Jihad Trending:

A Comprehensive Analysis of Online Extremism and How to Counter it

By Ghaffar Hussain and Dr. Erin Marie Saltman

QUILLIAM

Quilliam is the world's first counter-extremism think tank set up to address the unique challenges of citizenship, identity, and belonging in a globalised world. Quilliam stands for religious freedom, equality, human rights and democracy. Challenging extremism is the duty of all responsible members of society. Not least because cultural insularity and extremism are products of the failures of wider society to foster a shared sense of belonging and to advance democratic values. Quilliam seeks to challenge what we think, and the way we think. It aims to generate creative, informed and inclusive discussions to counter the ideological underpinnings of terrorism, whilst simultaneously providing evidence-based recommendations to governments for related policy measures.

For further information contact:

Quilliam

Email: information@quilliamfoundation.org

Tel: +44 (0)207 182 7280

www.quilliamfoundation.org

Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it
Quilliam, May 2014

ISBN number: 978-1-906603-99-1

Foreword

In his examination of the origins of Nazism, the great historian Norman Cohn warned against the mistake of supposing that the only writers who matter "are those whom the educated in their saner moments can take seriously". Swirling below lay a "subterranean world where pathological fantasies disguised as ideas are churned out by crooks and half-educated fanatics for the benefit of the ignorant and superstitious".

Who wants to waste valuable time confronting them? The debate will never progress. Crackpots never admit they are wrong, but shift from one conspiratorial tirade to the next. The true goal of debate, however, is not to change the minds of your opponents, but the minds of the watching audience. If you give up on the battle of ideas, or assume that you can win it without a fight, the audience may go over to the other side.

Europe learned the hard way in the 20th century that "pathological fantasies" can and will blight the lives of hundreds of millions. I accept that Islamist extremism is not in the same league as fascism, although that is not for want of trying. The danger remains that it may grow stronger if you pretend it is not there, or dismiss it with the comfortable delusion that is merely an inchoate reaction to western provocation which will vanish when we mend our ways.

The temptation for many governments is to fight by silencing its half-educated and, indeed, half-crazed adherents. Censorship seems so much easier than taking them on intellectually. There is a permeating belief that jihadi websites groom impressionable young men and turn them to violence. Edward Snowden's revelations show that the Western security services can invade the privacy of just about everyone and amass astonishing amounts of intelligence. Why not combine technical capacity with the moral imperative to stop men imbibing a murderous ideology.

Unfortunately, for the authorities, while the web may be a secret-policeman's dream, it isn't a playground for censors. Start closing down sites and not only will you deny our spies access to useful intelligence, but you will run into the technological limits of state power. Extremists use blogs, instant messaging, video sharing sites, Twitter and Facebook. Democratic states may try to tell their owners what content they should host, but it is a

doomed enterprise. When Twitter suspended the accounts of al-Shabaab it came back under different guises. True, China, Iran, Pakistan, Eritrea and Turkey have banned Twitter or YouTube. But this is not a club any self-respecting society should want to join. Even in these instances, blanket web censorship has been designed to stop the bulk of the population from finding information governments do not want them to read. The highly motivated have always found ways around their firewalls and, by definition, terrorists and potential terrorists are highly motivated.

The only state I can see that has imposed total web censorship is North Korea, and not even our most ardent national security conservatives want to emulate Pyongyang.

The alternative, advocated here, is for governments to mobilise liberal opinion: to give refugees from totalitarian religious ideologies – its idealistic opponents and its victims – the means to fight extremists online and challenge them at every opportunity. At present we are in the absurd position where Western governments condemn the Assad regime for its crimes against humanity, but arrest Muslims who travel to Syria to fight it. They do not bother to argue against jihadist groups, do not seek to explain to young men why they should not join them. The authorities believe their case is so obvious it does not need to be made, and succeed only in looking like perfect hypocrites.

For if you cannot explain yourself, you have no right to be surprised if no one respects you. More pertinently, you have no right to be surprised when young men pay heed instead to those who at least show them the courtesy of talking to them.

The authors of this essential report make a powerful and liberal case for the importance of fighting the battle of ideas. Technical quick fixes are an illusion; there is no alternative to confronting men, who need to be exposed and ridiculed at every turn. If the radical underground is not confronted, we know what may follow. “There are times,” said Cohn, “when this underworld emerges from the depths and suddenly fascinates, capture and dominates multitudes of usually sane and responsible people, who thereupon take leave of sanity and responsibility.” Better to argue the living daylights out of it, before it does.

Nick Cohen

British Journalist, author and political commentator.

Authors Note

This report hopes to contribute to developing research in the ever-evolving arena of radicalisation with a particular focus on the role of the Internet. Our aim is to provide a resource for both policy makers and practitioners that offers an in-depth insight into the means by which extremists use online tools to propagandise and recruit. While previous research has focussed on specific aspects of this phenomenon, this report aims to provide a comprehensive analysis encompassing both qualitative and quantitative methods. It is also unique in that it offers a detailed and practical guide on how to turn the tide against extremists online and reclaim the Internet.

Our research would not have been possible without the cooperation and assistance of colleagues, experts, mentors and focus group participants. In particular, we would like to thank our research assistants Ariana Skipp and Aimee Gentry who diligently collected data transcribed interviews and proofread drafts. We would also like to thank Jonathan Russell, Usama Hasan, Faisal Ghazi, Verity Harding, Florian Maganza and Benoit Tabaka for their support, assistance and guidance.

Table of Contents

Executive Summary

Online extremism and the role the Internet plays in the radicalisation process is currently being debated and discussed by journalists, academics, technologists and government officials alike. This report seeks to demystify this area and expose the manner in which online tools are being used by Islamist extremist organisations and individuals to recruit and propagandise. Current measures to tackle online extremism are assessed and critiqued, after which the report details a practical strategy for countering extremism online and making the Internet a less hospitable domain for extremists.

The research conducted for this report focuses on Islamist extremist groups operating in the UK and France, mapping their use of the Internet and what they hope to achieve through their online activities. Popular online platforms such as YouTube, Facebook, Twitter as well as chat rooms, discussion forums and static websites are analysed with a view to assessing the role online extremist messaging plays in the radicalisation process. The report also addresses the issue of censorship, assessing the effectiveness of current filtering methods available and their overall efficacy.

Key findings in this report:

- With the Internet often being accused of producing radicalisation in isolation of other factors, this report found the vast majority of radicalised individuals come into contact with extremist ideology through offline socialisation prior to being further indoctrinated online.
- Although governments are increasingly relying on censorship and filtering methods to counter online extremism, this report found that negative measures, or censorship in general, were not only ineffective and costly but potentially counter-productive.
- Positive measures, such as developing counter-extremist content and popularising online initiatives that fight against extremism are much more effective in challenging extremist ideologies. There are currently not enough materials that counter extremist content online, allowing extremists to monopolise certain issues.

This report seeks to differentiate itself from previous reports on online extremism in two ways; firstly the research itself is much more in-depth and diverse, combining qualitative and quantitative data to reach conclusions. Secondly, this report offers a comprehensive and practical list of recommendations which, if implemented fully, could unleash a new wave of online activism that will take the fight to extremists online, breaking the current monopoly they hold over certain socio-political issues.

These recommendations include:

- Establish a forum that deals with online extremism and brings stakeholders from key sectors together in order to do so.
- Improve digital literacy and critical consumption skills in schools and communities.
- Encourage the establishment of a social media outlet that clarifies government policies and debunks propaganda.
- A mapping exercise that explores current efforts to tackle extremism online and identifies partners that could be given support to develop an effective online presence.
- Establish a central body that offers seed funding and training for grassroots online counter-extremism initiatives.
- More research into how the radical right is using the Internet to propagandise.

The findings and recommendations of this report suggest a clearer understanding of the role the Internet plays in the radicalisation process, and an appreciation of the dangers that relying on illiberal censorship, can contribute towards the development of a more holistic approach to tackling extremism online. Relying on the cultivation of grassroots initiatives to develop and promote counterspeech online, as opposed to censorship, could help turn the tide against current extremist efforts. However, co-operation and regular communication between stakeholders from key sectors is vital in order for the above vision to be realised and, thus, the establishment of a forum that allows this to take place is also important.

Glossary of Terms

Al wala' wal bara': The belief that Muslims owe allegiance to Muslims alone and must reject non-Muslims as allies or friends.

Counterspeech: Articles, videos, speeches and other material that seeks to challenge hateful or extreme views through positive messaging and narratives.

Dark Web: Content that is not accessible on the web through conventional means and is unreachable through open source browsing.

Fatwa: A religious edict, often issued by a religious authority in response to a question seeking clarification of Islamic doctrine.

Hacktivism: Online activism which relies on hacking technology to disrupt, disturb or replace online content without the consent of the website or account owner.

Islamist Extremism/Islamism: The belief that Islam is a totalitarian political ideology. It claims that political sovereignty belongs to God rather than the people. Islamists believe that their reading of Shariah should be state law, and that it is the religious duty of all Muslims to create and pledge allegiance to an Islamic state that reflects these principles.

Jihad: Literally 'to struggle' but often used to refer to armed struggle.

Jihadism: Non-state violence used in the cause of Islamism. Just as Islamism is the politicisation of Islam, jihadists take the traditional concept of jihad and use it as a political and military tool to achieve a political end.

Lone Wolf: Is defined in this report as "a person who acts on his or her own without orders from – or even connections to – an organisation" and as such "is a standalone operative who by his very nature is embedded in the targeted society and is capable of self-activation at any time**".**[1]

[1] Burton Fred & Stewart, Scott (2008), 'The "Lone Wolf" Disconnect', Statfor Global Intelligence, 30 January.

Negative Measures: Counter-terrorist and/or counter-extremist initiatives which block, filter, take-down or censor extremist content.

Positive Measures: Counter-extremism and counterspeech initiatives that seek to challenge extremist narratives and propaganda by producing counter-content.

Radicalisation: Radicalisation is the processes by which individuals and/or groups come to adopt extremist ideologies. Scholars sometimes distinguish between 'radicalisation' and 'violent radicalisation' in order to highlight the difference between engagement in violent activities and radicalised non-violent thinking.

Salafism/Wahhabism: A revivalist Sunni Muslim literalist movement that believes Muslims should shed traditional theological edicts and instead derive new religious guidance directly from the sources.

Terrorism: The use of violence or illegal force targeted at civilians by non-state actors that seek to bring about political/societal changes.

Ummah: Often used to mean global community of Muslims, though the term has been used to refer of smaller political communities too.

Chapter 1. Introduction

We live in an age in which research, communication, shopping and even dating is increasingly taking place online. In fact, many online activities, such as sending e-mails, have become the default, replacing similar offline means, such as sending written letters. It is, therefore, inevitable that our political and religious views are also shaped by online content. In fact, the Internet is increasingly playing a role in disseminating and propagating messages of a political and/or religious nature.

As the Internet is a powerful tool for reaching a mass audience whilst maintaining anonymity, it has always attracted those wishing to promote marginalised views or risky behaviours. It, therefore, comes as no surprise that extremist groups, both Islamist and far-right, have exploited the potential of the Internet in recent years. In fact, there are now a number of highly sophisticated extremist websites with some attracting thousands of regular visitors, discussed further in Chapter 2.

The media has also targeted the Internet as a prime factor in the radicalisation process leading to terrorist-related incidents. Roshonara Choudhry, the university student who stabbed Stephen Timms MP with a kitchen knife in November 2010, was presented as having been radicalised by Anwar al-Awlaki's lectures found online. The Boston bombers, Tamerlan Tsarnaev and Dzhokhar Tsarnaev, who attacked the Boston marathon in April 2013, were also presented as having been radicalised by online content.

The debate about the impact of extremist content online is a live and active one. Europe is currently experiencing the exodus of a small, but potent, group of young fighters, joining jihadist forces abroad after having been supposedly radicalised by online content. The conflict in Syria, in particular, has a strong online dimension with both sides putting out propaganda videos and providing regular social media updates. In fact, it has been described by some as the first ever YouTube war. [2]

[2] Koetti, Christoph (2014) 'The YouTube War: Citizen Videos Revolutionalise Human Rights Monitoring in Syria', *PBS Media Shift*, (February 18).

In the UK, after the brutal attack on Drummer Lee Rigby in May 2013, the government came under increased pressure to prevent the proliferation of violent extremist ideas and, thus, the Internet became an easy target. A government task force that was subsequently set up identified online extremist propaganda as a key area of focus in a document it published in December 2013.[3] This document outlined the manner in which it hoped the government would tackle online extremism. It included:

- Building the capacity of communities and civil society organisations so that they can campaign against online extremism.
- Working with Internet companies to restrict user access to illegal terrorist materials online, which are hosted overseas.
- Improving the process for public reporting of extremist content.
- Working to include extremist content in family-friendly filters.
- Excluding from the UK foreign nationals who post extremist content online.

Despite the British government recognising the importance of countering extremism online, there continues to be a heavy emphasis on censorship and other negative measures aimed at restricting access.

Other European countries are also being impacted by the perceived threat of online radicalisation. France, for example, generally has very little Internet censorship and is ranked by Freedom House as one of the top countries for Internet freedom. However, more recently, the Interior Minister, Manual Valls, opined that "The Internet has become a vehicle for propaganda, radicalisation and recruitment inspiring jihadist terrorism."[4] He has also stated that he wants to intensify the fight against terrorism on the Internet and increase monitoring of online networks.

Amidst much of the alarmist media reporting and political debates about online radicalisation, the precise role of the Internet in the radicalisation process has not yet been explored in any great detail. The existing literature in this area, contrary to what many

[3] HM Government (2013) 'Tackling Extremism in the UK: Report from the Prime Minister's Task Force on Tackling Radicalisation and Extremism', 4 December, London: Crown Press.
[4] Valls, Maunal. Cited in: Marchive, Valery (2013) 'France Considers Stepping Up Internet Monitoring to Fight Terrorism', *Vive la Tech*, 4 June.

people think, acknowledges the expanding role of the Internet and the efficacy of online propaganda, yet often defines the Internet as a facilitator rather than a driver of radicalisation. In other words, there is very little evidence to support the notion that the Internet radicalises in isolation of external or offline factors.

Modern researchers of online extremist activism recognise that the Internet can become a self-imposed and isolated environment or 'echo chamber,' where individuals willingly and regularly subject themselves to certain narratives without exposure to counter arguments.[5] However, whether or not previously unexposed individuals are adopting extremist ideologies solely through consumption and interaction with extremist content online is questionable.

Previous Research

A report published by the Norwegian Defence Research Establishment (NDRE), entitled 'Jihadism Online', analysed the structures and functions of online jihadism in order to understand how the Internet is being used for terrorist purposes. A section on recruitment opens with "...the Internet plays an important role in recruiting new jihadists." Interestingly, on the very same page the report also states "...there are few examples of direct recruitment on the Internet." [6]

After assessing a few cases, the report asserts "...the Internet is not used as a direct means of recruitment...it functions merely as a facilitator for the recruitment process. Physical contact, in addition to online communication and propaganda, is essential." [7] Hence, whilst the role of the Internet in the radicalisation process receives a disproportionate amount of attention, the idea of the Internet radicalising in isolation is not supported by the evidence. In addition, the case studies make it clear that jihadist recruiters view the Internet, and especially chat rooms, as a means through which new recruits can be found, but the means through which individuals find extremist chat rooms in the first place is not discussed in this report.

[5] Torok, Rohyn (2013) 'Developing an explanatory model for the process of online radicalization and terrorism', *Security Informatics*, 2(6).
[6] Rogan, Hanna (2006) 'Jihadism Online – A study of how al-Qaida and radical Islamist groups use the Internet for terrorist purposes', Norwegian Defence Research Establishment:Kjeller, p. 29.
[7] Rogan, Hanna (2006) Jihadism Online – A study of how al-Qaida and radical Islamist groups use the Internet for terrorist purposes, p. 30.

According to counter-terrorism expert Marc Sageman: "The growth of the Internet has dramatically transformed the structure and dynamic of the evolving threat of global Islamist extremism."[8] Sageman goes on to draw an interesting distinction between the Internet, as an open yet passive source of news and information, and chat rooms or forums that offer interactivity. Regarding interactivity, he states: "No matter how important for propaganda purposes these passive websites are, they are not the engine of radicalisation," further explaining that "[t]hese sites merely reinforce already made-up minds." [9]

Sageman believes that interactive chat rooms can act as an engine of transformation, since they provide validation of existing ideas and support from like-minded people. Chat rooms are, however, self-selecting in that they tend to attract individuals that are already predisposed to a certain way of thinking. Jihadist chat rooms, in particular, are not easy to access or even stay in if you challenge the views expressed therein. Sageman's work suggests the Internet, or online extremist content and tools, act as a medium that facilitate the radicalisation process, rather than initiate it.

This conclusion is also supported by a report about online radicalisation that was published by The International Centre for the Study of Radicalisation (ICSR) in 2009. This report, entitled 'Countering Online Radicalisation – A Strategy for Action', primarily relied on qualitative data obtained from expert interviews and an analysis of online content. With reference to the role of the Internet in the radicalisation process, the report states: "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." [10]

However, the report also claims that the use of the Internet can intensify and accelerate the process of radicalisation because, as a medium, it can normalise more risky behaviours and act as an echo chamber in which extreme ideas are accepted and encouraged. As such, the Internet is not an efficient tool for drawing in new recruits but it is adequate for renewing

[8] Sageman, Marc (2008) *Leader Jihad: Terror Networks in the Twenty-First Century*, University of Pennsylvania Press: Philadelphia, p. 109.
[9] Sageman, Marc (2008) *Leader Jihad: Terror Networks in the Twenty-First Century*, University of Pennsylvania Press: Philadelphia, p. 114.
[10] Stevens Tim and Neumann, Peter (2009) 'Countering Online Radicalisation: A Strategy for Action', *ICSR*, London, p. 12.

the commitment and zeal of existing recruits.[11] Hence, even in an age in which radicalisation involving the Internet is frequently discussed, the offline, or real, world continues to play a pivotal role.

Another report, entitled 'A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists' published in 2011 and authored by Raffaello Pantucci, examines the role of the Internet in cases of lone wolf terrorism. The term 'lone wolf' refers to the theory that individuals can be radicalised solely through the Internet with no prior knowledge of radicalised ideology or people. With reference to a data set of recent lone wolf cases, the author asserts that the Internet "...appears to be a very effective tool: it provides a locus in which they can obtain radicalising material, training manuals and videos."[12] Furthermore, he states that since many lone wolves demonstrate a level of social alienation, online communities of an extremist nature can provide the social environment that such individuals lack in the real world.[13]

The Internet is given a significant role in the radicalisation process for lone wolf terrorists according to the above report. However, the author goes on to argue that since it is impossible to know what such individuals would do in the absence of the Internet, it would be premature to conclude that the role of the Internet is primary. This is especially the case since Internet usage is ubiquitous in today's age and creating a control group to test such a hypothesis is very difficult. [14]

In research about the multi-faceted usage of online resources, Gabriel Weimann, discusses the anonymity that online environments provide alongside the broadening of English language content.[15] Jihadist and extremist sympathisers freely post videos, tutorials and participate in forums which aim to cultivate and solidify partisanships. Increasingly, online information is also provided in English with a growing number of extremist videos containing English subtitles or audio dubbing. However, Weimann also points out that many

[11] Ibid. p. 13.
[12] Pantucci, Raffaello (2011) 'A typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists', *ICSR*, London, p. 34.
[13] Ibid..
[14] Pantucci, Raffaello (2011) 'A typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists', *ICSR*, London, p. 34.
[15] Weimann, Gabriel(2010) 'Terror on Facebook, Twitter, and Youtube', *Brown Journal of World Affairs*, 16(2), pp. 45 – 55.

extremist entities are wary of certain large-scale networks, like Facebook, since they can reveal too much about adherents' identities, networks, social circles and location, potentially informing authorities of crucial information.

NATO's *Science for Peace and Security Series* has produced a publication entitled 'Hypermedia Seduction for Terrorist Recruiting'.[16] The crucial conclusions in this series are that the Internet is a useful tool for developing psychological warfare and 'narrow-casting' in order to locate and specify limited, selective audiences for radicalisation. Membership in these online extremist communities increases the potential for isolation and radicalisation.

Within this series of reports, Jonathan Fighel discusses the relationship between the Internet and direct jihadist recruitment stating: "Terrorists do not use the Internet for direct operational recruitment, but rather to shape a committed virtual radical Islamic community from which individuals will be identified as potential candidates for recruitment."[17] In essence, the Internet is a tool used in a myriad of ways to channel dialogues between like-minded individuals, introducing the potential for recruitment. The Internet as an entity remains a passive platform of ideas.

Active recruitment, promotion and introduction to ideologies available on the Internet remain dependent on person-to-person communication, whether it is in real-life or through online aliases. A 2013 RAND Europe report, entitled 'Radicalisation in the Digital Era,' analysed fifteen case studies of radicalised individuals and used the data obtained in order to test five hypotheses. It found the following:

- The Internet creates more opportunities to become radicalised.
- The Internet acts as an 'echo chamber'.
- The Internet does *NOT* necessarily accelerate the process of radicalisation, rather it can help facilitate this process.
- The Internet does *NOT* allow radicalisation to occur without physical contact.

[16] Ganor, Boaz et. al. (2007) *Hypermedia Seduction for Terrorist Recruiting*, NATO Science for Peace and Security Series, IOS Press: Eilat Israel.
[17] Fighel, Jonathan (2007) 'Radical Islamic Internet Propaganda: Concepts, Idioms and Visual Motifs', *Hypermedia Seduction for Terrorist Recruiting*, NATO Science for Peace and Security Series, pp. 34 – 38.

- The Internet does NOT increase opportunities for self-radicalisation.[18]

These findings support previous studies showing that the Internet, with its ability to enhance information sharing and connectivity, can be a useful tool for those sympathetic to extremist narratives. More importantly, the findings also indicate that the extremist content online does not recruit or radicalise in a vacuum; rather it tends to complement offline efforts at radicalisation and makes life easier for recruiters and wannabe radicals alike, facilitating and accelerating rather than initiating the radicalisation process.

The increasing usage of social networking sites, such as Facebook and Twitter, by extremist and jihadist activists and foreign fighters has also been recognised more broadly in recent research. The ICSR report '#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks' discusses the social media usage of foreign fighters and the decentralised recruitment process through online networks.[19] The report notes that as young target audiences turn to the Internet as a source of learning and inspiration there is increasing concern about how the Internet is being used within the radicalisation process by those disseminating extremist messages and worldviews.

Although the existing research in this area broadly supports the notion that the Internet is a facilitator of radicalisation, rather than an initiator, most of the studies are small-scale and rely on a limited data set. This area of research lacks a larger scale study that incorporates a broad range of quantitative and qualitative data in order to explore the offline impact of online extremist content. The existing research also fails to examine the drivers of traffic to extremist sites, i.e. whether or not it is the quality and influence of the content itself or other external factors. Determining if increased traffic to such sites has an offline impact is also essential in order to assess the impact of extremist content online.

Research Overview

In light of the existing research, as outlined above, this report hopes to comprehensively analyse the impact of online extremist content, while exploring the extent to which such

[18] Behr Ines, Von et al (2013) 'Radicalisation in the digital era: The use of the Internet in 15 cases of terrorism and extremism', *Rand Europe*, Cambridge, p. Xii.
[19] Carter et. al. (2014), '#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks', *ICSR*, London.

material is able to radicalise and recruit people. In particular, this report will gauge the degree to which online radicalisation can take place within a vacuum, devoid of offline influences.

