicalization: Communication and Behavioral Perspectives* (The Hague: Clingendael Centre for Strategic Studies, 2006); available at http://www.hcss.nl/en/download/67/file/20060100_csss_insight_1.pdf.
- Gilbert Ramsay, 'Conceptualising Online Terrorism', *Perspectives on Terrorism*, Vol.2, No.7 (2008), pp.3-10.
- Louise Richardson, *What Terrorists Want: Understanding the Terrorist Threat* (London: John Murray, 2006).
- Hanna Rogan, 'Jihadism Online – A Study of how al-Qaida and radical Islamist groups use the net for terrorist purposes', *FFI Report*, 2006/0915; available at http://www.investigativeproject.org/documents/testimony/48.pdf.
- Johnny Ryan, *Countering Militant Islamist Radicalisation on the Internet: A User Driven Strategy to Recover the Web* (Dublin: Institute of European Affairs, 2007).
- Marc Sageman, *Understanding Terror Networks* (Philadelphia, PA: Pennsylvania University Press, 2004).
- Anne Stenersen, 'The Internet: A Virtual Training Camp?', *Terrorism and Political Violence*, Vol.20, No.2 (2008), pp.215-233.
- Max Taylor and Ethel Quayle, *Child Pornography: An Internet Crime* (Hove & New York: Brunner-Routledge, 2003).
- Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, D.C.: United States Institute of Peace Press, 2006).
- Paul Wilkinson, *Terrorism versus Democracy: The Liberal State Response*, 2nd edn. (London & New York: Routledge, 2006).

Web resources

- Anti-Defamation League
  www.adl.org
- Berkman Center for Internet and Society
  http://cyber.law.harvard.edu
- Center for Internet and Society
  http://cyberlaw.stanford.edu
- Child Exploitation and Online Protection Centre
  www.ceop.gov.uk
- Crown Prosecution Service
  www.cps.gov.uk
- Department of Communities and Local Government
  www.communities.gov.uk
- Electronic Frontier Foundation
  www.eff.org
- EuroISPA
  www.euroispa.org
- Home Office Counter-terrorism Strategy
  http://security.homeoffice.gov.uk/counter-terrorism-strategy
- International Association of Internet Hotlines
  www.inhope.org
- International Network Against Cyberhate
  www.inach.net
- Internet Services Providers Association
  www.ispa.org.uk
- Internet Watch Foundation
  www.iwf.org.uk
- Media Awareness Network
  www.media-awareness.ca
- Ofcom
  www.ofcom.org.uk
- OpenNet Initiative
  http://opennet.net
- Oxford Internet Institute
  www.oii.ox.ac.uk
- Southern Poverty Law Center
  www.splcenter.org

Countering Online Radicalisation

Political extremists and terrorists are increasingly using the internet as an instrument for radicalisation and recruitment. What can be done to counter their activities?

Countering Online Radicalisation examines the different technical options for making 'radical' internet content unavailable, concluding that they all are either crude, expensive or counter-productive.

It sets out a new, innovative strategy which goes beyond 'pulling the plug', developing concrete proposals aimed at:

- Deterring the producers of extremist materials
- Empowering users to self-regulate their online communities
- Reducing the appeal of extremist messages through education
- Promoting positive messages

Countering Online Radicalisation results from the first systematic effort to bring together industry, experts and government on the issue of online radicalisation. Its insights and recommendations are certain to be of great interest to experts and policymakers around the world.

Advance Praise for Countering Online Radicalisation

This accessible yet sophisticated analysis reflects a deep and up-to date understanding of Internet radicalisation. It offers detailed and practical solutions to the daunting challenge of regulating the jihadi Internet. In short, this is essential reading for policymakers and analysts worldwide.

Thomas Hegghammer
Kennedy School of Government,
Harvard University.
Contributor to *jihadica.com*

Particularly useful are the report's practical recommendations on user-driven mechanisms to regulate internet content, small grants for relevant stakeholders, arguments against censorship, and focus on the role of schools. Above all, the idea that 'less is more' in Government action online injects some much needed common sense: The authors clearly 'get' the Internet, radicalisation, and policy.

Johnny Ryan
Institute of International and
European Affairs, Dublin.
Author of *Countering Militant Islamist Radicalisation on the Internet* (IIEA, 2007)

KING'S College LONDON
University of London

Penn
UNIVERSITY of PENNSYLVANIA

IDC HERZLIYA
ICT International Institute for Counter-Terrorism

Regional Centre on Conflict Prevention

www.icsr.info