The report will also explore the contentious issue of Internet censorship, or negative measures, with view to seeking a better understanding of the effectiveness of filtering and blocking extremist content. This report also provides suggestions for how extremist content online can be countered and defines the roles different sectors in society can play. As such, this report is a useful resource for governments and policy makers looking into tackling online extremism, as well as academics and public sector organisations that wish to grasp the scale of the problem and develop innovative and proactive solutions.

Methodologically this report uses both qualitative and quantitative research methods with the key findings being based on primary data. The report relies on material gained from extensive interviews with experts in counter-terrorism and mentors who work with convicted extremists. It also relies on data collected from focus conducted with individuals that belong to target audiences, i.e. those that online extremist content seeks to influence. From mapping the scale of Islamist extremism online, the report analyses existing extremist websites, social media accounts, video channels, forums and conversational trends.

The UK and France are used as the primary country case studies since both are western European democracies with increasing concerns about home-grown Islamist radicalisation. Both countries feel at risk due to the influx of extremist Islamist content available in English and French in recent years. The countries also serve as a good point of comparison, due to their different political and historical relations with their domestic Muslim populations and since they have chosen slightly different ways of dealing with the threat of online radicalisation.

This report seeks to first map the scale and nature of radical Islamist content being produced in English and French before going into further analysis about how this content is being consumed and to what ends. Thus, the Chapter 2 analyses static websites, chat rooms, YouTube channels, Facebook pages and Twitter accounts, focusing on those targeted at British and French audiences. While using specific radical Islamist groups, primarily proscribed organisations, as case studies, this chapter addresses how such groups use the

Internet and how successful they are at attracting their target audiences. This chapter is largely quantitative in nature and presents statistics that demonstrate the popularity of certain extremist sites along with displaying the extent to which their content is shared and liked by users.

Chapter 3 seeks to analyse the radicalisation process and the role online extremist material can play. This chapter questions the possibility and likelihood of online radicalisation in isolation of other real-world factors. In other words, it assesses the 'lone wolf' phenomenon in light of other socialising agents and influences that serve to radicalise individuals. Mosques, prisons, universities and the media are analysed as potential 'first spark' agents in which individuals can first come into contact with extremist narratives. This chapter is largely based on qualitative research and valuable empirical data from interviews conducted with academics, mentors and a range of experts in the field of online extremism. It also incorporates data obtained from focus groups conducted with young individuals who have been exposed to extremist material and are familiar with its usage.

Chapter 4 analyses existing counter-extremist and counter-terrorist measures in the UK and France beginning with an assessment of government policies that are based on negative measures. It addresses the pros and cons of attempts to remove, filter or hide extremist content online through technological manipulation and legal means. The chapter then explores existing efforts to tackle extremism online through positive measures giving an overview of existing initiatives. It concludes by pointing to the shortcomings of existing efforts and highlights ways in which they can be improved.

The final body chapter of the report, Chapter 5, elucidates our suggestions and recommendations about what can and should be done to effectively counter extremism online. This chapter highlights what public, private and third sector organisations can and should be doing in this regard and how they can cooperate in order to achieve their end goals. The report concludes with a summary of the essential findings and reiterates the key recommendations offered for countering online extremism.

Chapter 2. The Scale of the Problem

Researching the role that the Internet plays in Islamist radicalisation is ultimately a qualitative endeavour. However, an overview of the scale and diversity of online Islamist extremism, along with its potential influence, is fundamental if the best methods to counter extremism are to be found.[20] Hence, it is necessary to quantify the impact of online Islamist extremism in the UK and France by analysing some of the key trends in availability and support for extremist content.

Our reliance on the Internet for communication and networking has increased dramatically with the arrival of social media tools such as Facebook in 2004, YouTube in 2005 and Twitter in 2006. Advances in online technology have also made Internet-based social networks, newsfeeds and video links more readily available and participatory. These advances, whilst beneficial to all, have also offered greater opportunities for extremists to engage with a wider audience.

This chapter focuses on mapping online material of the most prominent Islamist extremist groups, by analysing content available in English and French that targets British and French audiences. Websites, online organisations and video feeds chosen for analysis throughout this report are the most widely consumed in British and French contexts, rather than those merely created in the UK or France. This choice is deliberate since online content can be developed and distributed across borders, targeting audiences far beyond points of origin.

The first part of this chapter gives an overview of the primary Islamist groups that are used for tracking trends in how extremists are using the Internet. These groups vary in their usage of the Internet as a means for information distribution and recruitment while all having records of activism in the UK and/or France. The second part of this chapter uses these organisations as a basis for mapping the paths online users have available to them, that lead to extremist ideologies. This part also discusses the difficulty of finding extremist content via search engines and how Islamist groups are using websites, chat rooms, videos,

[20] Most of the limited literature on analysing online extremist activism and influence recognises the difficulties in quantifying impact and near impossibility of identifying whether or not the Internet plays a primary or secondary role in socialising extremist ideologies (See: ICSR 2009, Pantucci 2011).

Facebook and Twitter. It concludes with a discussion on the authenticity of online extremist materials and the problematic nature of such authentication. This is followed by a summary that highlights key findings from the chapter and their implications.

2.1 Islamist Organisations Operating in the UK and France

The Islamist groups shown in Table 2.1 were chosen due to their activism and notoriety in networking, recruiting and/or carrying out acts of terrorism by enlisting British or French-based citizens through online means. These groups are producing online content in English and/or French to distribute their messages and establish networks. While most of the selected groups have been proscribed within the UK and/or France, some remain legal. The controversy about how to monitor and deal with certain extremist organisations that do not openly support violence is still subject to debate. Therefore, some extremist groups continue to espouse extreme opinions and ideologies while remaining legal.

Legal structures around proscribing groups and handling controversial Islamist content are based on both EU and national policies and legislation in the UK and France. These legal structures have developed significantly since 9/11 and continue to evolve as new cases emerge and as online capacities advance. The Terrorism Acts that can be used both on and offline in the UK concern primarily the Terrorism Act 2001[21], which began extending the list of proscribed terrorist organisations outside of Northern Ireland as well as defining the meaning of racial hatred and fear offences, and the Terrorism Act 2006, which extended the legal offence of 'glorifying' terrorism. In France similar legislation exists that also defines legal offences for the association with terrorist criminals (article 421-2-1 of the Penal Code).[22] As European Union countries, both the UK and France also adhere to the European Union Counter-Terrorism Strategy, which aims to prevent, protect, pursue and respond to terrorist threats to Europe.[23] The primary aspects of both EU and national terrorism laws (and more broad legal structures) that are used to combat online terrorist efforts are: legal

[21] (2001) 'Anti-Terrorism, Crime and Security Act 2001', *Legislation.gov.uk*.
[22] (22 December 2012), 'LOIS n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme (1)', *Journal Officiel de la République Français*, 1(98).
[23] (2005) 'The European Union Counter-Terrorism Strategy', *Council of the European Union*, 14469/4/06 REV 4.

measures against hate speech; legal measures against planning, facilitating or carrying out terrorist activities; supporting or glorifying proscribed terrorist organisations.

Table 2.1 Islamist Organisations Targeting British and French Online Audiences

	Organisation	Founded	Illegal	Operating
1	Ahlus Sunnah Wal Jama'aah/ Ahl ul-Sunnah Wa al-Jamaah	2005	2006	UK
2	Al-Ghurabaa	2004	2006	UK
3	Al-Muhajiroun	1996	2004	UK
4	Al-Qaeda	1988*	2001	UK/FR
5	Al-Shabaab	2006	2010	UK
6	Ansar al-Haqq	2010	Legal	FR
7	Armed Islamic Group of Algeria/Groupe Islamique Armé (GIA)	1992	2001	UK/FR
8	Boko Haram *Allied with Al Qaeda	2003	2013	UK/FR
9	Forsane Alizza (Forsan al-Izza)	2010	2012	FR
10	Harakat-ul-Mujahideen (Harakut ul Ansar)**	1985	2005	UK
11	Hizb ut Tahrir	1952	Legal	UK/FR
12	Islam4UK	2008	2010	UK
13	Islamic Path	unknown	2010	UK
14	Izhar Ud-Deen-il-Haq	2011	Legal	UK
15	Jabhat-al-Nusra	2012	2014	FR
16	Jaish-e-Mohammed **	2000	2001	UK
17	Jama'at-ud-Da'wa *al-Qaeda sympathisers/aids	1985	2009	UK
18	Lashkar-e-Taiba (Tayyaba) *al-Qaeda sympathisers/aids	1990	2001	UK/FR
19	Libyan Islamic Fighting Group	1995	2005	UK
20	London School of Sharia	unknown	2010	UK
21	Minbar Ansar Deen: aka Ansar al-Sharia	2011	2013	UK/FR
22	Mouvement Pour L'Unicité et le Jihad en Afrique de L'Ouest (MUJAO) aka Mourabitounes or al-Murabitun	2011	2012	FR
23	Muslims Against Crusades (MAC)	2010	2011	UK
24	Need4Khilafah	2013	Legal	UK
25	Salafi Media	2009	Legal	UK
26	Salafi Youth Movement	2008	Legal	UK
27	Salafist Group for Preaching & Combat/Call & Combat / Le Groupe Salafiste pour la Predication et le Combat	1998	2001	UK/FR
28	Saviour/Saved Sect	2005	2006	UK
29	Sharia4UK	2007	Legal	UK
30	Supporters of Shariah	1994	Legal	UK

The colour coding within the above table shows affiliation, coalitions or direct relations between various groups. Groups highlighted in Yellow are all manifestations of the same group, al-Muhajiroun, which has changed names and taken on various facades over the years. Groups highlighted in Red are affiliates, allies or splinter groups of al-Qaeda. The two groups highlighted in Blue depict the fact that Jaish-e-Mohammed is a rival splinter to Harakat- ul-Mujahideen.
***While most agree al-Qaeda was founded in 1988 the organisation did not fully develop itself until 1996.**
****Jama'at-ud-Da'wa is the political arm of Lashkar-e-Taiba. They coordinate with Jaish-e-Mohammed.**

Besides their activism in the UK and France, the Islamist extremist groups listed in Table 2.1 are also chosen because they engage in a broad spectrum of online activism. Some organisations have barely any online presence readily available in French and English despite having French or British bases, such as al-Ghurabaa, Call to Submission or Islamic Path. Other organisations are highly active on one or two social networking outlets, such as Islam4UK's YouTube presence or al-Shabaab's Twitter usage. Lastly, some organisations have multi-faceted online platforms utilising all platforms available to them, such as al-Muhajiroun and its splinter networks.

Most groups listed are either affiliates or subsets of al-Qaeda or al-Muhajiroun. These connections primarily manifest in two ways; firstly, affiliation is often based on a smaller Islamist group gaining assistance or assisting a larger organisation in order to gain resources (physically or strategically) as well as notoriety. This often involves having individuals from one organisation assist in the management of an operation for the other organisation. It can also include one organisation providing aid, by way of shelter or giving arms, to another organisation. This is the case with most groups affiliated or linked to al-Qaeda.

Secondly, there is a trend in recent years of Islamist groups rebranding, renaming and repositioning themselves once they have received negative public attention or proscription. Name changing allows the group to maintain its activism, at least for a short while and, potentially, reach a wider audience. This name changing and rebranding is exemplified by the al-Muhajiroun (AM) network, which has worked under a myriad of different labels and organisational names. Rebranding and renaming allows an organisation to avoid legal repercussions and circumnavigate around proscription, thus highlighting the futility of banning content found under a specific organisation's name.

A Case Study on al-Muhajiroun (AM)

In mapping the nature of Islamist groups and their usage of online tools, AM offers an illustrative case study on how extremist organisations not only utilise the Internet but react to negative government measures by creating a myriad of online profiles under different names. AM is an Islamist organisation founded in 1996 by Omar Bakri Mohammed, a radical Islamist cleric, who moved to England after being expelled from Saudi Arabia. AM's political stance is based on an Islamist worldview, which centres on the aim of establishing the

caliphate as a global empire. AM has been highly successful in proliferating the organisation's efforts through its various online platforms as well as turning online activism into offline action.

The organisation also has a long history of promoting anti-Semitism, espoused by leaders and disseminated through posters, leaflets and online propaganda. They have targeted other faiths, such as Hinduism and Sikhism, as well as publicly promoted homophobia and the subjugation of women. Offline, AM has been successful in creating street protests and defending domestic and international terrorist efforts. Several of the organisation's activists have been convicted of terrorist activities,[24] including involvement in the following plots:

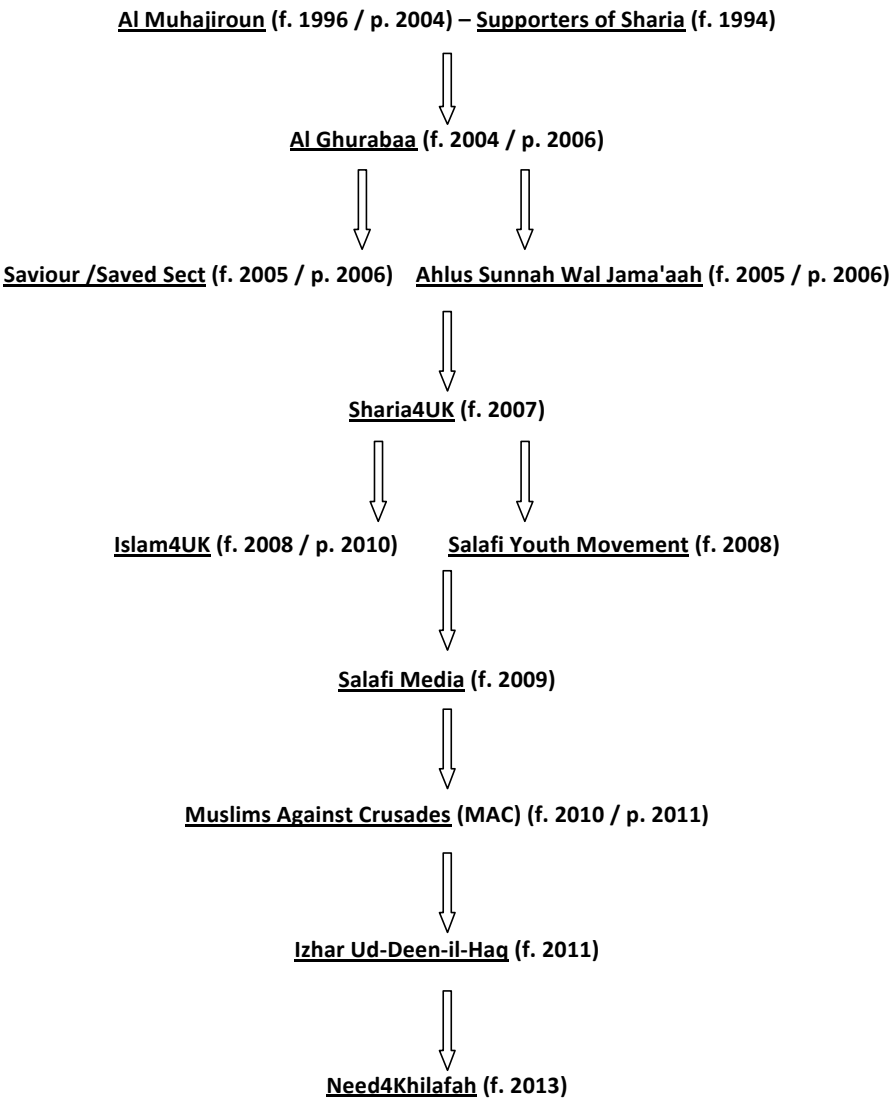
- **The Territorial Army Bomb Plotters** (2013 - all four plotters, convicted of bomb plots at a TA centre, were known AM followers),
- **The Royal Wootton Bassett Bomb Plot** (2012 - AM activist Richard Dart was one of the plotters),
- **The London Stock Exchange Bomb Plot** (2011 - all four plotters had AM links through its linked groups al-Ghurabaa, Islam4UK and Muslims Against Crusades),
- **7/7 Bombings** (2005 - Mohammad Sidique Khan, the leader of the group was linked with AM and used AM's safe houses to prepare for the bombings),
- **The Fertiliser Bomb Plot** (2004 - four of five convicted in the plot had AM ties)
- **Mike's Place Suicide Bombing** (2003 - second bomber, British Omar Khan Sharif, whose explosive device had a technical failure, had been leafleting for AM in Derby two weeks prior to flying to Tel Aviv),
- **Bilal Mohammad** is Britain's first potential suicide bomber who was involved in a plot in 2000. He admitted that AM was sending British fighters to Kashmir and that he was one of their recruits.
- **Amer Mirza** was the first AM supporter convicted of Islamist-related terrorism in March 1999 for petrol-bombing a West London Territorial Army base protesting against US bombs in Iraq.

In 2003, AM gained widespread media attention for advertising a public conference called 'The Magnificent 19', celebrating the second anniversary of 9/11. Following AM's numerous controversial actions, the British government proscribed the organisation in 2004 under newly instated anti-terrorism laws. Rather than stifling the organisation's activities AM has re-emerged numerous times under difference aliases, largely promoting itself and

[24] The organisation Hope Not Hate gave a detailed account of al-Muhajiroun's networks and social foundations in their report: Lowes, Nick & Mulhall, Joe (2013) *Gateway to Terror: Anjem Choudary and the al-Muhajiroun Network*, Hope Not Hate.

disseminating information through the Internet. Figure 2.1 gives a flow chart of AM splinter groups that have developed as the government has proscribed its groups and websites. While some have been noted and proscribed under UK Terrorism Acts, others remain legal due to the government's lack of clear evidence as a basis for proscribing.

Figure 2.1 Al Muhajiroun's Various Splinter Groups Online



Each AM splinter group listed in Figure 2.1 shows when the renamed group was founded (f.) and when/if they were officially proscribed in the UK (p.). Other AM-related groups have also appeared but have not been added to this chart because they have had a very short-lived online existence or unknown start date. These organisational subsets, including Call to Submission, Islamic Path and the London School of Sharia, were proscribed in the UK as of 2010/2011. The morphing and splintering of the AM network highlights the futility of traditional legal mechanisms to fight and/or censor extremism. Each time a new AM group has been set up they have established new websites, online networks and Internet profiles through various social networking outlets in order to give the new group name legitimacy and a valid online presence.

2.2 Mapping Online Extremism

Rather than strictly analysing the online habits of subscribed followers or dedicated members of Islamist groups, this report primarily targets pathways leading individuals to radical Islamist ideologies via the Internet. By observing online trends, it is clear that Islamist groups and their supporters are increasingly providing English and French language news feeds and commentary to inform people about their causes. Therefore, we need to ask two questions:

- For those who have little or no direct exposure to Islamist groups and ideologies, what online materials and Islamist narratives are easily available?
- How do individuals intrigued by the extremist narrative interact within online extremist platforms?

There is a distinct difference between passive and active Internet usage. *Passive* Internet platforms are non-interactive online content spaces, such as static websites or videos, where material is available purely for consumption with no interpersonal interaction. *Active* Internet platforms are social spaces where individuals can comment, discuss or chat about ideologies or specific subject matters. Active platforms include social media tools such as Twitter and Facebook, as well as chat rooms and forums.

This section discusses the primary online tools being utilised by Islamist and jihadist networks. It begins by exploring how individuals searching for extremist content through popular search engines would struggle to stumble across extremist websites or forums. This section then goes on to analyse five key Internet spaces that extremists use. These include: websites, chat rooms, YouTube, Facebook and Twitter.

Using Search Engines to Find Extremist Content

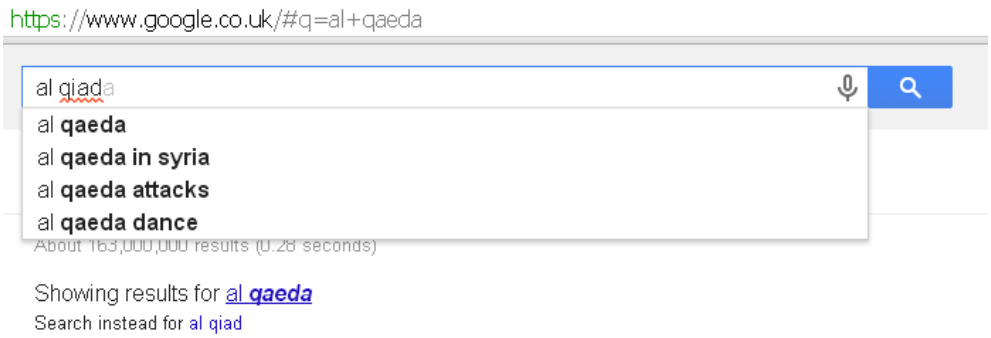
Search engines have complex algorithms that provide responses to online queries by siphoning results from thousands, sometimes millions, of related web pages. Algorithms are the calculated computer processes that take an online search question and provide suitable answers or results. Search engines like Google and Bing rely on more than 200 unique signals in order to guess what an online user might really be searching for in order to refine their results.[25]

In order to assess the ease with which individuals can come across extremist narratives while searching the Internet, research was carried out on a number of key Islamist extremist-related terms. Most searches for information in English and French use one of the following search engines: Google, Bing, Yahoo, Ask.com, AOL with Google and Bing collectively being used for over 94% of all searches.[26] With this in mind, key search terms were entered into Google and Bing's search engines and the primary search results were analysed and compared with search term results from Bing.

In testing the likelihood of individuals coming across extremist content by searching certain Islamist and jihadist-linked terms we first cleared our Internet user history so that there were as few biases or pre-existing filter settings on our search engine usage as possible.[27] We chose three key Islamist extremism related terms that individuals might enter into a search engine in order to analyse top search results, recommended terms and linked adverts.[28] The three terms we chose to analyse were: 1) **jihad**, 2) **Mujahideen** and 3) **al-**

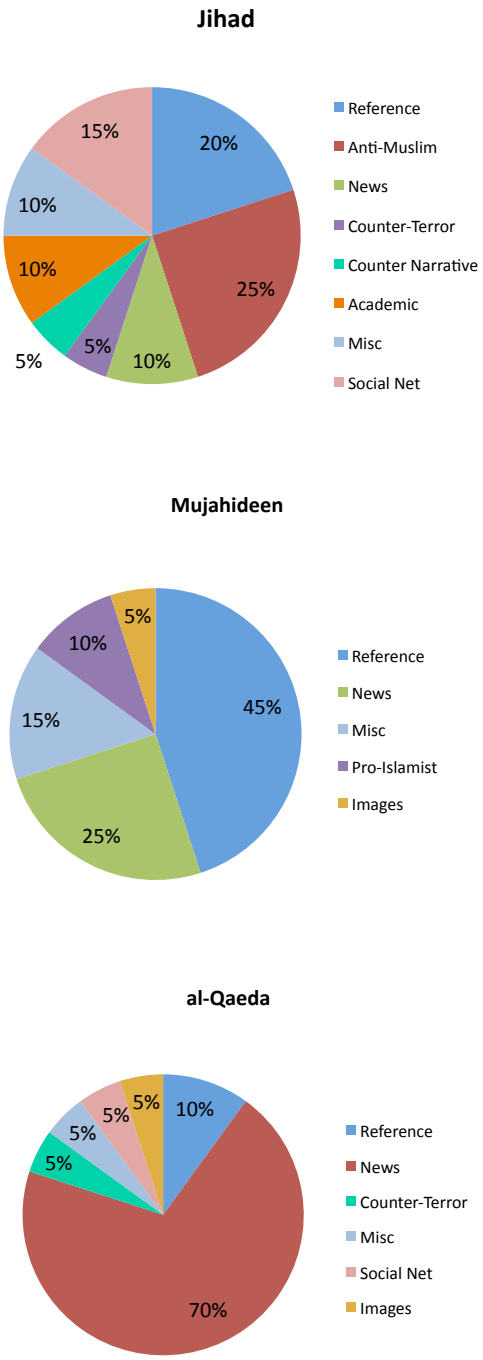
[25] 'Algorithms', *Google Inside Search: How Search Works*, www.google.com/insidesearch/howsearchworks/, [Accessed: March 2014]
[26] Chris, Alex, (2012), 'Top 10 Search Engines in the World', *ReliableSoft.net*.
[27] To clear pre-existing search filters we cleared the browsing data and download history, deleted cookies and site plug-ins, emptied the online cache and cleared auto fill formatting.
[28] Note: Terms were searched 1-3 February 2014. The quantity of results, top terms and top links are constantly changing due to current affairs, news media and other influencing factors affecting searches.

Qaeda. These terms are widely known to the greater public, even if only vaguely, through media and public discourse. Although the term 'al-Qaeda' has many different spellings it was searched under this spelling since this is the top suggested spelling through search engines even if another spelling is typed in initially, as seen in the image below.



For each term we looked at **suggested search** terms brought up by Google and Bing, **related searches** listed in relation to the term and the **top search results**, listed in the first three pages only. The search results displayed for this study were conducted in the UK, which had some effect on the outcome. However, the French search engine counterparts (<Google.fr> and <bing.com/?cc=fr>) were also consulted to ensure there were not large disparities in results. The three pie charts in Figure 2.2 track the nature of the top search results for the three terms. The images given show the results that Google produced. These were largely similar to the results found using Bing except that the results for 'jihad' produced a much higher frequency of links to reference material sites (60%) with a much lower result in other categories (between 5% and 10%).

Figure 2.2 Tracking Top Search Results for Radicalised Terms



The search results, seen in Figure 2.2, can be broken down into ten main categories:

1) **Reference Links** such as Wikipedia, dictionaries, encyclopaedias or historical material.
2) **News Sites** linked to a collection of stories around a term or single current affairs articles.
3) **Counter-Terrorist Sites** of content tracking, monitoring or exploiting terrorists/terrorism.
4) **Anti-Muslim Sites** with content implying Islam or Muslim communities are linked directly to terrorism and/or that Muslims inherently possess traits that are dangerous to society.
5) **Social Networking Pages** linked to Twitter, YouTube or Facebook accounts.
6) **Academic or Learning Sites** either of academic writings and research or educational sites.
7) **Pro-Islamist Extremist Sites** providing content supporting Islamist extremist narratives.
8) **Counterspeech Sites** giving content supporting moderate Muslims against extremism.
9) **Images** when there are a number of images relating to a term, a link to images is given.
10) **Miscellaneous Links** to books, movies, bands or other indirect links to the term.

As illustrated in Figure 2.2 there is a great deal of variation between the search results produced by the three terms. While the term al-Qaeda produced a high number of news and media reports in the top results, the term jihad only had two news links in its top results. The high level of variation is, of course, dependent on the factors discussed previously, however, it can be used to highlight two important points concerning Islamist-related search results.

Firstly, both pro-Islamist results and counter-Islamist narratives were lacking. This implies random searches by curious individuals are unlikely to lead to extremist content. In the top search results of the three terms, pro-Islamist sites or links only came up twice, both in relation to ‘Mujahideen’. This, at least in part, goes against theories claiming that individuals with no prior engagement or knowledge of extremist groups can find extremist content and thus be taken in by it.

Secondly, whilst the lack of extremist links in early searches is somewhat comforting, the lack of counter-narratives providing moderate views against extremism is equally worrisome. Only one site promoting moderate Muslims against extremism came up in relation to jihad, <myjihad.org>. Moderate engagement online is crucial and is currently lacking both in passive and active Internet usages. This is discussed further in Chapter 4.

Table 2.2 below shows the 'autocomplete' and related results given for the three terms.[29] If the results came up in *only* Google or Bing the name of the search engine is listed.

Table 2.2 Autocomplete and Related Searches

Jihad		Mujahideen		al-Qaeda	
Autocomplete	**Related**	**Autocomplete**	**Related**	**Autocomplete**	**Related**
jihad Watch	celebrity jihad (Google)	Mujahideen Taliban	Mujahideen jihad (Google)	al-Qaeda attacks (Google)	al-Qaeda official website (Google)
jihadist	jihad holy war (Google)	Mujahideen Bosnia (Google)	Mujahideen definition (Google)	al-Qaeda dance (Google)	al-Qaeda beheading (Google)
jihadology	islamic jihad	Mujahideen quotes (Google)	Mujahideen Taliban (Google)	al-Qaeda in Iraq (Google)	What does al-Qaeda mean?
jihadwatch.org (Bing)	jihad definition	Mujahideen poisons handbook (Bing)	Mujahideen video (Google)	al-Qaeda twitter (Google)	al-Qaeda attacks
Jihad in Islam	jihad lyrics (Google)	Mujahideen explosives handbook (Bing)	Mujahideen explosives handbook (Google)	al-Qaeda beheading (Google)	al-Qaeda website
jihad watch Robert Spencer (Bing)	jihad website	Mujahideen tarana (Bing)	Mujahideen news (Google)	al-Qaeda flag (Google)	al-Qaeda videos
jihadism	artistic jihad (Google)	Mujahideen wiki (Bing)	Mujahideen flag (Google)	al-Qaeda song (Google)	Osama bin Laden
	jihad terrorism (Bing)	Mujahideen in Algeria (Bing)	Harakut Ul Mujahideen (Bing)	al-Qaeda meaning	al-Qaeda meaning
	Jihad videos (Bing)	Mujahideen t55 (Bing)	Ansar Al Mujahideen (Bing)	al-Qaeda website (Bing)	Saddam Hussein (Bing)
	Jihad Seekers Allowance (Bing)		Al-Shabaab Mujahideen (Bing)	al-Qaeda training manual (Bing)	Taliban (Bing)
			Indian Mujahideen (Bing)	al-Qaeda in Europe (Bing)	
			Mujahideen Poisons Handbook (Bing)	al-Qaeda ideology (Bing)	
				al-Qaeda videos (Bing)	

[29] Autocomplete is the software function that completes words, or strings of words, without the user needing to type them in full. This function is based on what has been typed or input before by a user. Related search results are shown at the bottom of a search result page using Google, or at the right-hand side of the page using Bing.

As seen from Table 2.2, while some autocomplete suggested terms and related terms are neutral, or even farcical, others have more explicitly extremist intentions that lead to a more directed search looking for pro-Islamist extremist pathways online. These pathways can lead to beheading videos or various training handbooks and possibly even official websites.

Interestingly, similar trends were also found when searching the same terms in French on <Google.fr> and <bing.com/?cc=fr>. Although terms are slightly different (djihad and al-qaida in French) there are no significant differences in the results. The only noticeable difference was the higher quantity of miscellaneous material appearing in searches for the term 'djihad'.

Official Websites

For individuals doing online searches for websites attached to particular Islamist organisations there are two current trends. Firstly, the majority of Islamist groups that have controversial and/or violent histories tend to have websites that have been taken down or blocked. For websites that have been taken down, website data and traffic information is no longer accessible or reliable. The majority of Islamist groups looked at for this research did not have readily available British or French websites for online users. Secondly, for the groups that do have readily available websites, Islamist narratives are presented in a subtle manner and only by further exploration into a website are more hard-line and extremist views found.

Websites available in English or French that support extreme Islamist organisations are mainly information-giving sites that teach about Islam in a very specific way, paving the way for certain narratives. These narratives are subsequently activated with links to YouTube videos (mainly lectures either in English or French or provided with subtitles) or various other social networking platforms in which discussions with like-minded individuals take place. The static portions of Islamist extremist websites serve mainly as educational platforms, which solidify preconceived notions about Islam, whereas the active outlets available within the site delve further into extremist narratives. In most cases, access to a site's various extra functions, such as photo sharing, podcasts, blogs and chat rooms,

requires registration with the site's administrators, who often ask for personal details (seen in Example Box 2.1, 2.2 and 2.3 in the following pages).

Example Boxes 2.1 – 2.3 depict a range of open access Islamist websites and an analysis of their overall presentation, content, functionality and successfulness in attracting visitors. Example Box 2.1 examines how weakly constructed sites attract very little traffic. Example Box 2.2 focuses on how strong sites can still fail to attract significant traffic if they are not maintained properly. Lastly, Example Box 2.3 explores a strong site with consistently high levels of visitor traffic and analyses how this is produced and maintained.

Site traffic was measured using available analytic monitoring systems such as Alexa.com. While analytic monitoring sites do not give exact figures of sites they do provide general traffic ranking and analysis. Thus, we categorised sites based on low traffic (virtually no visitors or below general ranking sites) and high traffic, ranked within analytic monitoring sites and receiving a consistent and high volume of visitor traffic.

Sites like Ansar al-Haqq, explored in Example Box 2.3, produce articles that contain simple tips on how to be a good Muslim under an ultra-austere interpretation of Islam. Furthermore, the site imbeds more extremist ideologies through linked articles, videos, audios or through their chat forum. By creating a forum, the site allows for communication of a more extremist nature between adherents while also warning users to not implicate themselves by using certain terms or references.

Example Box 2.1 Weak Sites - Weak Impact
Supporters of Shariah (SOS) Website <http://www.angelfire.com/bc3/johnsonuk/eng/home.html>

The website of SOS is quite rudimentary, stating at the top of the webpage that the site is temporary. The site was developed in 1999 and lacks a modern look. However, this site is the first result that appears when 'Supporters of Shariah' is searched on Google and no other updated site for SOS comes up in the top search results.

The site is openly Islamist and anti-USA and UK. On the main page under Our Aim the site states: 'Muslims and non-Muslims are being oppressed throughout the world. SOS is one of the organisations struggling to remove the oppression created by man-made laws. So that the whole of mankind can enjoy the freedom, purity and justice of living under Allah's laws – The Shariah.'
The site is directly linked to the now incarcerated, Sheikh Abu-Hamza from when he used to run the Finsbury Park Mosque, listing his email, a general phone number and address for contact.

The Above Image is from the homepage of the website with numerous Islamist symbols interjected along with the depiction of martyrs and results of western brutality.

Similar to the site listed in Example Box 2.2, there are multiple links and facets embedded within the website, including audio files of Friday Khutbas in English or Arabic, downloadable catalogues (no longer available), links to other Islamist Shariah supporting sites (many of which have been taken down) and a link on 'How to Become A Muslim'.

Linking with Other Sites: The webpage has various links to other pages, most of which have been shut down or blocked. Examples include <www.shareeah.com>, a link to join a campaign against Israel and America's foreign policy at <www.stopamerica.org/>, and a link to <www.casi.co.uk> for the Campaign Against Sanctions in Iraq against the US, UK and Saudi efforts, all of which have been taken down.

Weaknesses: Despite the easily searchable nature of the site and its various online functions, the format and lack of updated materials means the site receives very little to no traffic. The most recent materials posted on the site were articles on the police raids of the Finsbury Park Mosque in 2003. While SOS had an impact on the Islamist scene in London this was based more on real-world interactions, rather than Internet-based activity.

Sometimes websites are also presented in the form of blogs, which allows for a more interactive and informal environment for information distribution. For the most part, static websites in English and French do not have publicly, or openly, accessible content that might be considered libellous, illegal or insightful. However, sites can easily imbed extremist

narratives in open content, while a myriad of further options are available in a website's private capacity to registered members. This can be seen in both Example Box 2.2 and 2.3.

Example Box 2.2 Strong Sites - Weak Impact
Minbar Ansar-ul-Deen Website/Blog <http://minbaransardeen.wordpress.com/>

The Minbar Ansar-ul-Deen website is an illustrative example of a strong English language Islamist website with poor traffic and impact. It is the top website to appear in a Google search for the proscribed group. It would also appear attractive to younger audiences with its style, format and accessibility. It has clear web browsing options in good English without external advertisements, and is a tech-savvy site with video, audio and chat capacities.

The homepage of the site states that 'in light of the unjust wars waged against the Muslim Ummah in various lands, Minbar Ansar intends to expose the (Foreign Policy) atrocities, double standards and deceptions being committed by the West as led by America and her puppets in the East.'

Martyrdom: The Ansar-ul-Deen website is a good representation of using the Internet to 1) teach about Islam through an Islamist narrative of domination and oppression, and 2) to solidify narratives of martyrdom justifying extremist actions against non-Muslim entities. There is a separate page dedicated to Muslim Prisoners that presents testimonials and videos of imprisoned 'martyred' Muslims.

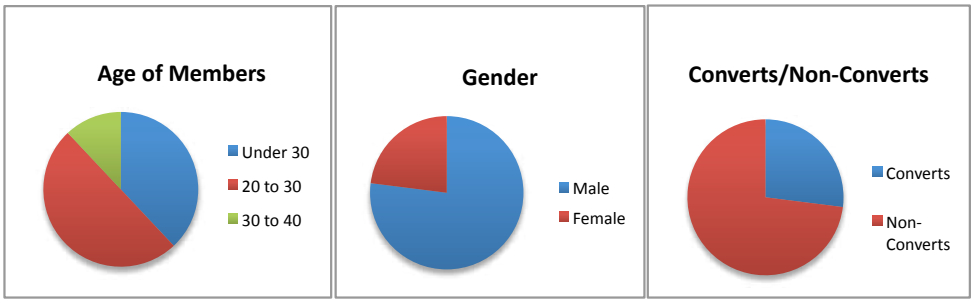
AUDIO FILES	154	109 Biography/History of Islam
		6 Beliefs and Knowledge
		7 Current Affairs
		32 Islamic Domination
VIDEO FILES	51	10 Songs
		36 General Pro Islam/Anti West
		5 Muslim Prisoners

Weaknesses: While the blog seems to fit a niche for 'at risk youths' the site also exploits the difficulty that many UK-based Islamist websites face. Despite being attractive, accessible and interactive, the site does not receive much traffic. The site is not traceable on general analytic trackers due to its low usage. The site also seems to have peaked between its creation in September 2011 and January 2012, during which all its content was created or uploaded. Subsequently, many audio files no longer connect due to blocking or content erasure. This exemplifies a site's dependency on the activism of the site creator and the ability of the site and its supporters to network.

Example Box 2.3 Strong Sites - Strong Impact
Ansar al-Haqq Website <ansar-alhaqq.net>

The French-based Ansar al-Haqq website has drawn much attention towards the original Yemeni group of the same name. Currently, Ansar al-Haqq is considered 'the face of French jihadism' by the French press. The website is one of the only Salafist and jihadist propaganda websites in French and, since its inception in 2010 it has been viewed by over 1.5 million visitors with an average of 1,000 daily visits.[30] While the content is mainly subtle the jihadist support is clear from the sites main page iconography, showing the black and white *al-raya* flag favoured by jihadists.

The site is particularly successful in attracting young women trying to join al-Qaeda, offering a closed section to 'sisters' who obtain access to the female-only forum by applying to the site administrators. The site also has a high level of youth and Muslim convert support as seen by research done tracking details on Ansar al-Haqq website members:[31]



The site's subtlety is partly due to the French laws around *Laïcité* (secularist legislation) which prohibit openly extreme religious values to the public. However, upon closer inspection the site includes pro-jihadist articles, such as al-Awlaki's article '44 ways to support jihad'[32] and advises true followers to go abroad in order to learn how to handle weapons and discusses the benefits of dying a martyr.

Keeping the Site Legal: In 2010, 2012 and again in September 2013 site administrators and regular visitors were arrested for 'apology' and 'provocation' of terrorism on the Internet. The site's forum temporarily ceased to be available to users after the arrests in 2012, although the site itself remained active. Subsequently, the forum has been re-established but now requires registration to participate in discourse. The site remains active because French authorities feel these sites provide huge amounts of data and information that would be lost if the sites were shut down.

Passive-Active Websites: The success of the site is not only down to its constant maintenance and upkeep but also because it incorporates other active and interactive tools. The Ansar al-Haqq site leads to other multi-media outlets, including a forum. The forum contains both private and public conversations with a myriad of topics and posts. The site also links with other French Islamist sites and offers audio courses, articles on jihadism and ideological discussions.

[30] Duportail, Judith (2013) 'Ansar Al-Haqq, le visage du djihadisme à la française', *Le Figaro*, 1 October.
[31] Data for pie charts from: 'Ansar al-Haqq, le forum islamiste française fermé suite à l'arrestation de 12 suspects', *La Libellule*, (11 October 2013).
[32] Al-Awlaki, Anwar (2009) '44 ways to support jihad', January.

The accessible websites that are linked to Islamist extremist organisations vary in content and format; however, these sites frequently have three primary purposes.[33] The first is to propagate the Islamist narrative through a selective and de-contextualised reading of scripture. This involves promoting a 'saved sect' concept that depicts followers of Islamist ideologies as being the only ones who are rightly guided with all others doomed. Therefore, re-education is needed and can be given in the static main pages of a website or linked videos.

The second theme that is most common among such extremist websites is the promotion of martyrdom. This is developed through the concept of *taghut*, or 'idolatry', which condemns man-made laws that are thought to go against the Shariah. Martyrs are made of individuals fighting against the imposition of these laws or individuals facilitating them. Some Islamist websites also provide biographies of 'martyrs' and multiple British Islamist sites link to <muslimprisoners.com>, which offers complete biographies and pictures of Muslim prisoners detained in various countries. Martyrdom is used to solidify adherence to Islamist organisational efforts and potentially promote extreme and illegal acts against non-Muslims.

The third purpose of these sites is to solidify an allegiance to Muslims and a rejection of non-Muslims (*al-wala'wal bara'*). Both propagating extremist narratives and promoting martyrdom can facilitate this allegiance-building. Developing the self-other narrative of 'us versus them' is key to forwarding the Islamist extremist goals of the organisations in question.

While stagnant and active Internet usages were discussed at the start of this chapter, it is becoming increasingly difficult to separate one function from the other. As seen in Example Boxes 2.1 – 2.3, static websites have the ability to imbed active social networking functions within a site. This takes place primarily in the form of adding chat room and discussion forum functions. Websites are also linking to Facebook and Twitter accounts and vice versa to drive traffic.

[33] See also: Musawi, Mohammed (2010) 'Cheering for Osama: How Jihadists use Internet Discussion Forums', *Quilliam*: London.

Chat Rooms & Discussion Forums

Chat rooms and forums were widely used by Islamist extremist groups and their supporters in the mid-2000s. While they continue to be a platform for discussion between like-minded extremists, there is increased reticence to use open forums for controversial discussions. Islamist and jihadist forums are suspected of having yielded terrorist-related leads that have led to many al-Qaeda arrests and subsequently, many chat rooms and forum platforms directly linked to Islamist organisations have been proscribed, discontinued or shut down.[34] Forums based in Saudi Arabia in particular have encountered specialist cells fighting cyber-jihadism, which led to arrests of webmasters and moderators in the late 2000s.[35]

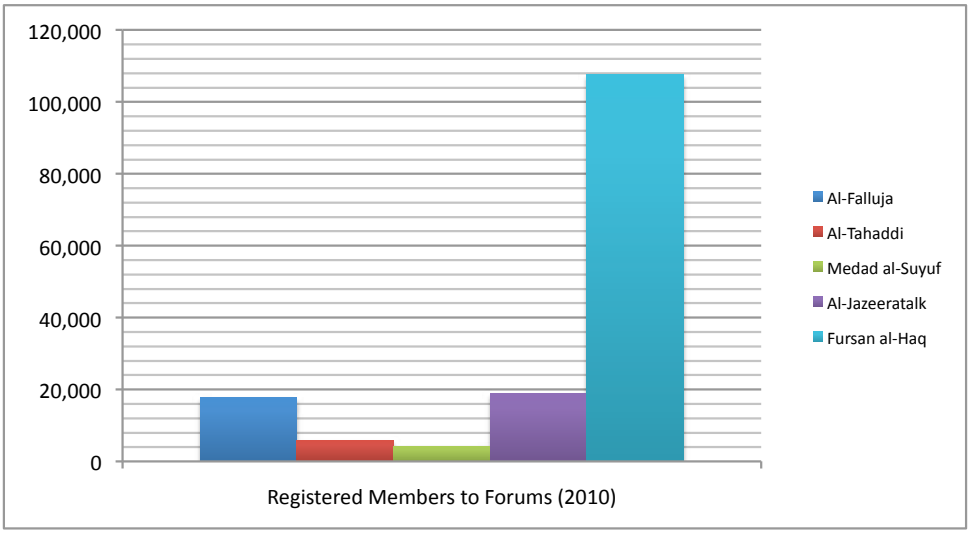
While some of these chat sites reopened, they were later treated with caution. Users now suspect that security services might be luring jihadist supporters back to collect additional personal information. In response, many forums have introduced new ways of showing and testing for authenticity, which have, in turn, created new dissemination channels for specific jihadist organisations. Such authenticity measures act as a seal of approval to officialise content. Another backlash to forum-based arrests has been the usage of non-jihadist forums devoted to regional or tribal folklore, which are now used for discussions and information dissemination along with measures to illustrate authenticity.

Islamist forums and chat rooms in English and French are still widely available, but, as mentioned, a large portion of more extremist Islamist discourse now takes place within the dark web where membership, passwords or authentication are required. Private virtual spaces are not readily indexed. In other words, they cannot be located by basic search engines and would take pre-existing knowledge to find.

[34] Alonso, Pierre (2012) 'Twitter: The New Frontline in Global Cyber-Jihad', *OWNI.eu*, 10 January.
[35] Ibid.

Example Box 2.4 Al-Fajr Media Center

The key jihadist online discussions still take place in Arabic, but serve to exemplify the usage of forums in both public and dark web contexts. Al-Fajr Media Center is a core Arabic jihadist forum that operates as the non-official media distributor and online logistical network for al-Qaeda. Approval and distribution of content through al-Fajr Media Center acts as a form of accreditation from al-Qaeda, allowing other jihadist networks to accept the authenticity of propaganda being distributed through the site. Since core forums are not 'owned' by jihadist organisations, material distributed through them cannot be labelled as 'al-Qaeda content'. A number of jihadist forums have been endorsed by al-Fajr Media Center such as: Al-Falluja, Shumukh al-Islam, Al-Tahaddi, Al-Mujahidin, Medad al-Suyuf. All of these discussion forum outlets discuss a variety of topics and have a range of registered members:[36]



Forum Hijacking

Al-Fajr Media Center has also been a key element in the jihadist hijacking of previously non-jihadist web forums. Fursan al-Haq had previously been a religious Wahhabi discussion forum consisting primarily of Egyptian Wahhabis while Al-Jazeeratalk had previously been a general news and views discussion forum attached to Al-Jazeera Media. Large jihadist constituencies infiltrated both sites after these websites were promoted through al-Fajr Media Center networks. The infiltration of non-Islamist, mainstream Muslim forums by extremists is used to reach a wider audience. As seen by the figure showing the registered members to forums, Muslim-based forums sometimes hold large numbers of registered users. Islamist and jihadist supporters bring their own narratives and debates to these forums seeking to re-educate and cultivate support for their cause. Subsequently, Al-Jazeeratalk temporarily shut down and reconfigured itself to restore its previously neutral nature.

The influential capabilities of a core forum, or content distributor, are highly dependent on whether or not jihadist media organisations approve of the forum. Becoming a non-official distributor of al-Qaeda propaganda, for example, means that accreditation from al-Fajr

[36] Data for the figure in Example Box 2.4 comes from: Musawi, Mohammed (2010) 'Cheering for Osama: How Jihadists use Internet Discussion Forums', *Quilliam*: London.

Media Center gives authenticity to materials distributed through them. Example Box 2.4 displays how jihadist forums distribute materials and formulate ways to validate and authenticate which forums can be trusted or used for their purposes.

However, with regards to the potential for young target audiences being radicalised, it is worth emphasising that prior knowledge would be needed to find most open access Islamist and jihadist chat rooms, as exemplified in the prior discussion about search engines. Succesful Islamist websites also tend to provide users with their own chat rooms and forum spaces, usually available through subscription or site membership, as seen in Example Box 2.2 and 2.3. Pathways leading to extremist chat rooms can also be found on social media accounts of extremist groups or supporters of such groups. Hence, with the increasing reliance on social media for information, younger audiences are more likely to arrive at extremist chat rooms through social media rather than traditional websites.

The multi-faceted nature of online platforms today suggests that chats can be embedded within most Internet-based mediums. This is where the majority of 'at risk youth' would be likely to organically come across Islamist narratives without previous exposure. Many social media platforms allow for users to post comments, which, dependent on the post or video, can become a space for extremist dialogue in which supporters of extremism can interact with other users.

However, real-time chats can also be embedded in chat room spaces that are not ostensibly jihadist, although prior knowledge and timing arrangements would need to be known for real-time participation. The usage of real-time chats and forums require a greater degree of subscription within an online group or organisation to arrange a conversation. It is challenging to find forums or chat rooms that link with particular Islamist organisations for individuals casually trawling the Internet.

There are very few official open-access forums directly relating to extremist organisations. When searching for al-Qaeda-linked forums and chat rooms in popular search engines a vast majority of results were encrypted or closed-access spaces. Open chats and discussion forums can be found through proxy sites. One example of this would be using sites like <godlikeproductions.com> to create a topical discussion around an extremism-related

subject matter or organisation to draw in commentary. Chats are used to produce real-time conversation or instruction.

Numerous open chat rooms that belong to neutral and non-extremist websites also have the potential to develop debates over whether or not a contentious organisation is reliable. Example box 2.5 below shows a thread started by a forum user asking about UK-based Islamist groups:

Example Box 2.5 Conversation on <ummah.com/forum>

Thread Heading: What's your opinion on al-Muhajirun and Supporter of Shariah?

Soulja Guests: I don't live in the UK so I don't know much about them. I support HAMAS, and Ikhwan al-Muslimeen and the Chechen Mujahideen, etc. yet when I went on the al-Muhajirun website I really wasn't impressed with what I saw at all. I did like the Supporters of Shariah articles and Abu Hamza al-Masri.
Can anyone give more information on these groups? From the viewpoint of Ahlul Sunnah wa Jama'ah.
Allah (SWT) knows best.
Peace be upon those who follow guidance.
Ameen.
Jazakallah wa Khayrun.

Brother_Daniel: I love Shaykh Abu Hamza and the brothers at Ansaar al-Shareeah.I have e-mailed questions to them and they are very good in giving answers promotly. As for al-Muhajiroun, my issue with them is they are a little on the takfeeri side sometimes.

Soulja Guests: Exactly what I was thinking.
But you know one thing about both Abu Hamza and Omar Bakri, where were they educated? Do they have ijazas in Islamic law? Do they have knowledge of fiqh, tazakiya nafs, etc.?
All I see from them is politics, like even in the Khutba I heard of Abu Hamza. I didn't hear one Qur'an ayah or one hadith - if my memory serves me correct - on the latest Abu Hamza khutba.
Jazakallah wa Khayrun

Brother_Daniel: I know that Omar Bakri studied in Syria and Saudi Arabia, I'm not sure about Abu Hamza. And yes they do talk alot about current events and the implications they have for the Muslims both in the Middle east and in the West. But they also do talk alot about other Islamic issues. They promote the correct aqeedah and stuff like this. A purely political organization would be Hizb ut-Tahrir (I know I used to be big on their stuff).

Khuzamah: I've never heard of "Supporters of Shariah"....
as for Al Muhajiroon, if I tell u my view on them, it might be classed as backbiting... 

The thread above is an excerpt from a conversation that took place on the Ummah.com forum. It is a prime example of how answers to questions are sought, and the fact that it takes place within a popular, neutral and open forum allows for alternative narratives to arise. After the comment by Khuzamah an array of questions and discussions about the various groups' legality and motives is sparked, offering both positive and negative views about AM and Supporters of Shariah.

While chat rooms and forums have been used for networking, instruction giving and real-time planning, this has very little impact on the process of radicalisation and is more important in maintaining ideological links with like-minded individuals. Due to this, openly extremist individuals offering their narratives can easily infiltrate forums, providing alternative views and opinions on Islamist groups. However, as seen in Example Box 2.5, if forums are left open it is also possible for participants with a positive message to interject and challenge extremist narratives.

Facebook

Today Facebook is used by over 1.28 billion people around the world. With regards to Islamist radicalisation processes on Facebook, some of the larger Islamist extremist groups are quite sceptical and openly anti-Facebook. Al-Muhajiroun, for example, is openly against using Facebook as a source of networking and distributing information. The main cause of scepticism is the ease with which Facebook can identify users and link people to one another. Facebook has inbuilt facial recognition technology, so that photos that are uploaded are scanned for recognition automatically, linking individuals with others in specific times and places. With extremists preferring to operate with a degree of anonymity and covertness, Facebook tends to act more as a decentralised hub for information distribution or a means of showing support. The Facebook groups that can be found, written in English or French, tend to be created by young sympathisers for the most part, with activists taking it upon themselves to post regularly, linking sympathetic, martyr-based or educational videos to the Facebook wall.

While some Islamist organisations have virtually no presence on Facebook, i.e. al-Ghurabaa, al-Muhajiroun, Call to Submission, Islam4UK, Muslims Against Crusades, others have multiple Facebook profiles in various forms. These Facebook profiles were created by sympathising individuals with or without the central permission or support of organisation leaders or members. The decentralisation of Islamist networks on Facebook means that numerous groups, individuals and/or pages are present under identical or very similar names, as seen in Table 2.3.

Table 2.3 Examples of Supportive Islamist Extremist Facebook Pages

Group	Facebook Page	Open/Closed	Members/'Likes'[37]
Al Shabaab	AL SHABAAB	Open	65
	Al-Shabaab Jihad	Open	215
	AL SHABAB	Open	252
Boko Haram*	Boko Haram (Group)	Open	210
	Boko Haram (Individual)	Semi-Private	84
	Boko Haram (Community)	Open	458
	Boko Haram (Individual)	Closed	226
	BOKO HARAM NEWS	Open	7,563
	Boko Haram (organisation)	Open	1,799
Hizb ut Tahrir	Hizb ut-Tahrir (Pol Party)	Open	15,585
	Hizb ut Tahrir Pakistan**	Open	173
	Hizb ut-tahrir America (Interest Group)	Open	280
	Hizb ut-Tahrir (Pol Party)	Open	677
	Hizb ut Tahrir Afghanistan (Pol Party)	Open	400
	Central Contact Committee – Hizb ut Tahrir Wilayah Pakistan (Community)	Open	380
	Hizb-ut-Tahrir	Closed	228
	Hizb ut Tahrir (Pol Party)	Open	13,632
	Hizb Ut Tahrir (Community)	Open	5,793
	Media Office Hizb ut-Tahrir Wilayah Pakistan (Pol Org)	Open	528
	HIZB UT TAHRIR (parti de l'indépendance)	Closed	90
Mouvement Pour L'Unicité et le Jihad en Afrique de L'Ouest (MUJAO)	MUJAO, ARMEE DU COREN	Open	520
	Mujao Clan	Open	486

***Boko Haram, along with other group names, appears as a part of a myriad of various Facebook names. The ones mentioned in this table are British or French-based Facebook pages.**
****Hizb ut Tahrir Pakistan, along with other Facebook pages, contains content in both English and Urdu. Hizb ut-Tahrir offers an interesting Facebook case study since it has up to 56 Facebook pages, under various guises, supporting the group. The ones listed in Table 2.3 are the pages with English and French content.**

Like many of the more popular modern social networking outlets, Facebook has a multi-platform potential for users, allowing for in-group messaging, sharing of videos, photos and chat capacities. For more extreme organisations, this means group administrators and members can easily distribute information to followers, as well as converse with other like-minded individuals. It also allows individuals to invite friends to join Facebook groups that they think might interest them.

More extreme Islamist Facebook groups, like the ones currently supporting Boko Haram, openly show violent imagery and footage as well as martyrdom propaganda. Images of death scenes after Boko Haram attacks can be found on these Facebook pages, and while

[37] Individuals 'like' Facebook pages whereas individuals can join groups and become a 'member'.

they are often bloody and violent, they are not illegal and no more explicit than images shown in the news. These Facebook groups also provide links to websites such as <www.BOKOHARAMNEWS.org>, although many of the linking sites tend to be blocked or taken down. Many of the better-known proscribed jihadist organisations, such as al-Qaeda, have brief official statement pages provided by Facebook that state the illegal nature and proscribed status of 'terrorist organisations'.

Facebook has its own Statement of Rights and Responsibilities (SRR) for users that explains Facebook's basic legal framework and regulations. The SRR is constantly being updated to ensure Facebook develops its legal structure as the online outlet progresses, with the last revision being on the 15th November 2013. Section 3.7 of the SRR states explicitly that users "will not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence." [38] Section 3.10 states that users "will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory." Violations of the SRR result in infringing content being removed and the account disabled.[39]

For young individuals scouring Facebook, there would generally need to be a previous knowledge or inclination towards these groups in order to find them and join. There are also a number of anti-Islamist Facebook groups that might be found when looking for Islamist organisations on Facebook. Like other social networking outlets, there is an issue with authenticity. It is almost impossible for a general user or sympathiser to know whether or not a Facebook group is directly linked to an organisation. For this reason, Facebook is less about recruitment and more about finding like-minded sympathisers and solidifying preconceived notions.

Twitter

By 2012 Twitter had over 500 million registered users posting 340 million tweets per day.[40] Twitter provides an open forum for content sharing and debate, so that any user can see and follow Twitter feeds. While this has deterred some Islamist and jihadist groups from using the application, due to its inability to hide content sharing and conversation, other

[38] 'Facebook's Statement of Right and Responsibilities', *Facebook Legal Terms, (*SRR last updated 15 November 2013).
[39] Ibid.
[40] Lunden, Ingrid (2012) 'Analyst: Twitter Passed 500M Users in June 2012', *Tech Crunch*, 30 July.

Islamist organisations are using the open platform to engage in real-time organising, provocation and debate. Islamist extremist interactions through Twitter are on the rise. Often the main Twitter feeds of popular Islamist groups are written in perfect English. Sometimes they are paired with social feeds in other languages and sometimes messages are written bilingually to reach a wider audience.

While most active online platforms are aimed at potential supporters or followers, Islamist Twitter users are also directing their *tweets* outwards at their opposition. One interesting development has been the open provocation and engagement between jihadist tweets and government networks. An example of this has been the 'Tweetclash' between NATO's International Security Assistance Force (@ISAFmedia) in Afghanistan and the Islamic Emirate of Afghanistan (@ABalkhi), a Taliban faction.[41] Parlance between the two groups via micro-blogging sites regularly includes replies to jihadist tweets correcting their statements and claims or engaging in public provocation. Islamist groups using Twitter will also direct their commentary at specific political or international figures.

Al-Shabaab in particular, using various forms of @HSMPress, have responded to tweets ranging from Kenyan military spokespersons to Al-Jazeera correspondents. The group has also used their tweeting capacity to organise and publicise terrorist acts, see Example Box 2.6. While the al-Shabaab network has used Twitter to further their Islamist extremist agenda, they are also wary of the potential repercussions of online usage and realise that their Twitter accounts can be used to track and counter their efforts. In January 2014, al-Shabaab threatened untold consequences if Somalia-based telecom companies did not terminate Internet connectivity. Other online activists are also using similar tactics to warn authorities of al-Shabaab actions in various localities and track the group's movements: [42]

[41] See: Alonso, Pierre (2012) 'Twitter: The New Frontline in Global Cyber-Jihad', *OWNI.eu*, 10 January.
[42] Matinde, Vincent (2014) 'Somalia's al Shabaab threatens to cut Internet connectivity', *IT Web Africa*.

Example Box 2.6 Al-Shabaab's use of Twitter

Al-Shabaab had been active on Twitter previously, however, the group became internationally known for their *tweeting* during the shootings that took place 21 September 2013 at the Westgate Centre, a prominent Kenyan Mall. Al-Shabaab claimed that the attacks, which resulted in 62 fatalities and 120 injuries, were in retaliation for the deployment of Kenyan troops in Somalia. As the attack was taking place, al-Shabaab members conducting the violence live-tweeted their actions, commenting on the general scene of chaos and goading Kenyan authorities. While Twitter attempted to shut down al-Shabaab's account, new accounts rapidly appeared under various forms of the Twitter account 'HSM Press'. Around the time of the terrorist attack, Twitter shut down five accounts while at the same time copycat accounts, countering al-Shabaab, appeared.

Examples of Official and Copycat al-Shabaab Twitter Accounts

Official Al-Shabaab Twitter Accounts	Copycat & Misleading Counter Accounts
@HSMPROffice	@HSM_PRESOFFICE2
@HSM_Press	@HSM_PRESS2
@HSM_PR	@HSM_Press2
@HSMPress1	@HSM_PresOffice2
@HSM_PROffice	@HSMPRESS1
@HSMPressOffice	@HSMPress4

A War of Authenticity: Copycat accounts also began claiming to have the names of al-Shabaab members involved in the attack. This was countered by official al-Shabaab accounts (now shut down) stating that they had never revealed details of attackers. As explained by David Barnett, expert in jihadism, authentication of Twitter accounts became a large issue for al-Shabaab administrators trying to make sure they were in control of the al-Shabaab message.[43] Clues for authenticity were there for the keen eye, however, for the average user large-scale confusion ensued. Official accounts at the time had a grey and white al-Qaeda flag as their photo, while copycat sites used white and black. Even this simplification was confused since previous official sites had used white and black. Official al-Shabaab accounts also tend to first tweet in Arabic as well frequently including the first verse of the Quran which translates as 'In the name of God, the Most Gracious, the Most Merciful':

Misleading Counter Accounts: Copycat Twitter accounts can be set up by decentralised or non-official supporters of al-Shabaab, other Twitter accounts have developed for the specific purpose of providing a counter narrative or derailing al-Shabaab efforts:

[43] Barnett, David (2013) 'Are you looking at an official Shabaab Twitter account?', *Threat Matrix: A Blog of the Long War Journal*, 25 September.

The identity and location of authors on Twitter remains unknown even to government officials, meaning that tracking the source of 'tweets' is impossible. Similar to the proliferation of different Facebook groups supporting the same Islamist organisations, without being able to track the account of Twitter users the issue of authentication remains, as seen in Example Box 2.6. Social media support networks have become increasingly decentralised, with this having both positive and negative effects for Islamist and jihadist groups. Decentralisation allows their message to reach wider audiences while at the same time exposing trends, goals and intentions to the wider public.

Social sharing outlets have also allowed certain key figures within Islamist organisations to personally spread their ideas and goals to wider audiences. Anjem Choudary, co-founder of the Islamist group al-Muhajiroun, is a modern extremist utilising the online social networking sphere to his advantage. Choudary has been a key figure in re-branding and renaming al-Muhajiroun (refer to Table 2.1). He is an active Islamist figure in the UK, utilising Twitter to disseminate information and distribute his YouTube videos. He was particularly vocal during the Woolwich trials, defending the two men on trial. Choudary has multiple Twitter accounts with the first entry in Table 2.4 believed to be his authentic one:

Table 2.4 Anjem Choudary Twitter Accounts	**Followers (Jan 2014)**	**Tweets (Jan 2014)**
@anjemchoudary	6,907	3,028
@anjemchoudary_	1,438	4,821
@Anjem_Choudary	375	470
@AnjemChoudarbr	71	6
@anjemchoudary2	282	203

Twitter confronts extremist accounts and/or unwanted materials within their Terms of Service, stating clearly:

We reserve the right at all times (but will not have an obligation) to remove or refuse to distribute any Content on the Services, to suspend or terminate users, and to reclaim usernames without liability to you. We also reserve the right to access, read, preserve, and disclose any information as we reasonably believe is necessary to (i) satisfy any applicable law, regulation, legal process or governmental request, (ii) enforce the Terms, including investigation of potential violations hereof, (iii) detect, prevent, or otherwise address fraud,

security or technical issues, (iv) respond to user support requests, or (v) protect the rights, property or safety of Twitter, its users and the public. (Section 8, Twitter's Terms of Service)

With regards to information sharing and disclosure, Twitter clarifies that they do not disclose private personal user information except in the limited circumstances they describe, which includes legal disputes and harm done to others. In this case Twitter states:

Notwithstanding anything to the contrary in this Policy, we may preserve or disclose your information if we believe that it is reasonably necessary to comply with a law, regulation or legal request; to protect the safety of any person; to address fraud, security or technical issues; or to protect Twitter's rights or property. However, nothing in this Privacy Policy is intended to limit any legal defenses or objections that you may have to a third party's, including a government's, request to disclose your information. (Information Sharing and Disclosure, Twitter Privacy Policy)

As illustrated by this subsection, the legal practices and policies of widely used social networking sites, like Facebook and Twitter, have to balance the advocacy of free speech with government regulation.

YouTube

Whilst many free video sharing sites have been developed in the last ten years (i.e. Vimeo, Vevo, Dailymotion, Veoh and Flickr) YouTube continues to be the most widely viewed and used video site in Europe and North America. There are upwards of 26 million French citizens and 32.1 million UK citizens using YouTube.[44] YouTube globally attracts upwards of 1 billion unique active users each month.[45]

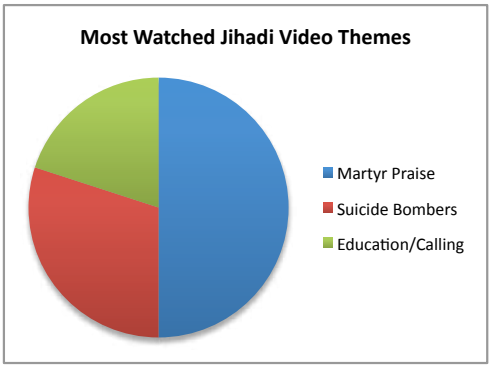
A study in 2008 found that extremist videos on YouTube could be divided thematically into a) the praising of martyrs, b) promotion of suicide bombing and c) educating about the Islamist extremist worldview. These findings are shown in Figure 2.3. However, in recent years, YouTube introduced a flagging mechanism so that users can report videos that breach their Community Guidelines. Flagged videos are reviewed by a human reviewer and removed if they breach YouTube's policies, which for extremist videos includes any video

[44] French statistics were correlated by Médiamétrie while UK statistics were processed by UMPF.
[45] 'YouTube Stats: Site Has 1 Billion Active Users Each Month', *Huffington Post*, (20 March 2013).

that incites violence, glorifies terrorism, or attempts to recruit extremists to a violent cause. Some videos showing terror attacks are legitimate news, especially in regions where journalists can't go, like Syria at the moment, and so even though they can be misappropriated for negative reasons, the videos must remain on the site as a method of legitimate news source.

Figure 2.3 A Breakdown of Most Viewed Jihadist YouTube Videos[46]

Previous research analysing the most highly viewed jihadist videos on YouTube demonstrated that 50% of jihadist videos contained 'martyr hailing' content or praise of martyrdom. Meanwhile an estimated 30% contained footage of suicide bombings. Another significant percentage contained educational content about Islam and the call to martyrdom. While such videos can contain other elements, these are generally the top three themes found in the most watched jihadist videos.



Based on the research done for this report, a visible shift in Islamist videos distributed within British and French websites been detected. UK and French-based Islamist extremist video content now aims towards a more neutral but sympathetic audience. Videos attached to static websites in particular focus more on education and the praising of martyrs, rather than more overtly violent content, such as suicide bombing. This is partly due to awareness of potential extremist labelling that might lead to government blocking or censoring of these sites and also YouTube proactively removing content that is openly in breach of their user guidelines.

Young online users are the primary distributors and consumers of online jihadist YouTube videos, like the ones mentioned in Figure 2.3. It is estimated that upwards of 85% of posting and consumption of such videos is by users aged 18 to 34.[47] Often a range of videos covering the themes outlined above can be found on a single YouTube channel, as illustrated in Example Box 2.7. Channels allow followers to access a number of videos with

[46] Data for Figure 2.3 Cited from: Conway, Maura & McInerney, Lisa *Jihadi Video & Auto-Radicalisation: Evidence from an Exploratory YouTube Study*, First European Conference on Intelligence and Security Informatics, (December 2008).
[47] Ibid.

similar themes and agendas, solidifying preconceived notions while also allowing followers to comment and network with each other through YouTube.

Example Box 2.7 Salafi Media UK on YouTube

Salafi Media UK runs one of the larger pro-Islamist YouTube channels, and provides a platform for the al-Muhajiroun network (see Figure 2.1 for reference). As of January 2014, the YouTube channel had 2,281 subscribed followers and, since its creation in October 2011, has had 229,828 views.

Networking Content: As seen by the image of the YouTube channel's homepage, this channel also has links to its official Twitter account (@SALAFIMEDIAUK with 1,227 followers) and Facebook account (Salafimediauk with 858 likes) as well as a website page (though the website has subsequently been blocked). Twitter and Facebook accounts serve as secondary platforms for reposting all the videos uploaded to the Salafi Media YouTube channel. A majority of video content contains lectures given by various Islamist preachers. However, content about converting to Islam is also highly popular.

Top 10 SALAFIMEDIAUK Videos

	Video Title	Posted	Views (as of Jan 2014)
1	I Used To Be A... Gangster !	26-5-2012	17,423
2	Rules & Fiqh of Fasting in Ramadan - Abu Muwahhid	9-7-2012	8,862
3	Abu Abdullah | The Return | Part 1	27-11-2013	5,520
4	To Mr Obama | Abu Abdullah Speaks | SALAFIMEDIAU	27-12-2013	4,390
5	Will He Become Muslim Full || Al Siraat Dawah UK || SALAFIMEDIAUK	22-2-2013	4,158
6	Invitation To Islam - Abu Hamza Al Masri	11-4-2012	3,616
7	Abu Abdullah | The Return | SALAFIMEDIAUK	25-11-2013	3,566
8	The Days Events Episode 3	13-5-2012	3,102
9	Our Enemies || Abu Waleed || SALAFIMEDIAUK	14-3-2013	2,772
10	Baddies n Hoodies Trailer	2-8-2012	2,733

It is worth noting that the most viewed videos were posted more recently (in the last year) showing growth, rather than stagnation, of the channels viewership. The Salafi Media UK platform is run by a Londoner who goes by the pseudonym Abu Waleed, a 33-year-old Islamist activist and regular speaker at the London School of Sharia, the fabricated Islamist teaching group set up through AM.[48]

[48] Lowes & Mulhall (2013) *Gateway to Terror: Anjem Choudary & the al-Muhajiroun Network*, (Hope Not Hate).

While some Islamist and jihadist videos gain very little attention, others go viral. In other words, some videos become very popular gaining huge attention; in that they are watched, shared and redistributed numerous times. Some videos of popular Islamist preachers' speeches, or videos calling to Islam, receive more than 100,000 views. While numbers this high are quite rare, a video's ability to gain a wide audience is dependent on online activists posting and sharing the video on multiple online platforms.

Videos also serve as a form of documentation and validation, in that they preserve live footage of terrorist acts and document Islamist extremist events, providing proof of a group's impact. Whilst extremist video content can be easily found by searching the names of organisations directly on YouTube, videos are also found shared on other social media platforms. Islamist websites, Twitter links, Facebook walls and forums all provide a space for sharing links to videos.

In recent years, there has been an increasing amount of extremist video content available for British and French consumption. In attempts to broaden a video's potential viewership, some non-European Islamist YouTube videos are created equipped with English or French subtitles. However, a large number of YouTube videos and channels are being created within European countries to cater for Islamist supporters at a local and national level.

A large amount of the YouTube content aimed at English and French-speaking audiences would not fall under legal dispute since it does not break any content laws. However, video sharing sites often take down videos that are reported and found to be explicitly illegal or go against user Guidelines. With reference to the legality of potentially extremist Islamist videos, YouTube includes the following in its guidelines: [49]

- *Don't post videos showing bad stuff like animal abuse, drug abuse, or bomb making.*
- *Graphic or gratuitous violence is not allowed. If your video shows someone getting hurt, attacked, or humiliated, don't post it.*
- *YouTube is not a shock site. Don't post gross-out videos of accidents, dead bodies and similar things.*
- *We encourage free speech and defend everyone's right to express unpopular points of view. But we don't permit hate speech (speech which attacks or demeans a group based*

[49] Terms of Use, YouTube Community Guidelines: <https://www.youtube.com/t/community_guidelines>.

on race or ethnic origin, religion, disability, gender, age, veteran status, and sexual orientation/gender identity).

- *There is zero tolerance for predatory behavior, stalking, threats, harassment, invading privacy, or the revealing of other members' personal information. Anyone caught doing these things may be permanently banned from YouTube.*

Although YouTube continues to face criticism for some of the video content it hosts, the scale and constant addition of content to the site makes proper filtering and taking down of all illegal content almost impossible. It should also be noted that a large portion of Islamist extremist videos do not go against any regulations and laws. Importantly, extremist content does not have to be overtly violent, openly hateful or openly in support of an illegal organisation in order to be effective in its message.

Issues of Authentication

As with social media outlets discussed, for individuals searching for websites and online communities in English and French there is a growing issue with authentication. Considering that sites can be run from virtually anywhere, there is no need for leaders within Islamist organisations to be in charge of online sites supporting them. External supporters in any country can easily create online content and support sites with or without central permission.

Experts speculate that expatriates in the US and Europe help form a key network of online jihadists. This creates a large gap between the territory in which these movements are based and the technology being used to disseminate messages and potentially recruit new followers.[50] Since 2001, al-Qaeda has been losing territorial bases in some places whilst gaining others elsewhere. Online social networks, therefore, have become an alternative means through which extremist messages can be disseminated. In this way, supporters are no longer confined to local or national settings, and in spite of setbacks on the battlefield, the messaging remains uninterrupted.

The virtual domain also allows for decentralised support networks to form and develop independently of centralised authorities. Producers of jihadist websites, for example, tend

[50] Alonso, Pierre (2012) 'Twitter: The New Frontline in Global Cyber-Jihad', *OWNI.eu*, 10 January.

not to be official members of jihadist organisations. Research by the General Intelligence and Security Service in the Netherlands found that the majority of online website and content 'producers' were fanatical jihadist supporters, but not official members, maintaining and feeding the online spaces for jihadism.[51] Administrators of a site, or account, fund and build the core of web forums whilst moderators tend to be the most avid users and consumers. Dedicated administrators and users of these sites monitor the content and direction of online discourse.

As explained by counterterrorism analyst, Aaron Zelin, in an interview with the Washington Free Beacon: "If the dissemination of official releases is no longer to be done centrally, it has the potential to make the forums obsolete and usher in a new era whereby jihadi activists primarily rely on social media platforms to interact with one another."[52] Examples of this kind of decentralised support of extremist organisations have been given within this chapter, such as Example Box 2.6.

Summary

This chapter has given an overview of the scale and diversity of online Islamist extremism in the UK and France. By mapping the Internet usage of Islamist organisations that operate in English and French, it has shown the diversity of international and illegal Islamist organisations that now have online support networks operating in Europe. This suggests there is a rise in decentralised communication hubs as individuals and smaller groups are taking it upon themselves to disseminate the Islamist message to a broader audience.

In using search engines to find extremist content, this chapter has shown that search engines, like Google, rarely produce direct links to pro-Islamist online materials among the top search results. However, positive counter narratives are also absent in top results, implying there is simply a lack of such content. In analysing static websites it has shown that most illegal Islamist groups do not have easily available websites, or sites that have not yet been taken down. Websites in English and French are most often used to propagate the

[51] Bertholee, Rob (2012) *Jihadism on the Web: A breeding ground for Jihad in the modern age*, General Intelligence and Security Service: Ministry of the Interior and Kingdom Relations.
[52] Gertz, Bill (2013) 'Al Qaeda Opens First Official Twitter Account', *The Washington Free Beacon*, (27 September.

Islamist narrative, promote the idea of martyrdom and solidify an allegiance to specific Islamist causes, rather than directly recruit or distribute directly violent messaging.

Open chat rooms and discussion forums used by Islamist networks in the UK and France are declining due to the reticence around having extremist views aired publicly. In fact, many forums linked directly with proscribed groups have been shut down. Islamist forums and chat spaces in English and French still exist but, increasingly, more extremist discourse is taking place on the dark web where membership, passwords or authentication are required. Where discourse that occurs at the early stages of radicalisation can be found there is a potential for counter-narratives to have an impact.

Regarding Facebook, most centrally controlled Islamist groups are sceptical of this social networking service due to its facial recognition capacities and ability to identify networks. Islamist Facebook supporters are primarily young sympathisers taking it upon themselves to post regularly, linking sympathetic martyr-based or educational videos to Facebook walls. Twitter, on the other-hand, has become increasingly popular and is utilised in various ways by Islamist groups. It has been used in the lead up to, and during, violent attacks as a way of disseminating information about a group's actions as well as a means of provoking authorities and those viewed as enemies. Because the identity and location of Twitter users remains unknown, even to governments, tracking the identity of account users is difficult.

YouTube contains an extensive and accessible collection of extreme Islamist videos with themes that are similar to those found on static websites. These include martyr praising, promoting suicide bombing and educating about Islam from an Islamist extremist perspective. YouTube channels also allow individuals to access streams of films that contain extremist narratives yet lack counter-narratives, allowing the individual to create their own online echo chamber. Such video content is increasingly available in English and French.

The next chapter moves on to analyse the likelihood of radicalisation taking place in isolation of other socialising agents as well as exploring how extremist content is currently being used by consumers.

Chapter 3. Radicalisation and the Internet

The previous chapter mapped the primary ways in which the Internet, or online extremist content, is used by Islamist extremist groups in the UK and France. This chapter analyses pathways leading to radicalisation and the role the Internet plays in the radicalisation process. In particular, it seeks to find the point at which the Internet becomes salient in the radicalisation process and whether or not the Internet can radicalise individuals in isolation of real-world factors or interactions.

This chapter is divided into three sub-sections:

- The first section of this chapter discusses 'lone wolf' theories and assesses their credibility in light of existing expertise on radicalisation.
- The second tracks the various 'first sparks' of radicalisation, analysing the primary agents that tend to introduce individuals to radical Islamist narratives.
- The third offers an in-depth insight into the role of the Internet in the process of radical Islamist indoctrination.

These three sections are followed by a summary that offers an overview of the exact role the Internet should be afforded in the radicalisation process. The three sections will draw on research conducted between January and March 2014 that was qualitative in nature. This research included interviews with experts on online radicalisation and counter-terrorism who have researched and written reports dealing with radical Islamist trends and counter-extremist efforts. It also included interviews with mentors who have counselled radicalised individuals who had previously engaged in Islamist extremist activities.

Furthermore, focus groups with target audiences, i.e. individuals of a particular age, location and background that are more likely to be exposed to Islamist extremist online content and propaganda, were conducted in order to gain an appreciation of how online extremist content is perceived and consumed.

3.1 The Myth of the 'Lone Wolf'

The term 'lone wolf' has become increasingly popular in recent years as a number of terrorist attacks have involved a single actor. Other buzz terms such as 'grassroots terrorists', 'virtual training camps' and 'home-grown Islamists' have also been used in relation to the theorised 'lone wolf' phenomena. These various terms also suggest that there is a lack of agreement when it comes to understanding the process behind the phenomena. For example, 'freelance terrorism'[53] insinuates different underlying processes when compared to more controversial labelling such as 'sudden jihad syndrome'.[54]

In its most simple form a 'lone wolf' is "a person who acts on his or her own without orders from – or even connections to – an organisation" and as such "is a standalone operative who by his very nature is embedded in the targeted society and is capable of self-activation at any time."[55] Since the mid 1990s, and particularly since 9/11, fears over 'lone wolf' terrorism have increased. While 'lone wolves' of the past were primarily linked to the radical right, contemporary concern has shifted to militant Islamists.[56] For law enforcement officials and counter-terrorist analysts lone wolves pose a major threat to security efforts due to the fact that they are often difficult to identify and track before acts are attempted or carried out.[57]

The FBI in the US has expressed concern that lone extremists represent an ongoing threat to security measures, and that the threat is increasing, rather than subsiding.[58] In trying to explain this phenomenon many government reports on 'lone wolf' attacks in the USA, UK, France and Canada focus on the Internet as a key source of radicalisation. The perception that Internet forums, such as Sada al Jihad, and al-Qaeda's *Inspire* magazine, directly lead individuals to carry out terrorist attacks autonomously is very real.[59] With these fears of an

[53] Hewitt, Christopher (2003) *Understanding Terrorism in America: From the Khan to Al Qaeda* , Routledge: London & New York p.79. Kushner, Harvey (2003) *Encyclopedia of Terrorism*, Sage: Thousand Oaks and London p.144-145.
[54] Pipes, Daniel (2008), 'Sudden Jihad Syndrome – It's Now Official', *Middle Eastern Forum*, 2 January.
[55] Burton Fred & Stewart, Scott (2008), 'The "Lone Wolf" Disconnect', *Statfor Global Intelligence*, 30 January.
[56] (2007), *Lone-Wolf Terrorism*, Instituut voor Veiligheids- en Crisismanagement,
[57] Ibid.
[58] Mueller III, Robert (2003) 'War on Terrorism', *Testimony of Robert S. Mueller, III, Director, FBI, Before the Select Committee on Intelligence of the United State Senate*, Washington.
[59] Bakker,Edwin & de Graaf, Beatrice 'Lone Wolves: How to Prevent this Phenomenon?', *Expert Meeting Paper*, November 2010, International Centre for Counter-Terrorism: The Hague.

out-of-control 'lone wolf' epidemic, we need to question who these 'lone wolf' attackers actually are and whether or not we are really witnessing home-grown radicalisation driven by the Internet.

Table 3.1 lists all the cases of 'lone wolf' attacks in the UK and France since 2000. The table lists the perpetrators along with data on the injuries or deaths incurred as a result of their actions and whether or not the attack was carried out or in its planning stages. This is followed by a brief description of each 'lone wolf' case with special reference to the role of the Internet or other factors that could have contributed to their radicalisation.

Table 3.1 Islamist 'Lone Wolf' Cases in the UK and France since 2000

Year	From	Perpetrator	Killed	Injured	Attack	Actor Type
2000	UK	(1)Nabil Ouldeddine	0	1	Carried out	Loner
2003	UK	(2)Rahaman Alan Hazil Mohammed	0	0	Attempted	Loner
2006	UK	(3)Hamaad Munshi	0	0	Attempted	Wolf Pack
2007	UK	(4)Bilal Abdula/Kafeel Ahmed	1	0	Carried out	Wolf Pack
2007	UK	(5)Nicholas Roddis	0	0	Attempted	Loner
2008	UK	(6)Nicky Reilly	0	1	Attempted	Lone Wolf
2008	UK	(7)Krenar Lusha	0	0	Attempted	Loner
2009	UK	(8)Andrew 'Isa' Ibrahim	0	0	Attempted	Loner
2010	UK	(9)Roshonara Choudary	0	1	Carried out	Loner
2012	FR	(10)Mohammed Merah	8	5	Carried out	Loner
2012	UK	(11)Mohammed & Shasta Khan	0	0	Attempted	Wolf Pack
2013	UK	(12)Michael Adebolajo & Michael Adebowale	1	0	Carried out	Wolf Pack
2013	FR	(13)Alexandre Dhaussy	0	1	Carried out	Loner

There is a high degree of variation in background, motivation and method of attack between the various perpetrators. In an attempt to categorise this variation Raffaello Pantucci developed a *Typology of Lone Wolves* resulting in four categories, which were referenced in Table 3.1:

- **Loner:** An individual who plans or attempts an act of terrorism justifying their actions through an extreme Islamist ideology although they do not seem to have any actual connection or contact with other extremists. They are individuals fascinated by Islamist extremism despite no evidence of external command or control.

- **Lone Wolf**: An individual who appears to carry out their actions alone but, in fact, does demonstrate some level of contact with other operational extremists. There is some form of command structure even if through remote means only.
- **Lone Wolf Pack**: A group of individuals, usually a pair, who self-radicalise using Islamist extremist narratives. They radicalise in isolation and then seek to commit acts of terror. Though they have may have operational contact with extremists they are not instructed by a broader terrorist community to act.
- **Lone Attacker**: Lone Attackers are individuals who operate alone but clearly show control links with actual terrorist affiliates that are operating a hierarchy of command.[60]

Even with this typology, a character type is still difficult to develop due to the variation amongst perpetrators. With most of the aforementioned cases we must be very careful before deeming them 'lone wolf', especially since the report is dealing with individuals suffering from severe mental health issues (Nabil Eddine and Nicky Reilly) or individuals with highly troubled pasts and previous criminal convictions (Andrew Isa Ibrahim and Alexandre Dhaussy). In some instances it was not necessarily the case that individuals were radicalised in isolation; rather, there is a lack of data on the previous experiences of foreign nationals before they came to the UK (Rahaman Alan Hazil Mohammed and Krenar Lusha).

In other cases it also seems clear that there was, in fact, direct offline contact with other radical Islamists in the perpetrator's localities (Hamad Munshi, Michael Adebolajo and Michael Adebowale). In studies conducted on the labelled 'lone wolf' attackers in the US it was found that over a quarter of perpetrators did, in fact, have major links with international jihadist groups like al-Qaeda.[61] In these cases further investigation into the

[60] While there are currently no Lone Attackers listed in the cases to date in the UK and France the typology is included since there are instances of this typology in other case studies, mainly in the US. See Pantucci, Raffaello (2011) 'Wolves: Preliminary Analysis of Lone Islamist Terrorism', *ISCR*: London.
[61] Johnson, Toni, (2011), 'Threat of Homegrown Islamist Terrorism', *Council on Foreign Relations*.

extremist networks behind the perpetrators is key. While further arrests were made in relation to Munshi's network we have yet to see continued investigations into the Woolwich attackers' relations with the al-Muhajiroun network, which has been reported in the media.

The remaining 'lone wolf' cases are laced with a number of unanswered questions relating to the 'first spark' that initiated the perpetrators' journeys towards extremism. However, even within these more questionable cases there seems to be a large focus on media-related events that triggered discontent with global geo-politics. This discontent is combined with the sentiment that there is no outlet for discussing or impacting the situation leading to a sense of helplessness. The impact of the media in combination with a lack of humanitarian infrastructure to address concerns is discussed further in the next section of this chapter along with the psychological processes behind radicalisation.

Is the Fear of 'Lone Wolf' Terrorism Realistic?

Not only are 'lone wolves' a rare phenomena, often causing minimal harm to the greater public, but the term itself seems flawed as a category when so many of those falling under this generalisation are highly varied and laced with larger causal factors. In studies done across Europe, Australia and North America, terrorists acting as lone wolves accounted for only 1.28% of the total number of terrorist incidents.[62] With such a small sample incidents of this nature are almost impossible to categorise, let alone predict.

The high rate of psychological disturbance and social ineptitude among actors of this kind is also important to examine.[63] The issue of mental disturbance and sociopathic tendencies was brought up in interviews with mentors dealing with convicted violent Islamist extremists. In many 'lone wolf' cases there is a higher tendency for mental health illness, which has manifested or intensified in the lead up to attacks ranging from delusional and obsessive fantasists to more severe displays of schizophrenia.[64] Therefore, we need to ask whether these were attacks driven by extremist ideology or whether they were attacks by disturbed individuals looking to fixate and justify their feelings of isolation.

[62] Bakker, Edwin & de Graaf, Beatrice 'Lone Wolves: How to Prevent this Phenomenon?', *Expert Meeting Paper*, November 2010, International Centre for Counter-Terrorism: The Hague.
[63] Ibid.
[64] In interviews with Mentors dealing with convicted extremist they all cited issues of mental health; mental health is spoken about by Raffallo Pantucci. Interviews were conducted between February and March 2014.

As discussed in an interview with lone wolf expert, Pantucci, very few, if any, of the terrorist cases deemed 'lone wolf' include individuals that were socialised in an isolated 'vacuum'. In other words, the vast majority of terrorist cases involve a real world experience or relation that introduces extremist ideologies to the individual. That is not to say that online materials and social networking on the Internet do not play a large role in the process of radicalisation leading to 'lone wolf' attacks, but it is necessary to point out that the Internet is often not the sole agent or initiator of the radicalisation process. Hence, the ability of extremist material online to create that first spark that initiates a journey towards extremism must be questioned.

Roshonara Choudary and Krenar Lousha are perhaps the only two examples to date of isolated individuals who have carried out terrorist acts seemingly without any known connection or relation to other radicalised individuals. However, sometimes there are simply elements of the story missing. In Lousha's case, questions remain about the possible radicalisation he might have experienced before seeking asylum in the UK. In the Choudary case, questions about the strong influence of certain individuals close to her remain and although these negative influences were not divulged in court, they were mentioned by mentors in interviews.

Implications for the Internet

In the aftermath of the Roshonara Choudhary attack in 2010, hundreds of YouTube videos were taken down by request from the US government. This was done citing YouTube's own regulations prohibiting 'dangerous or illegal activities such as bomb-making, hate speech and incitement to commit violent acts,' as well as content coming from accounts 'registered by a member of a designated foreign terrorist organization'.[65] In 2007, according to media reports, after the two attacks listed in Table 3.1, the British Labour Party government requested that YouTube block terrorist recruitment videos which featured extremist Islamist fighters with rockets or guns.[66] In May 2010, the US Senator, Joseph Lieberman, asked Google to remove over 120 terrorist recruitment videos from YouTube.

[65] Burns, John & Helft, Miguel (2010) 'YouTube Withdraws Cleric's Videos', *New York Times World,* 4 November.
[66] Ibid.

After government requests, some videos, which contain outright violence or hate speech, have been removed whilst others have remained online. This has been done in an attempt to distinguish between content that is merely offensive and content that is hate speech or incites violence.[67] Periods of pressure on search engines and sharing sites, like Google and YouTube, often begin in the aftermath of militant Islamist attacks.

The problem remains that while governments are quick to attack the Internet as the source for radicalisation, there are few measurable outcomes from content take-downs. More importantly, content removal as a reaction to violent extremist acts is attacking a symptom, rather than dealing with the source, i.e. the proliferation of extremist narratives in society. Hence, broad censorship would fail to impact Islamist radicalisation trends, whilst an argument to take down content that explicitly breaks the law still remains.

3.2 Radicalisation: The 'First Sparks'

While governments have outlined regulations to counter and prosecute terrorist activities online, defining and countering the Internet's role in the process of radicalisation is much more difficult. Despite many academics and researchers assuming a link between online extremist material and radicalisation in the real world, proving such a link is very difficult.[68] Clearly online extremist content plays a significant, and increasing, role in Islamist radicalisation in British and French contexts; however, the notion that it is a primary or isolated radicalising agent has been undermined in the previous section of this chapter.

Furthermore, this report has shown, in Chapter 2, that it is rare for individuals to come across pro-extremist narratives online through basic term-related searches. There is, however, a much higher likelihood of finding radical content with more advanced knowledge and pre-interest. Or, in other words, the vast majority of those that visit extremist websites and consume the content enthusiastically are likely to have been heading in that direction, and the websites in question are merely aiding an existing journey. The first sparks, or primary socialising agents, are, therefore, likely to be things other than extremist websites, forums, videos and social media accounts.

[67] Rosen, Jeffrey (2012) 'The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google', *Fordham Law Review* (80), pp. 1525-1538.
[68] Edwards, Charlie & Gribbon, Luke (2013) 'Pathways to Violent Extremism in the Digital Era', *The RUSI Journal*, 158(5), pp. 40 – 47.

In this chapter, four primary socialising agents, identified as having an impact on Islamist radicalisation and providing the 'first sparks' for the radicalisation process, are explored. These agents are:

- Mosques
- Universities
- Prisons
- Media/News Reports

All four agents have a previous history of providing a gateway into radicalisation, either by way of providing a space where previously radicalised individuals can disseminate their views or, as is the case with the media, exposing subject matters that are monopolised by extremists online to previously unaware individuals. Individuals are likely to have been introduced to extremist narratives through one of these four socialising agents prior to searching out extremist content or explanations online. As such these socialising agents have the ability to prime and prepare individuals for extremist indoctrination, which they subsequently encounter online. They will now be explored in more detail.

Mosques

Mosques have been identified as 'places of vulnerability' because they have the potential to provide a space for those seeking to recruit and radicalise others. [69] Research by Rogers and Neumann concluded that in countries like the UK and France, that have large proportions of second and third generation Muslims, there was a higher likelihood of radicalisation in religious spaces, primarily Mosques.

This is not to say that mosques need extremist imams or extremist members of the management committee in order to become places of extremist recruitment, though this has happened in some rare cases (see Example Box 3.1). In fact, the vast majority of mosques in the UK and France do not have extremist imams, nor are they run by extremists. However, they are still hubs where lots of young Muslim males with religious inclinations can be found. As such, they can be targeted by extremists within the mosque, or as they leave the mosque after prayers, with strong political messages dressed up in religious

[69] Rogers, Brooke & Peter Neumann (2007) 'Recruitment and Mobilisation for the Islamist Militant Movement in Europe' *Kings College London*: London.

language. In focus groups conducted with young UK-based Muslims, one participant highlighted that mosques previously served as a location for radicalised individuals to proselytise to other Muslims:

I remember going to Regents Park mosque after 9/11 and they said that they could arrange people to go to Afghanistan. (Focus group 1, Male, Age 28).

Radicalisation at mosques seems to have been more prevalent in the lead up to and after 9/11, primarily in the mid to late 1990s and early 2000s. An example of a mosque being used as a centre for radicalisation and recruitment is given in Example Box 3.1 on the following page. While mosques were targeted by extremists in the late 1990s and early 2000s, more recent evidence indicates that mosques are now less likely to be focal points and extremist efforts are increasingly focused on the private sphere.[70] This is partly due to mosques not wanting to be associated with extremist trouble-makers and management committees, by and large, are rejecting the extremist message.

According to the Director-General of the UK's Office for Security and Counter-Terrorism (OSCT) within the Home Office, it is estimated that radicalisation in mosques and other religious institutions now makes up less than 2% of the total recorded radicalisation cases in the UK.[71] This is also the case in France, where in recent years an intricate monitoring system has been set up in places of worship, making it highly difficult for radicalisation in mosques to take place.

[70] Precht, Tom (2007), 'Home Grown Terrorism and Islamist Radicalisation in Europe: From Conversion to Terrorism', *Danish Ministry of Justice*.
[71] (2012), 'Roots of Violent Radicalisation', *House of Commons Home Affairs Committee*, (19th Report Session 2010-12, Vol. 1).

Example Box 3.1 Abu Hamza and the Finsbury Park Mosque

The Finsbury Park Mosque is a prime example of Islamist extremists using the premises of religious institutions to recruit and develop links to violent jihad. The Finsbury Park Mosque was opened in 1994 with the aim of cultivating a centre for peaceful worship, however, by the late 1990s the mosque was found to be the centre point for a significant group of young men being radicalised and subsequently sent to al-Qaeda training camps in Afghanistan. This active process was led by the radical imam, Abu Hamza, along with the radical cleric Abu Qatada. They also set up radicalisation centres in a number of other mosques around London.

Images above show Abu Hamza (left) and Abu Qatada (right).[72]

At least thirty-five Guantanamo Bay detainees reportedly passed through the Finsbury Park Mosque. The primary target for Hamza and Qatada were young men immigrating to London to claim political asylum, primarily from North Africa and the Middle East.[73] For these young men the mosque provided shelter, food and community. At the mosque the two leaders showed their recruits videos of atrocities against Muslims and lectured them on the virtues of the necessity of a pure Islamic state. As foreign fighters their flights were paid for by associates from the mosque.[74]

After the arrest of its leading extremists, the mosque subsequently purged itself of extremist links, re-opening in 2005 under new management with new imams and a new ethos. As one of their main objectives is listed below:

To endorse interfaith dialogue with other religious groups dialogue will focus on clarifying misconceptions, finding common ground, and enhancing civil society through promoting core values, such as, Community, Personal Integrity, Wisdom and Love of Truth, Care and Compassion, Justice and Peace, Respect for One Another and for the Earth and Its Creatures.[75]

[72] Images of Abu Hamza and Abu Qatada were sourced from *Al Jazeera* and the *Birmingham Mail*.
[73] Swinford, Steven (2011) 'WikiLeaks: How Britain Became a Haven for Migrant Extremists', *The Telegraph*.
[74] O'Neill, Sean & McGrory, Daniel (2010) *The Suicide Factory*, (Harper Perennial: London and New York).
[75] 'Aims and Objectives of the Organisation', *FPM Website*.

In focus groups with UK-based Muslims, the majority of participants stated that there was no radicalisation taking place inside any of the mosques they were associated with, nor did they know of any mosques that had a radical reputation. Despite this, one of the problems many individuals identified was that mosques, hoping to remain politically neutral, did not address subjects of a controversial nature and in many times, avoided discussions about contemporary topics that might be in the media.

For some focus group participants this was satisfactory, since mosques were seen as a 'sanctuary' or a 'pure space' that should be devoid of politics. However, many other participants felt that mosques were doing a disservice by not addressing contemporary and/or sensitive topics, and this in turn turned a lot of younger Muslims away from the mosque and into the arms of other more extremist groups.

My mosque in West Ealing, I never hear anything on Woolwich or Muslim problems. It's just normal religious stuff. No modern or current topics. (Focus Group 2, Female, Age 18)

There needs to be a strong response after radical incidents'. [Among Muslims] our go-to stance previously has been to just pray and hope that the backlash on our community isn't too bad. At our local mosque a few years ago someone lit a firebomb in Leyton on the side of the mosque and we just put our heads down and carried on. (Focus Group 2, Male, Age 27).

When speaking to the mentors dealing with Islamist extremist convicts, a similar depiction of mosques was given. Often mosques and religious leaders within Muslim communities prefer to remain neutral on sensitive topics since their knowledge and expertise is on religious matters, and they have very little knowledge of socio-political issues. Therefore, they are ill equipped to hold a conversation with individuals under the influence of extremist ideologies. One of the interviewed mentors stated:

There needs to be support. Mosques and many influential leaders don't even know how to handle someone being radicalised. Where is the good news about Islam? Governments should provide support to educate on how to handle radicalised individuals. (Anonymous Mentor 1)[76]

[76] Mentor interviews were conducted between February and March 2014. All Mentor interviews were anonymous due to the sensitive nature of their work and cases.

Prisons

Prisons also play a critical role in the indoctrination and mobilisation of Muslims across Europe and, as such, are also 'places of vulnerability'.[77] The manner in which prisons function make them conducive to radicalisation in that they produce 'identity seekers', 'protection seekers' and 'rebels' in larger numbers compared to other environments.[78] In prisons individuals experience social isolation and often a personal crisis and these factors can increase a person's responsiveness to extremist messaging.

Within prison systems in the UK and France, the radicalisation of Muslim prisoners is not a new phenomenon, but it is a growing one. There is a long list of individuals that have undergone at least partial, if not full, radicalisation in prison and subsequently have been re-imprisoned for terrorist-related acts. Individuals such as Khaled Kelkal (1995) in France along with UK cases such as Richard Reid (2001), Muktar Said Ibrahim (2005), Mohammad al-Figari (2008) and Martin Mubanga (2001-2005) make up some of the more well-known cases of prison-based radicals attempting, or carrying out, terrorist attacks.

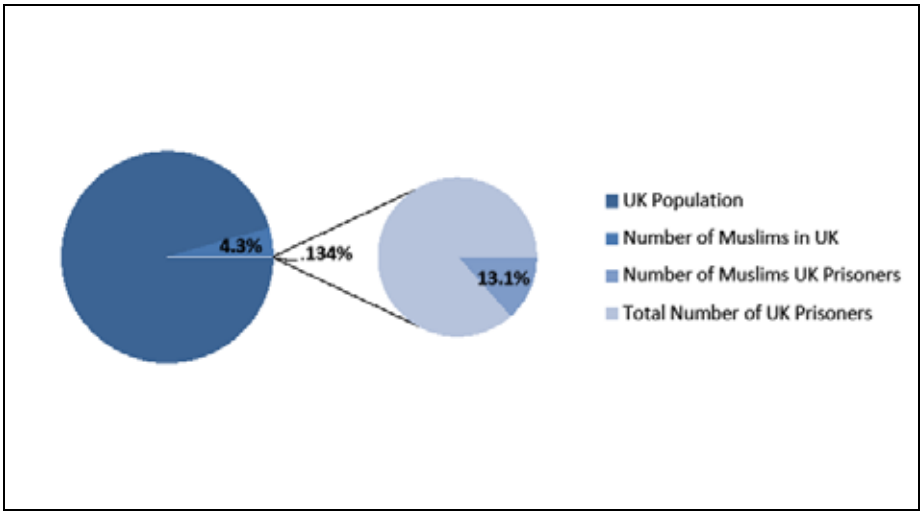
Those converting to Islam in prison are over represented among those adopting extremist or jihadist ideologies in the UK.[79] This is partly explained by the heightened awareness of identity and group loyalty experienced by converts in prison compared with those brought up as Muslims and as such they are seen as easy targets for extremist recruiters. Similar trends are seen in France, where reports have shown that nearly 150 inmates have been caught engaging in proselytising Islamist extremism specifically targeting French-born converts and younger inmates.[80] By giving an allegiance to extremist interpretations of Islam, detainees integrate into a community of brothers, which offers ideology, loyalty and protection.[81]

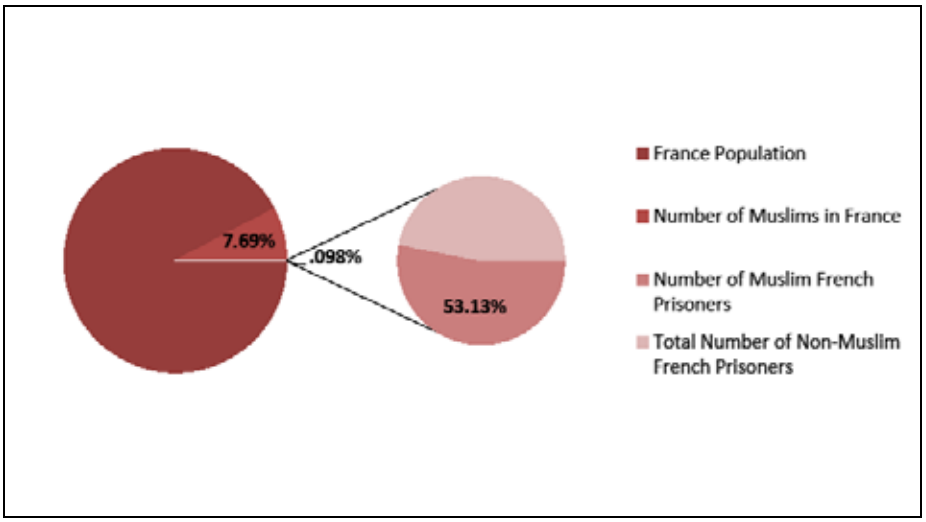
There are some crucial differences, however, when comparing UK and French case studies on the spread of Islamist extremism in prisons. This mainly has to do with the Muslim populations in the UK and France and their representation in prison. There are an estimated

[77] Rogers, Brooke & Neumann, Peter (2007) 'Recruitment and Mobilisation for the Islamist Militant Movement in Europe' *Kings College London*: London.
[78] Neumann, Peter, (2010) 'Prison and Terrorism', ICSR: London.
[79] Brandon, James (2009)'Unlocking Al-Qaeda: Islamist Extremism in British Prisons', *Quilliam*: London.
[80] Khosrokhavar, Farhad (2004) *L'Islam dans les Prisons: Voix et Regard*s, Balland: Paris.
[81] Hannah, Greg et al (2008) 'Radicalisation or Rehabilitation'. *Rand Corporation:* Santa Monica CA.

2.7 million Muslims in the UK making up around 4.8% of the total British population. However, in UK prisons Muslims account for up to 13.1% of the total prison population.[82] While this seems like a high figure, in France the figures are much higher. A comparison of Muslim national populations compared with prison populations in the UK and France is given in Figure 3.1.

Figure 3.1 Muslim Populations compared with Prison Populations in the UK and France





[82] Berman, Gavin & Dar, Aliyah (2012) 'Prison Population Statistics', *Social and General Statistics*, (House of Commons).

In France, statistics on the Muslim population range between 3%[83] and 13%[84] because the French Republic prohibits performing censuses which make distinction between citizens based on their race or their beliefs. This report uses the figure of 7.69 % [85] as the true figure is disputed and this percentage is a moderate estimation. There are large Muslim-majority suburbs outside of Paris, and in other major cities, that are seen as target areas for police officers and law enforcement agents. Perhaps because these areas with condensed Muslim populations are heavily targeted, Muslims make up around 53% of French prisoners.[86]

There have been some government initiatives in the UK and France developed in an attempt to tackle the problem of radicalisation in prisons. In the UK, a programme set up through the government's 'Prevent' strategy aims to provide support for de-radicalisation efforts.[87] This programme targets mainly 15 to 24 year olds that are being drawn into Islamist extremism, though 10% of the cases are far-right extremists. The new UK 'Ibaana' programme is also recruiting Muslim prison chaplains to challenge extremist views of prisoners and provide religious direction, targeting the small number of prisoners with the most extremist views.[88] Individual sessions over several hours will be given to challenge theological arguments used to justify terrorism. This project commenced in April 2013 so its effect is yet to be seen.

Media

The media plays a critical role in shaping the discourse around terrorism, influencing how individuals understand extremism, terrorism and terrorists.[89] The media frames terms, sometimes changing their original context and meaning, and seeks to offer context to major international events and conflicts. They also select panellists and studio guests and thus have the ability to choose which perspectives on a given conflict or issue are aired.

[83] CIA World Factbook statistics from 2007.
[84] A Study conducted by the INED and INSEE in (October 2010) as reported in: Cosgrove, Michael (2011) 'How Does France Count its Muslim Population?', *Le Figaro,* 7 April.
[85] Gerard, Djamila (2012) 'La sur-représentation des musulmans dans les prisons françaises est très importante et indéniable', 10 october.
[86] Estimate given by Guéant, Claude Cited in: Djamila, Gérard, (2012), 'La sur-représentation des musulmans dans les prisons françaises est très importante et indéniable', *Riposte Laïque*, 10 October.
[87] Travis (2013) 'Hundreds of Young People have Received Anti-Radicalisation Support', *The Guardian*.
[88] HM Government (2013) 'Tackling Extremism in the UK: Report from the Prime Minister's Task Force on Tackling Radicalisation and Extremism', 4 December, *Crown Press*: London.
[89] Vliegenthart, Rens (2007) *Framing Immigration and Integration: Facts, Parliament, Mediab and Anti-Immigrant Party Support in the Netherlands*. Vrije Universiteit: Amsterdam.

The increased distribution and easy access to new media has had a huge impact on radicalisation. The term 'CNN Effect' has been coined to describe the influence of satellite news on intergroup conflicts in other parts of the world. As explained by Rens Vliegenthart, "a global conscience comes into being through the global mass media."[90] Crucially, the media plays an important role in influencing the popular image of minorities, how they are viewed within a country as well as how minority members view themselves.[91] Often derogatory depictions of a minority group lead to increased prejudice towards that group. Yet the media often picks up on more sensationalist topics that can negatively impact perceptions of minority groups. Dramatic headlines sell newspapers and the use of emotive language and inaccurate terms can lead to further confusion and the isolation of minority groups.[92]

Media portrayal of Muslims has been particularly important in framing Muslim identities in Europe in recent years. Since 9/11, Muslims in the media have often been depicted as either 'suppliers of oil or as potential terrorists', as some researchers have found.[93] Martin and Phelan argue that since the 9/11 attacks Western discourse has, in the main, connected the terms 'terrorism' and 'Islam'.[94] The media has a critical role in determining the discourse and subscribing meaning to such a pejorative phenomenon as terrorism.

Increasingly, Western media has framed terrorism within an Islamic context; this was particularly evident in the reporting of the Oslo attack in 2011. Before the identity of Anders Behring Breivik was known, UK papers reporting on the attack initially termed it as 'Norway's 9/11', referring to the unknown attacker as a terrorist. However, after it was discovered that he was a non-Muslim, the media rhetoric changed and he was subsequently referred to as a 'lone gunman or attacker' in many media outlets (see Example box 3.2).

[90] Ibid, p. 28.
[91] Cortes, Carlos (1986) 'Minorities: Insinuating Images Influence Perceptions', *Media & Values*, (35).
[92] (Public Perceptions about Minorities and Immigrants: the Role of the Media', (31 May 2011), *European Policy Centre*, (Event Report S49/11).
[93] Nacos, Brigitte & Torres-Reyna, Oscar (2003) 'Framing Muslim-Americans Before and After 9/11', Cited in: Norris, Pippa. Kern, Montague & Just, Marion. (2013) *Framing Terrorism: The News Media, The Government and the Public*, Taylor & Francis: London. p. 134.
[94] Martin, Patrick & Phelan, Sean (2002), 'Representing Islam in the Wake of September 11: A Comparison of US Television and CNN Online Messageboard Discourse', *Prometheus: Critical Studies in Innovation*, 20(3).

Example Box 3.2 Media Terminology Around the Breivik Attacks in Norway

On 22 July 2011, Anders Breivik bombed government buildings in Oslo, killing eight people. He then killed sixty-nine more people, mostly teenagers, in a mass shooting at a Workers' Youth League (AUF) camp on an Island off of Norway. In the headlines coming out before his identity was known it was assumed, without any real evidence, that the attacks were al-Qaeda inspired.

Examples of Headlines and Article Clips Prior to Knowledge of Breivik's Identity:


'AL-QAEDA' MASSACRE
NORWAY'S 9/11
'20 dead' in attacks Kids shot on island


The Telegraph
Home News World Sport Finance Comment Culture Travel
USA Asia China Europe Middle East Australasia Africa
France | Francois Hollande | Germany | Angela Merkel | Russia
HOME » NEWS » WORLD NEWS » EUROPE » NORWAY
Norway: 'At least 87' killed in terror attacks

(The Sun)

The Telegraph, (23 July 2011): *'*British security forces were immediately placed on alert amid fears that Norway's worst terrorist outrage might be the first in a series of attacks on the West. The carnage followed repeated warnings that al-Qaeda was planning a Mumbai-style attack on countries involved in the war in Afghanistan, where Norway has about 500 troops*.'*

Examples of Headlines and Article Clips After Breivik's Identity was Confirmed:


THE wire
what matters now
Media Reacts to News That Norwegian Terror Suspect Isn't Muslim


The Telegraph
Norway killings: The laughing gunman who shot 85 young victims, one by one

The Wire, (23 July 2011): 'Only later was the news released that the suspect taken by police, Anders Behring Breivik, was apparently a conservative, right-wing Christian with strong anti-Muslim and anti-immigration beliefs. Many in the media were left reeling over the fact that others were so quick to report and comment that Muslims were involved, before there was clear evidence.'

As seen by the above, UK coverage of the Breivik attack was quick to assume that the perpetrator was motivated by al-Qaeda and international wars being fought in places such as Afghanistan. This fabricated narrative was then debunked when more information came to light about Breivik, at which point the media narrative began referring to Breivik as a lone gunman with few further references to him as a 'terrorist'.

Research has found that European print media most commonly discusses Muslims in reference to terrorism.[95] An analysis of 974 UK news articles between 2000 and 2008 found that the most common nouns used in relation to Muslims were: terrorist, extremist, Islamist, suicide bomber and militant.[96] Whether inadvertently or deliberately, such strong media rhetoric does have implications and can help solidify certain negative stereotypes, which, in turn, can affect radicalisation trends. Previous research has shown that cohorts or groups given labels are more likely to behave in accordance with their proscribed labels.[97] Thus, assigning a particular group, i.e. Muslims, with the label 'terrorist' may subconsciously or consciously drive certain behavioural patterns.

Many individuals in the focus groups conducted for this report spoke out about their discontent with Muslim stereotyping, and the highlighting of the negative traits of certain Muslims in the mainstream media.

The problem is, although the voices of moderate, normal Muslims are out there, at the moment those who have the extremist views, they are the ones who are in the mainstream media... and those [radicals], that is what the media picks up on though. (Focus Group 1, Male, Age 25).

People are justified in saying that the media portrays us [Muslims] quite badly. Crime committed by individuals, the grooming of young girls in different parts of the country - the term Muslim is used and it goes back to [judging] faith and belief. And if the same thing happened with people with an English background it's not focussed on. I think reading comments on news links is often quite interesting. Those tend to be a bit more anonymous that you wouldn't dream of them saying to anyone's face. Very racist and bigoted. I think a lot of that has to do with media being subtle about it but throwing in a few terms relating to race and background. (Focus Group 2, Female, Age 28)

[95] Poole, Elizabeth (2002) *Reporting Islam: Media Representation and British Muslims*, (IB Tauris & Co: London).
[96] Moore et al, (2008), *Images of Islam in the UK: The representation of British Muslims in the National Print News Media 2000-2008*, (Cardiff: Cardiff University), p.3.
[97] Cicourel (1976) cited in: Moghaddam and Marsella, (2005), *Understanding Terrorism: Psychosocial Roots, Consequences, and Interventions*, American Psychological Association: Washington, DC.

People might think that Islam tells us to kill non-Muslims or something like that. That's like what the media shows and they might think that is what we believe and that we are bad people. (Focus Group 2, Female, Age 19)

With regards to the actual process of radicalisation, terrorism specialist Mathieu Guidère explained in an interview that the media can play a large role in the first spark, i.e. igniting an interest in a subject matter that can lead to radical pathways. Foreign fighters from Europe are often introduced to conflict zones through TV documentaries or news programmes. Individuals then seek further information either through friends, family members or online and, depending on the nature of their social circles, they can be directed to certain websites, video channels or social media accounts.

Once an individual has been exposed to extremist content online, it is easier to become immersed in one-sided propaganda, which the mainstream media narrative does not necessarily contradict. The appeal of the extremist message is subsequently enhanced by the fact that there are very few organisations that provide an outlet for young and impassioned individuals. This can, therefore, lead to more extreme organisations offering an outlet for discussion and engagement.[98]

Universities

Similar to mosques and prison environments, universities are also considered to be potential 'hotbeds' for radicalisation due to individuals being placed in a new environment where they are exposed to feelings of isolation and vulnerability.[99] Due to the different regulations and institutionalised practices in France, university-based radicalisation seems to be less of a concern. The French constitutional concept of *laïcité*, passed in 2004, requires the absence of religious involvement in government affairs as well as the absence of government involvement in religious affairs. Universities, as state-run bodies, do not incorporate religious organisations or student groups in the same way as the UK.

Thus, France and the UK are very different when researching university-based radicalisation. For this reason this section will focus solely on UK research and case studies, briefly going

[98] Interview with Mathieu Guidère on 3 March 2014.
[99] Rogers, Brooke & Neumann, Peter (2007) 'Recruitment and Mobilisation for the Islamist Militant Movement in Europe' *Kings College London*: London.

over current concerns for radicalisation within universities in the UK. Research carried out in 2005 found that twenty four separate UK academic institutions contained extremist and/or terrorist organisations using the campus facilities to recruit individuals and disseminate their messages.[100] In the UK there have been a number of cases where individuals attempted or carried out violent attacks after having been introduced to radical Islamist groups through universities.

Universities can be important in the initial stages of radicalisation since they provide a space where people who are likeminded can meet and develop their ideas. This environment can also lead people into certain crises of identity causing them to seek affirmation, which can be manipulated in times of identity development.[101] The number of individuals thought to have been radicalised in UK universities is extensive. Key UK cases shown in Table 3.2.

Table 3.2 Key UK Cases of University-Based Radicalisation

Name	University	Uni. Affiliations	Year caught	Plot/attack
Omar Sharif	Kings College London	Hizb-ut-Tahrir	2003	Tel Aviv Suicide bomber
Waheed Zaman	London Metropolitan University	Islamic society al-Muhajiroun	2006	Liquid bomb plot
Kafeel Ahmed	Queen Mary Belfast/ Anglia Ruskin Cambridge	Islamic Academy	2007	Glasgow international airport attack
Waseem Mughal	University of Leicester	Islamic Society	2007	Convicted of inciting murder for terrorist purposes overseas
Yassin Nassari	University of Westminster	Islamic Society	2007	Possessing documents to be useful to a terrorist
Mohammed Naveed Bhatti	Brunel University	Met recruiter in Uni. prayer room	2007	'Dirty bomb' plot
Umar Farouk Abdulmutallab	University College London	Islamic Society	2009	Failed bomb attempt of Northwest Flight 253

A study conducted by the *Centre for Social Cohesion* showed that the majority of Muslim students across UK campuses have tolerance towards other minorities, reject violence in the

[100]Glees, Anthony & Pope, Chris (2005), *When Students Turn To Terror: Terrorist and Extremist Activity on British Campuses*, Social Affairs Unit: London.
[101] Precht, Tom (2007) 'Home Grown Terrorism and Islamist Radicalisation in Europe: From Conversion to Terrorism', *Danish Ministry of Justice.*

name of their faith and support Britain's secular and democratic society.[102] However, the same study also showed that student association with Islamic societies (ISOC) on campus led to a higher likelihood of more conservative, and sometimes extremist Islamist views. The study, which focused on ISOCs, found that in 2010 active members of ISOCs were more than twice as likely to say that killing in the name of religion was justifiable. Active members were also almost three times more likely to believe that Muslims who leave Islam should be punished under Shariah law and a majority of active members supported the introduction of a worldwide Caliphate.[103]

There is a constant struggle within universities to decide what should and should not be allowed to take place on campus. In a democratic society that upholds freedom of speech, it remains difficult to decipher the line between contentious discourses, which is welcome in the marketplace of ideas, and hate speech, which is illegal. However, it does seem like universities have been made aware of the sensitive issue of on-campus radicalisation. In focus groups most participants that were in, or had just left, university said that they had not experienced extremist groups on campus. However, some did mention that the existence of such groups was dependent on the university.

I didn't hear any extremist groups. They were pretty much banned on campus... But maybe it depends on the university. City University was quite radical. The ex-Islam president (meaning ex-president of ISOC) is vocal. The underpants bomber went to UCL. But from what I hear he was fairly OK on the surface. (Focus Group 2, Male, Age 25)

As the quotation above shows, it also seems that the salience of a radicalised group on campus is highly dependent on an individual or small active group of individuals following more extreme Islamist ideologies.

The preceding discussion sought to explore the manner in which four primary socialising agents act as spaces in which the first sparks for the radicalisation process can be initiated. As was mentioned, once the fuse has been lit curious individuals seeking to develop their knowledge begin to search for other means through which they can learn more about their

[102] (2010), *Radical Islam on UK Campuses: A Comprehensive List of Extremist Speakers at UK Universities*, Centre for Social Cohesion: London.
[103] Ibid.

newfound ideas. In light of the fact that the Internet is rarely, if ever, the first spark for the radicalisation process, Section 3.3 analyses the exact role the Internet plays.

3.3 The Role of the Internet in Radicalisation

As discussed in the first section of this chapter (3.1), the Internet does not play as big a role in the initial introductory radicalisation process as often suggested. While the Internet is rarely, if ever, the initial spark it still plays a crucial role in contemporary Islamist radicalisation trends. However, the precise nature of that role needs to be contextualised and understood. Concerning Islamist radicalisation, the Internet is used in three ways:

- To **indoctrinate**: deconstructing previous beliefs in order to be able to proselytise and re-educate individuals to be less critical of Islamist extremist doctrines.
- To **teach** about Islamist ideologies: providing learning tools, lectures and educational resources.
- To **socialise**: solidifying the radical Islamist ideology by providing a sense of community, like-minded individuals and media that conform to the radicalised narrative.

The first spark, as discussed in section 3.2, is usually caused by human contact or through real-world experiences. Online extremist content is not so easy to find and usually individuals are already on a journey towards extremism before they seek it out. Once such individuals do encounter extremist content, it can help facilitate radicalisation in the ways mentioned above, which will now be elaborated upon.

Indoctrination

The Internet plays a key role in indoctrination because it creates a variety of opportunities for extremist groups to create platforms for their beliefs that are free of any external critique. These platforms do not allow them to control the message but facilitate indoctrination by offering a manufactured consensus through a virtual world that provides its own media, social world and education. In an attempt to further the indoctrination process for non-traditional audiences, some Islamist extremist activists are developing a

myriad of avatars and profiles to show solidarity and widespread support for a set of extremist beliefs. As explained by Lisa McInerney, an expert on terrorism and the Internet:

We have seen a selection of user profiles online. Some people are using multiple profiles for different audiences. A few years back, we had a case of an individual who was supposedly a fifteen year-old US high school student... We reckon she had at least six different YouTube profiles.[104]

Indoctrination can take place in a number of ways; individuals can either indoctrinate themselves through uncritical consumption of extremist materials, or individuals may come into contact with an online recruiter that aids and assists the indoctrination process. Of course, it can be a combination of the two as well. With regards to the uncritical consumption of extremist materials, this is made easier if individuals buy into the notion that mainstream media and non-extremist sources of information are biased and agenda driven. Hence, extremists also seek to deconstruct mainstream narratives, attributing nefarious motives and pointing to the vested interests of those that produce them.

Beyond extremist propaganda, scepticism of mainstream media sources is widely shared. Some of the participants in focus groups felt that online sources often provided an alternative and more trustworthy reading of world events. As participants explained:

I think people turn to the Internet so much for alternative...as an alternative source although they run into conspiracy theories, the reason they turn to the Internet is because they don't trust the mainstream media at all. I know I don't. (Focus group 1, Female, Age 19).

I get my news online, and never watch any mainstream news....All mainstream media here and in America and pretty much everywhere, how much of that is true? Because there is a whole other world going on, the independent media online which sets a completely different story. (Focus group 1, Female, Age 26).

The uncritical consumption of extremist propaganda videos is a very interesting phenomenon, especially since video-sharing platforms automatically recommend similar videos, and by default channels, after one has been viewed (discussed in Chapter 2). Mathieu Guidère, an expert on the psychology of radicalisation and terrorism, states:

[104] Interview with Lisa McInerney on 5 February 2014.

Because he doesn't want to really read, he doesn't have the time to read, he hasn't the culture of reading... He begins to watch [videos] 1 and 2 and 3 and 4 and 10 and 20. And after three or four hours of watching he is actually taken into a network, or rather a sub-network.... He doesn't know that the suggested videos by the system are from the same source or from the same group or they're about the same group... The image, or video would be so traumatic that he enters in a new phase, the humanitarian phase. He wants to act.[105]

As seen from this descriptive narrative, an individual can easily end up in a self-created echo chamber of indoctrination with extremist videos. They are easy to consume, easier to find than extremist websites and the use of images, theme music and footage make them much more impactful. There is also currently a severe lack of content on YouTube that challenges the extremist content through counterspeech.

The most well-known examples of indoctrination propaganda are al-Qaeda's online magazines. *Inspire* was the first widespread English-language propaganda magazine that emerged in 2010, which included instructions on how to make weapons and bombs at home. More recently the newer al-Qaeda magazine, *Resurgence*, has used Malcolm X quotations to appeal to disaffected Muslims in the US and Europe. *Resurgence* appeals to raw emotional responses to the perceived Muslim victimhood around the world.

106

[105] Interview with Mathieu Guidère 3 March 2014.
[106] Image from a reposted video launching *Resurgence Magazine*, reposted by (@matthewkeyslive).

As mentioned in an article about the reappearance of the new al-Qaeda magazine, Magnus Ranstorp, a terrorism expert at the Swedish National Defence College, said that the publication used English to direct its attention to non-traditional recruits. Messaging was aimed primarily at second and third-generation immigrants that were more fluent in English than other languages. Magazines and other content of this nature indoctrinate more effectively by relating to individuals on their level and providing educational resources for operational usage.

Teaching

Primarily, the Internet is a place for teaching, allowing individuals to search and investigate almost any topic they can think of. Large quantities of the videos and web links that are produced in support of Islamist extremist narratives have an educational purpose. However, as confirmed in our interviews with a range of Internet, terrorism and radicalisation experts, extremist content is often sought out by those seeking specific content or answers to specific questions. As such, it is not something that one accidently stumbles upon.

There is an inherent duality in Islamist extremism, with one side focussed on theological re-interpretation and the other on political justifications for violent jihadist actions. Subsequently, extremist material produced for educational purposes also reflects this duality. As mentioned by Alberto Fernandez, coordinator of the Center for Strategic Counterterrorism Communications (CSCC):

There is radicalisation occurring as a result of deep searching regarding religion. Then there are people who are attracted to this thug life style, where it is about an attitude or rebel life style.[107]

With regards to religious teaching, there are thousands of videos available providing sermons and speeches given by extreme Islamist preachers who speak on topics such as the call for a Caliphate and give their interpretations of the Quran, promoting a more extreme version of Islam. The consumption of these videos has been mentioned by many convicted and former extremists and jihadists who have justified their violent actions through extremist ideology, as shown by the various 'lone wolf' cases analysed in Section 3.1. The

[107] Interview with Alberto Fernandez on 12 February 2014.

Internet is the perfect platform for non-traditional teaching that would not be allowed in most mosques or places of worship.

The line between indoctrination and teaching is also often blurred in online Islamist radicalisation. Within publications, like *Resurgence* and *Inspire*, there has been an increase in people who may not be willing to fight, but are part of extremist Islamist circles that sympathise with the narrative.[108] The manner in which this educational material is marketed means that it can reach a wide range of people including, more generally, those harbouring anti-Western or anti-capitalist sentiments.

The more obvious extremist teaching content provides for the fully radicalised individual who wants to engage in more violent forms of jihad. The usage of this material is much more limited; however, as seen from Section 3.1, those wanting to commit violent acts of terror can use the Internet to find supportive resources. Resources can also be found in the form of assisting individuals in raising funds for terrorist acts.

Socialisation

Socialisation is the 'the means by which social and cultural continuity are attained'.[109] Socialisation taking place on the Internet plays a key role in solidifying extremist ideologies and ideas within the process of radicalisation. Agents of socialisation working online are using: 1) religious teaching content, mentioned above, 2) radicalised media content and 3) social networking platforms. Combining education, media and a social sphere, individuals can immerse themselves in an online world which supports the Islamist extremist agenda without incorporating any rational or mainstream counter-narrative.

Social movement theorist Quintan Wiktorowicz argues that: "violence comes after an intense socialisation in which perceptions of self-interest diminish and the value of group loyalties and personal ties increase".[110] The Internet in particular has allowed individuals to create 'social-spatial enclaves'[111] which enable people to form online 'in-groups' based on

[108] Burke, Jason (2004) 'Think Again Al Qaeda' Foreign Policy, 142, (May- June), p.18.
[109] Clausen, John A. (ed.) (1968) *Socialization and Society*, Boston: Little Brown and Company. p5
[110] Wiktorowicz, Quintan (2004), *Islamic Activism: A Social Movement Theory Approach,* Indiana University Press.
[111] Sanderson, D. & Fortin, A. (2001) 'The Projection of Geographical Communities into Cyberspace' in Munt, SR. ed. *Technospaces: Inside the New Media* Continuum: London.

shared interests and ideologies. Thus, facilitating an 'echo chamber' and furthering the possibility of group cohesion or 'group think'.[112]

The use of social media by extremist groups is relatively new but rapidly developing. According to Dominique Thomas, a researcher of Islamist movements, the diffusion of information and propaganda online is in its own way creating a virtual territory for an Islamist state.[113] The aim of developing online spaces is, therefore, not as much about direct recruitment but about creating a sphere of influence and sympathy or, put in other words, an 'imagined online community'.[114] As mentioned by a variety of other experts and mentors looking at radicalisation, the Internet opens up a world to people, providing them with a social circle that is much larger than their offline reality.

According to Mathieu Guidère, in the process of radicalisation, teaching oneself can lead to indoctrination, which can subsequently facilitate multi-agent socialisation. Once an ideology has been socialised, strengthened by education, media and a social subculture, factors that lead to activism can be more easily instigated. It is, therefore, important to broaden the scope for developing counter narratives to address online education, media and social networks. As discussed by Alberto Fernandez:

There should be a growing of the wider circle of partners, working with Muslim groups, civil society groups, and NGOs. [The government] has a digital presence [Digital Outreach Team] and other groups need to do the same. There is mass of radicalising material online that is there forever. There is more bad stuff than good stuff. We need to grow the mass of the counter arguments. Governments can do that, but it is better done with a multiplicity of actors. We need to grow additional voices and people.[115]

Summary

The Internet plays a crucial role in our everyday lives and, as our reliance on the Internet increases, it is only natural that the usage of the Internet by extremists, trying to spread their message and expand their following, will also increase. However, as the first part of this chapter discussed, there is little to no evidence showing that individuals are radicalising

[112] Janis, Irving (1983) *Groupthink: psychological studies of policy decisions and fiascos, Houghton Mifflin.*
[113] Alonso, Pierre (2012) 'Twitter: The New Frontline in Global Cyber-Jihad', *OWNI.eu*, 10 January.
[114] Ibid.
[115] Interview with Alberto Fernandez on 12 February 2014.

online without any contact or information given prior by real-world interactions or experiences. ‘Lone wolves’ very often have had some form of contact with other individuals and also, in many cases, have previous records of mental illness or drug abuse, making them vulnerable to counter cultures. For the few that have seemingly been completely radicalised online many questions about real-world influences remain.

While this report focuses on the Internet’s role in the process of radicalisation, there remain many real-world ‘hot-spots’ for radicalisation that need public and private attention. Some of these areas, such as mosques, seem to be aware of previous radicalising activities and have made conscious efforts to eradicate the more extreme elements from their religious spaces. However, there is great potential for the development of youth-outreach programmes in mosques and within schools. It would be highly beneficial to better develop religious teaching spaces that provide young Muslims with a moderate discourse around contemporary topics, openly addressing areas that extremists currently monopolise through their online activities.

The same learning and sharing environment would be beneficial within universities and the introduction of more moderate imams in the prison system would also be hugely helpful in countering extremist narratives used to indoctrinate inmates. The media and its inadvertent or deliberate typecasting of Muslims as extremists and terrorists also contributes to the process of radicalisation, solidifying negative stereotypes. There is room to develop accountability and better usage of terminology when reporting on sensitive social and cultural topics or violent acts, whether conducted by Islamist extremists or other violent actors.

The Internet’s role within the process of radicalisation, subsequently, takes on different forms, both reacting to the real-world and creating its own idealised world online. Once an individual’s interest around radicalised topics has been primed, the Internet has the potential to provide the rest, indoctrinating, teaching and socialising extremist ideologies.

Chapter 4. Existing Counter-Extremism & Counterspeech Measures

As previous chapters have discussed, regardless of whether or not the Internet is the 'first spark' of radicalisation, Islamist extremists are increasingly using the Internet and online tools to their advantage. Therefore, it is necessary to explore initiatives that are currently underway to counter their efforts. These efforts, which shall be critically examined in this chapter, can be divided into two broad categories:

- **Negative measures**: counter-terrorist and/or counter-extremist initiatives, which block, filter, take-down or censor extremist content online.
- **Positive measures:** counter-extremism initiatives that seek to challenge extremist narratives and propaganda by producing counterspeech online.

Currently, there is a national debate around the efficiency and the implications of censoring the Internet, especially when the material in question blurs the lines between legality and illegality. While negative measures are frequently scrutinised by researchers and academics, the quality and nature of online counterspeech materials also need examination. This chapter reviews current efforts countering online extremism in the UK and France with a view to identify what works best and what more needs to be done.

The first part of this chapter reviews the online usage of negative measures in their various forms, before analysing the various pros and cons of using negative measures for furthering counter-extremism and counter-terrorism efforts. The UK and France both remain primarily free, democratic nations, opposed to impeding freedom of speech. However, both countries have slightly different stances towards the usage of negative measures, which will also be discussed.

The second part of this chapter reviews the online usage of positive measures and goes over some of the larger projects currently trying to counter online extremism through content production and counter-narrative development. This is a much newer field that has just started developing in the private and public sectors in recent years. The report then goes on to discuss what form positive counter-messaging is currently taking and where there is room to develop and encourage a growth in this field in the future.

4.1 Censorship and Negative Measures

The issue of censorship is central to the debate about how to counter extremism online. A wide range of negative measures, designed to restrict access to extremist content, have been developed internationally using increasingly sophisticated techniques. The usage, motives, scope and effectiveness of Internet censorship varies highly from country to country. European countries are less likely to introduce large-scale, centralised censorship. However, even in Europe there are certain forms of filtering, blocking and site take-downs taking place.

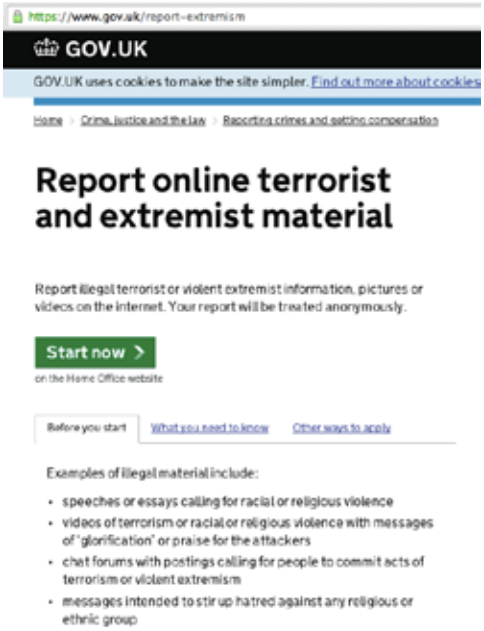
There is a constant struggle for governments to uphold their support for the freedom of expression while also protecting the public from online content that might disseminate hate speech, incite violence or support terrorism. While some national filtering is culturally specific (for example France and Germany filter and block content that is related to Nazism or Holocaust denial), other filtering trends are European-wide and have been put forth as initiatives on a European Union level (such as the filtering and attempted eradication of Child Sexual Abuse Imagery – CSAI).[116] Emerging trends are showing increased filtering as more people in more places use the Internet increasingly in their daily lives.

In the British context, filtering Internet traffic with a view to blocking access to extremist websites would be enacted primarily at the Internet Service Provider (ISP) level. Discussions around the topic of large-scale filtering of 'extremist content' are gaining support in government circles.[117] However, filtering content on the basis that it is deemed 'extremist' is highly problematic since one can promote an extremist worldview without breaching national or international laws.

British and French governments have even set up online portals in recent years which allow members of the public to anonymously report potentially illegal sites and/or materials. These official portals allow individuals to report content that they believe to be contentious and illegal. While these portals provide an outlet for civilians to flag material they believe to

[116] Zittrain, Jonathan & Palfrey, John (2008), 'Introduction', in Deibert, Ronald et. al. (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering*, MIT Press: Cambridge, pp. 1-4.
[117] HM Government (2013) 'Tackling Extremism in the UK: Report from the Prime Minister's Task Force on Tackling Radicalisation and Extremism', 4 December, *Crown Press*: London

be illegal there remains significant dispute over what can be deemed 'extremist' and subsequently fall under filtering regulations. Furthermore the adoption of an agreed definition of extremism is deeply problematic.



The above images show the web portals for the UK and France that allow the public to submit online materials, websites and video links that they feel are illegal. In the UK the public website link can be found at <www.gov.uk/report-extremism> and in France the link is found through the Ministry of the Interior at <www.internet-signalement.gouv.fr/PortailWeb/planets/Accueillinput.action>.

Some government officials in both the UK and France view the Internet as an easy target in the fight against extremism with censorship being viewed as the key tool. Whilst very few oppose the removal or blocking of clearly illegal content, the practicality and effectiveness of negative measures used to counter extremist narratives is hotly disputed with most experts in the field opposing such initiatives. According to an ICSR report: "...the systematic, large-scale deployment of negative measures would be impractical, and even counterproductive: it would generate significant (and primary political) costs whilst contributing little to the fight against violent extremism."[118] Similarly, a report by the Bipartisan Policy Center states "...censoring the Internet is rarely effective" and "the filtering of Internet content is impractical in a free and open society."[119]

An analysis of key negative measures used to combat undesirable online material, namely removing content and restricting access, and ways in which they can be overcome, seems to justify the stance taken in the reports quoted above. These measures include:

- Removing websites
- IP filtering
- Domain name filtering
- Content filtering
- Hybrid IP and proxy filtering
- Hiding websites

Removing Websites

Removing websites entails asking hosting companies to take down websites or domain name authorities to deregister domains being used by websites. Currently in the UK the Counter Terrorism Internet Referral Unit (CTIRU) asks hosting companies and domain name authorities to take down websites that are in breach of the Terrorism Act 2006, which outlaws the glorification and incitement of terrorism. The CTIRU also has an online reporting

[118] Stevens, Tim & Neumann, Peter (2009) 'Countering Online Radicalisation: A Strategy for Action', *ICSR*: London. p. 15.
[119] Ibid. p. 23.

mechanism for websites suspected to be in contravention of the law and has, thus far, removed over 29,000 pieces of illegal terrorist propaganda in the last three years.[120]

If the content the CTIRU wishes to remove is outside of the UK government removal jurisdiction the CTIRU flags the material to the platform the material is hosted on. For example, the CTIRU may flag a video that it finds to breach terrorist laws and the video-hosting site will subsequently review the material and take a video down if it is found to be illegal.[121] Online hate speech and incitement to violence are also of concern to the CTIRU and can also lead to censorship. France has similar mechanisms, such as *Haplopi 2*, which allows content providers to conduct online surveillance, thus creating a precedent for censorship.[122]

However, these measures of censorship rely on hosting companies and domain name authorities to be based in the same legal jurisdiction as the government that is making the request. This can be problematic since website operators are free to move their sites and have them hosted and registered in different countries or jurisdictions, rendering British or French authority over them obsolete. In fact, the two services that websites rely on, hosting and domain name registration are readily available from anywhere in the world. In many cases companies choose to voluntarily comply with government regulations when such requests are made.

This was exemplified in the LICRA vs. Yahoo court case in 2000 when French courts demanded that Yahoo block Nazi materials. In 2001, a US District Court Judge held that Yahoo could not be forced into compliance with French laws since this would violate its right to freedom of expression under the First Amendment of the US Constitution. The US Supreme Court also refused to consider an appeal to this mandate.[123] Whilst larger responsible organisations, like Yahoo, voluntarily comply with laws in the UK, other foreign organisations hosting websites may not.

[120] Brokenshire, James (April 2014), 'House of Commons: Oral Answers to Questions 10 March 2014', *House of Commons*, (Section on Extremism) See also: HM Government (2013) 'Tackling Extremism in the UK: Report from the Prime Minister's Task Force on Tackling Radicalisation and Extremism', 4 December, *Crown Press*: London.
[121] Clark, Liat (2014), 'UK gov wants unsavory web content censored', *Wired,* (15 March).
[122] Index on Censorship (2013) 'France: Strict Defamation and Privacy Laws', 19 February.
[123] (12 January 2006), '9th Curcuit En Banc Panel Rules Against Yahoo in French Internet Censorship Case', *Tech Law Journal.*

Removed websites can quite easily reappear within a short space of time and, therefore, censorship measures work effectively only as a form of temporary disruption. Overcoming this obstacle would require an international treaty or memorandum of understanding between different nations, which, for the matters discussed in this report, would also require the adoption of a formal definition of 'extremism'. Previous international attempts to arrive at universally accepted definitions of even more definitive terms such as 'terrorism' have proved futile as different countries have differing political priorities. Schmid and Jongman cited 109 definitions of terrorism used by academics and politicians, highlighting the ambiguity underlining the term. [124] This along with other obstacles to website removal renders censorship measures around 'extremist content' highly problematic and ineffective in the long run.

Internet Protocol (IP) Filtering

Online filtering creates settings that monitor and control what websites can or cannot be accessed by a computer or set of computers. Since the majority of online traffic goes directly through Internet Service Providers (ISPs) in the UK and France, these can act as virtual bottlenecks through which the flow of information can be filtered.[125] With regards to domestic Internet usage, family safety settings that rely on Internet filters have been introduced to help parents manage the content accessible to their children.

Every website needs to attach itself to an IP address in order to be searchable and accessible. Filtering via IP address involves having ISP routers block access to websites that use blacklisted IP addresses. In a Western democratic context, family filter settings are often available to parents through their service providers. In its most basic form, IP filtering is a relatively straightforward method and can be used to block access to sites that are not hosted in the country that is seeking to block them, thus, cannot simply be removed.

However, filtering Internet traffic, in general, is fraught with difficulties and many of the filtering technologies have been deemed "...either too crude or too expensive to

[124] Schmid, Alex and Albert Jongman (1988) *Political Terrorism*, Rutgers University, New Jersey.
[125] (2009), *Countering Online Radicalisation: A Strategy for Action*, (ICSR, London).

operate."[126] Broad IP filtering comes under the 'too crude' category since it can affect perfectly legitimate websites that are using the same IP address as a blacklisted site. Livingston's study found a political bias in AOL's filtering measures for 'young teens', inadvertently blocking access to the Democratic National Committee and Green Party websites', whereas access to the Republican National Committee Website remained.[127]

Over-blocking could result in legal challenges if businesses or organisations are unfairly blocked, or brands feel their image has been unfairly tarnished. It could also create political controversy if certain communities or groups feel they are being unfairly targeted and a disproportionate number of sites associated with an otherwise benign section of people are being filtered. The Gay and Lesbian Alliance against Defamation (GLAAD) have cited a significant number of examples where filtering of sexually explicit content has led to the over-blocking of legitimate sites. A GLAAD report found that AOL parent controls blocked websites such as 'Children of Lesbian and Gays Everywhere', as well as a number of websites of national organisations which had 'gay and lesbian content'.[128]

As seen in the recent introduction of widespread filters for legal pornography in the UK, a number of sex education and advice services websites were wrongly targeted.[129] BBC's Newsnight reported on three different Internet providers (Virgin Media, TalkTalk and Sky) that used content filtering in an ineffective manner, preventing individuals from accessing sexual health advice.[130] TalkTalk classified the Edinburgh Women's Rape and Sexual Abuse Centre as 'pornographic', BT had blocked access to the website for the Doncaster Domestic Abuse Helpline and Sky blocked access to six websites that help people overcome their porn addictions. Although efforts are being made to prevent existing filtering methods from blocking legitimate sites there remains no encompassing solution to over-filtering.

[126] Neumann, Peter (2012) 'Countering Online Radicalisation in America', *Bipartisan Policy Center*: Washington DC. p. 24.
[127] Livingston, Brian (2000) 'AOL's 'Youth Filters' Protect Kids from Democrats', 24 April, *CNet News.* Cited in: Heins et al (2006) 'Internet Filters a Public Policy Report', Brennan Centre for Justice.
[128] (1999) 'Access Denied, Version 2.0: The Continuing Threat Against the Internet Access and Privacy and its Impact on the Gay, Lesbian, Bisexual and Transsexual Community'; Cited in: Heins et al (2006) 'Internet Filters a Public Policy Report', Brennan Centre for Justice.
[129] Note: Both the UK and France filter for child pornographic content. With reference to overfiltering see: (18 December 2013), Smith, Mike Deri, 'Porn Filters Block Sex Education Websites', *BBC Newsnight*.
[130] Ward, Mark (2014) 'UK Government Tackles Wrongly Blocked Websites', *BBC News*.

Domain Name Filtering (URL Filtering)

Domain name filtering involves blacklisting certain domain names so that computers are unable to find the content associated with blacklisted domains. This would be the names associated with the website title that one types into the search bar. When an individual searches for a domain name on a search engine a corresponding IP address is also sought. If an ISP has been instructed to block a domain name computers will link to an ISP server instead, which will display either an error page or a page recommending other sites. Thus, searches for content residing under the blacklisted domains will not be found.

This form of filtering also has the effect of over-censorship since the website could be part of a larger domain that involves other websites or web functions, such as blogging platforms. Furthermore, this form of filtering can be circumnavigated by determined users if they know the IP address of a specific website, which they can use to find the site. Alternatively, they can use servers located in jurisdictions where domain name filtering is not being applied in order to access blocked sites.[131] In fact, it is now possible to easily install applications that allow computers to behave as though they are in a different country and subsequently, evade national filters.[132]

Content Filtering

Content filtering involves blacklisting certain key words and using software to drop requests for websites that contain them. This is also a crude, not to mention expensive, method that can have the effect of blocking access to legitimate content, as mentioned previously. The software that filters content needs to maintain a framework that can determine when otherwise blacklisted content is allowed. This entails a hybrid model of application by technology-based filtering as well as teams of individual monitoring filtering outcomes. This method not only slows Internet speeds but is also highly expensive if human resource teams, going through affected content, are added.[133]

[131] Ryan, Jonathon (2007) *Countering Militant Islamist Radicalisation on the Internet*, Cromwell Press, Trowbridge, p. 91.
[132] Schneier, Bruce (2013) 'Evading Internet Censorship, Schneier on Security'.
[133] Previous research from ICSR as well as other negative measures reports discusses the cost of such measures further: Neumann (2009) *Countering Online Radlicasation: A Strategy for Action* (ICSR), p. 17.

Furthermore, either a government agency or a team within an ISP will have to maintain a list of content and sites that are deemed worthy of being blocked and a framework that determines when, and in what context, they are allowed. In either case, government-imposed filtering regulations and a list of censored sites must be made public and that could lead to a public debate about censorship. A public debate, in turn, can give unwanted exposure to otherwise fringe organisations or sites that gain kudos by being deemed worthy of censorship. Further to this, debate could lead to unnecessary attention being given to a minority of extremists, thus elevating them to a celebrity status. It could also push online extremists into the darker recesses of the web, where monitoring and countering content is much more difficult.

Proxy Filtering and Hybrid IP and Proxy Filtering

Two further methods that overcome some of the hurdles facing the aforementioned methods are also available, namely proxy filtering and Hybrid IP and proxy filtering. Proxy filtering relies on ISPs using proxy servers, which produce local copies of popular websites, to determine whether or not requests for certain web pages should be allowed.[134] Hence, it can be viewed as a more refined version of domain name filtering. Whilst this method can avoid over-blocking, it is very expensive, relying on a significant hardware investment, and it slows Internet traffic down considerably.[135]

Hybrid IP and proxy filtering seeks to combine IP filtering with proxy filtering so that IP addresses are checked first, without being blocked. Subsequently, IP addresses deemed suspect are passed onto proxy servers which, in turn, block sites that are deemed to contain blacklisted content. Thus, at the IP level over-blocking is avoided and at the URL level, proxy servers have fewer requests to deal with and content to analyse, which means Internet traffic is not affected in any significant way. However, whilst this method is much less crude, it still relies on maintaining a list of blacklisted content which, as discussed earlier, is deeply problematic.

[134] Stevens, Tim & Neumann, Peter (2009) 'Countering Online Radicalisation: A Strategy for Action', *ICSR*: London p. 18.
[135] Travis, Alain (2012) 'MP Call Communications Data Bill 'Honeypot for Hackers and Criminals', 31 October, *The Guardian*.

Hiding Websites

Online extremist content can also be hidden from users by manipulating the way in which search engines present the results of a search. As discussed in Chapter 2, when a search engine is used, an algorithm, which ranks sites by relevance, presents websites that are related to the words searched. Controversially, algorithms could be manipulated so that searches for extremism-related content are dropped and only results that do not include extremist websites are returned. Alternatively, the algorithm can be manipulated so that extremist websites feature much lower down in searches.[136] However, as discussed, the problem with this strategy is defining and ring fencing what would be deemed 'extremist'.

This kind of manipulation is also a form of content filtering and, therefore, a list of blacklisted content needs to be maintained, with all the drawbacks such a list carries. Even then, if users are aware of the exact web address they wish to access, they can still find the websites they want by simply typing addresses into the address bar.

In spite of these obvious drawbacks, the key problem for this method is that extremist websites are usually arrived at through links from other sites or through private recommendations rather than random searches. As such, those that frequent them usually know what they are looking for and are determined to find it. As shown in Chapter 2, extremist websites currently do not feature very prominently in searches for terms such as 'jihad' or 'mujahideen'. Even a search for 'al-Qaeda' in Google brings back no extremist related content in any of the top search results. Thus, manipulating searches offers limited practical utility, yet raises a series of moral and ethical issues.

The Ineffectiveness of Negative Measures

The negative measures discussed so far would only affect static websites and materials that are openly accessible. They are unable to affect more active online functions or areas of the dark web that can easily avoid tracking. This is highly problematic based on the active Internet usage by extremist organisation discussed in Chapter 2. In truth, extremists use a wide range of social media, blogs, instant-messaging applications and video-sharing sites to promote their messages. An example of this is illustrated in Example Box 4.1. Web tools,

[136] Manber, Undi (2011) 'Google Lied about Manual Changes', *SEO Black Cat* (4 February).

such as Twitter, Facebook, Reddit or instant messaging and chat sites, offer more interactivity and are more effective as a means through which extremist content can be shared and discussed. Not only are negative measures problematic for the logistical reasons discussed previously, but they also are inadequate, if not entirely ill-equipped, to target active Internet usage on non-static platforms.

Policing or removing content that is embedded in privately owned platforms is highly complex since such platforms rely on user-generated content and already have their own service user agreements in place. The extent to which governments can interfere or dictate what content private sector organisations host is limited in a free society, especially when those companies are based in a variety of legal jurisdictions. The option of banning such platforms altogether is not a step any free society should be prepared to take.

Indeed, there are countries that have sought to ban social media platforms altogether. Twitter and YouTube are currently banned in China, Iran and North Korea whilst YouTube alone is also banned in Pakistan, Eritrea and Turkey. The success these countries have had in maintaining such bans is highly questionable; especially since proxy servers are frequently used in countries such as Pakistan to circumnavigate YouTube bans.[137] Turkey attempted to introduce a ban on Twitter; however, means to circumnavigate the ban were openly promoted by activists across Turkey. Turkish citizens were also able to get around the ban using a virtual private network or by using Tor, a service that hides the location and browsing habits of a user.[138] Subsequently, the Twitter ban was lifted by the Turkish Supreme Court, who deemed that the ban was a breach of free expression.[139]

Furthermore, the political systems in these countries are not ones the UK and France should be aspiring to emulate since press freedoms, minority rights and transparent governance are not features of such countries. It is also highly unlikely that the British and/or French government will have the willingness or ability to police people's opinions in this manner, hence such platforms should only remain open and free in democratic societies.

[137] Aziz, Farieha (2013) 'Bolo Bhi Amicus Reports on YouTube Case Hearing', *Bolo Bhi*, (1 May).
[138] Hilburn, Matthew (2014) 'Turkey's Twitter Ban Backfires as Millions Find Workarounds', *Voice of America: Middle East*, (March 21).
[139] (2014), 'Officials in Turkey lift Twitter ban', *BBC World*, (3 April).

However, even when service user agreements of privately owned platforms are violated and accounts held by extremists are suspended, extremist content and messages are still disseminated. As discussed in Chapter 2, the Somali terrorist group al-Shabaab has managed to maintain English-language Twitter accounts and, in its own words, used them to "vigorously challenge defamatory reports in the media by presenting an accurate portrayal of the current state of Jihad in Somalia."[140] These accounts have been suspended by Twitter on numerous occasions, yet have managed to reform each time under different guises, as seen previously in Example Box 2.6.

Other active social networking sites, such as Paltalk, have played a substantial role in extremist actions as seen in Example Box 4.1. In fact, the most dangerous usages of the Internet, leading to acts of terrorism, have often been through the operational usage of such sites. These social sites are often politically neutral in the UK and France, and their platforms are open to being used in a variety of ways. Thus, knowledge of how they have been used has only come to light in the aftermath of terrorist attacks. Since platforms consist of user-generated content, the only way extremist content can be fully eradicated would be by closing the entire platform down, which is both a drastic and unwanted measure. Thus, whilst governments focus efforts on static websites, these active platforms are not affected by proscriptions.

[140] Mohamed, Hamza (2013) 'Al-Shabab Say they are Back on Twitter', *Al Jazeera*.

Example Box 4.1 Paltalk used as a tool to promote extremism

Paltalk is a free downloadable application developed in 1998 that enables Video Chat Room capacities. Paltalk is the integration of video, audio and texting options within a chat room setting. In order to use Paltalk, individuals must complete a registration form. Once registered the Paltalk application can be added to any desktop, fixed or portable computer. Paltalk is just one of the chatroom spaces that has been utilised by radical Islamist groups. Besides implementing Paltalk onto specific Islamist websites so that like-minded followers can privately interact online, Paltalk has also been used to track and harass non-Muslims. One of the most famous of these cases was in 2005 when the password protected radical Islamist website <www.barsomyat.com> was found to be systematically tracking Christians on Paltalk. The site featured pictures and information on Christians that had been active in debating Muslims on Paltalk. A man from New Jersey received death threats for two months in the lead-up to the murder of him and his family. [141]

Paltalk has also been used extensively by notorious hate-preachers Omar Bakri Muhammad, leader of al-Muhajiroun, and Abdullah el-Faisal, in order to encourage British Muslims to take up arms.[142] Nine would-be British terrorists, who were plotting to blow up the London Stock Exchange and US Embassy in London in the run up to Christmas in 2010, established contact over Paltalk and were believed to have been inspired, at least in part, by al-Muhajiroun and Abdullah el-Faisal. [143]

Fighting extremism online is also not analogous to fighting child abuse online, as some have argued. Child Sexual Abuse Imagery (CSAI) is unquestionably and uncontroversially illegal, regardless of context and legal jurisdiction. Extremist content, on the other hand, is much more debateable and can be legal in a variety of contexts, for example placed within a news broadcast or within an academic platform. Furthermore, it is possible to hold and express viewpoints that are supportive of Islamist extremism in many jurisdictions. The same can not be said for CSAI. Therefore, the lessons learnt from the fight against online child abuse do not apply.[144]

However, when it comes to websites discussing, debating or even promoting ideas that are deemed extreme, there are some very real intellectual debates to be had and engagement is both viable and useful. Such engagement and access to extremist viewpoints also informs the work of counter-extremist organisations who use this information to develop counterspeech. In a free and democratic society that cherishes intellectual curiosity;

[141] Ross, Gartenstein, Daveed (2005) 'Christians on Paltalk Chat Service Tracked by Radical Islamic Website', New York the Sun, (31 January).
[142] Ward, Victoria (2012) 'Website Allowed Terrorists to Come Together to Plot Carnage', *The Telegraph*, 1 February.
[143] 'Terrorism Gang Jailed for Plotting to Blow Up London Stock Exchange', *The Telegraph*, (9 February 2012).
[144] Garside, Juliette (2013) 'Ministers will order ISPs to Block Terrorist and Extremist Websites', *The Guardian*, 27 November.

individuals should be allowed to expose themselves to a wide variety of political and religious positions. Obviously, when the law is broken and individuals do incite hate, violence or glorify terrorism, they are liable to be prosecuted under existing legislation.

The visible presence of online communities that are sympathetic or active supporters of extremist groups can also be an advantage for security and intelligence officials. Public data extracted from open discussion forums and chat rooms can be used to investigate terrorism related cases, as well as used as evidence in prosecutions. Online extremism also provides an opportunity for a wide range of individuals to discuss and debate extremist ideas and narratives. For counter-extremism practitioners in particular, it's a chance to engage in conversations with those sympathetic to extremist ideas and analyse conversational trends, which, in turn, inform counter-extremism strategies.

Engaging with and challenging extremist content online represents an alternative to negative measures. With extremists increasingly using social and interactive media platforms, as discussed earlier, the opportunities to take the fight to extremists online are now greater than they ever have been. It is, therefore, necessary to explore existing attempts to engage with and challenge extremist content in order to gain an appreciation of what work is being done in this area and its current limitations.

4.2 Current Efforts: Positive Measures

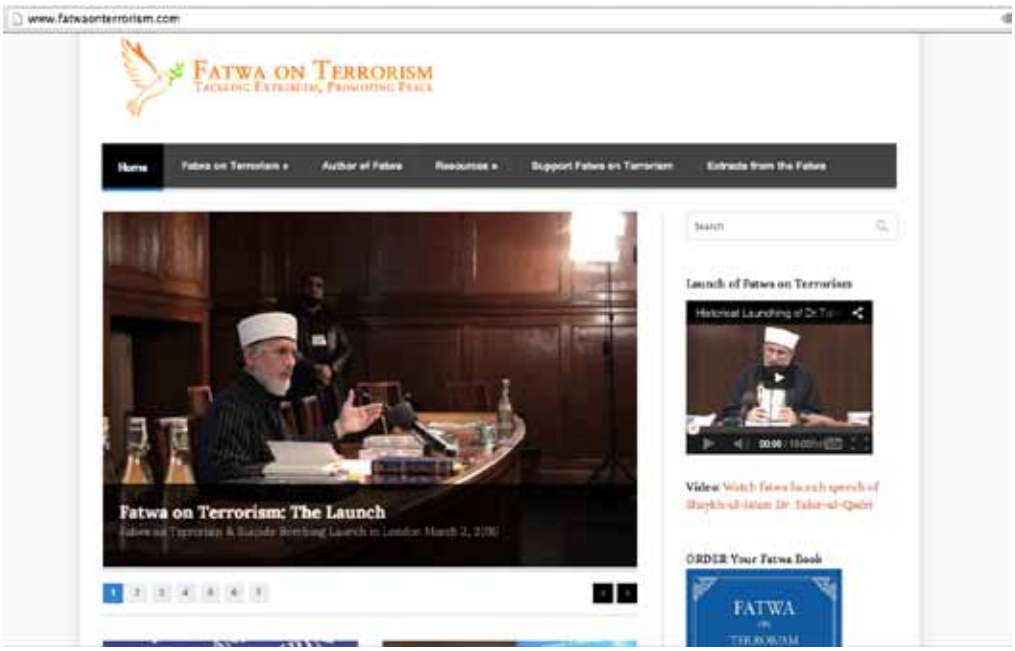
A number of public and private initiatives to counter extremism online have been launched in the past few years. Counter extremist initiatives online can broadly be divided into two forms: firstly, online initiatives that are dedicated solely to challenging extremist narratives and secondly, websites or organisations that deal with a wide range of religious and/or political issues but also offer some counterspeech messaging. These sites also vary in the extent to which they are proactive and engage in discussion and debate. Some are very active, having their own forums and social media platforms, whilst others are merely static websites with text and videos.

These web-based initiatives tend to target those who are toying with extremist ideas or are in the initial phases of the radicalisation process, rather than hardened extremists. Many of these initiatives offer theologically rooted counter-messaging. They can also take the shape

of a campaign in which the counter-messaging is presented in the form of short strap lines, posters, lengthier publications or video content. Beyond website-based initiatives, there are also educational projects that seek to raise awareness among users, making them much more cognisant of the dangers of online extremist propaganda. The following subsections offer six examples of current counter-extremist online initiatives in the UK and France, discussing their platforms, activism and success in penetrating wider audiences and spreading their ideas.

Fatwa on Terrorism

With regards to dedicated counter-extremist websites that are static, one prominent example is the site <www.fatwaonterrorism.com>. This site is dedicated to one of the world's foremost Muslim clerics, Dr. Tahir ul-Qadri, who produced a 600-page book entitled 'Fatwa on Terrorism and Suicide Bombings'. This book created a media storm when it was released in March 2010, since it was perhaps the first English language scholarly refutation of jihadism that was both comprehensive and written by a widely respected Islamic authority.



The website itself contains pertinent extracts from the book in question and answer form. These extracts discuss the legitimacy of acts of violence conducted in the name of Islam, offering theological refutations to jihadist interpretations of certain doctrine. The site has an embedded video link of Dr. Qadri discussing the material in his book, which is taken from the London launch of the book. It also has a detailed profile of Dr. Qadri, news articles related the book as well as an option to order a copy.

Overall, the site is a good example of a static website that seeks to challenge extremist narratives. However, some of the sub-sections of the website are empty and, thus, give the impression that the site is a work in progress. The content contained within the site is very powerful and certainly does pose a strong challenge to jihadists, but the lack of interactivity, in the form of a blog or forum, and integration with social media tools, such as Twitter and Facebook, makes it difficult to assess the full impact of the site. As such, the site is not achieving its full potential as an online counter-extremism tool.

Islam Against Extremism

Another example of a static counter-extremist website is the Salafi-run site 'Islam Against Extremism': <www.islamagainstextremism.com>. This site presents profiles of prominent British Islamist extremists and organisations with a view to exposing them as deviants that are not actually following the path of Islam. It contains short commentary pieces on developments within the British extremist scene, such as the Woolwich attack. It also contains much longer theological refutations of jihadist doctrine that are authored by prominent Salafi clerics, such as Imam al-Albani.

The site is visually appealing in its lay out and style and it makes its stance very clear with powerful imagery and appealing article titles. Like the site discussed previously, this one relies heavily on text to make the case against the extremists it seeks to tackle, though the style of writing in some articles is colloquial, with certain vulgar tendencies. The website could be improved by adding interactive features so that individuals could leave comments on articles. Furthermore, its content is currently not regularly updated.

Another limitation to the site is that the content and scholarly references are almost exclusively salafist, which means they are only impacting a salafist-inclined audience. This limits the appeal of the content and possibly poses a credibility dilemma, since many of the salafist clerics used to decry terrorism are also on record as having made unacceptable statements about other issues. For example, Sheikh al-Uthaymeen, issued a religious ruling on globalisation, liberalism and secularism in which he derided the concept of equality between people from differing faith backgrounds.[145] Hence, the extent to which they can be held up as role models for younger English-speaking Muslims is somewhat limited, though authentic Muslim voices denouncing extremist activities from a variety of perspectives and backgrounds is welcome.

Radical Middle Way (RMW)

The website of a British government-funded initiative called the RMW, <www.radicalmiddleway.com>, is an example of a site dealing with a range of issues, from charity to religious teachings, whilst also seeking to tackle extremism. The RMW as a whole is not necessarily a website-driven initiative, rather the site supports the offline work of RMW, which includes seminars, campaigns and speaking tours by prominent Muslim scholars. It is also visually appealing, integrated with social media, and contains a wide range of content, including video and audio recordings of RMW events.

[145] Salaf-us-Saalih.com (2013) 'Liberalism, Secularism, and Globalization'.

The content that focuses on tackling extremism is of a high quality and potentially impactful for audiences that online extremists usually target. It does not have a forum and is thus less focussed on creating debate and discussion. There is an over-emphasis on theologically rooted argumentation, which serves to limit the appeal and reach of the content, since not every potential extremist recruit is driven entirely by theological reasoning. However, as mentioned in the last example, having authentic Islamic groups acting on and offline to counter-extremist ideologies is a positive step.

Since the site is largely supporting the offline work of the RMW, and the content largely reflects real world events, it does not frequently contain new and regularly updated content. It, therefore, does not attract a high volume of traffic. The social media penetration of the group is reasonable, with over 2,000 Twitter followers and 6,600 Facebook likes, but still not at its full potential given the scale of RMW's work.

The French Council of the Muslim Faith

The French Council of the Muslim Faith (*Le Conseil Français du Culte Musulman* - CFCM) is a national elected non-profit group that was founded in 2003 to serve as an official communiqué to the French state with regards to regulations of Muslim religious activities. Since March 2012, when the Islamist extremist Mohamed Merah carried out a series of

killings, the group has also begun to focus on extremism by providing training for Imams and creating online content which is hosted on its own website.

The CFCM website, <www.lecfcm.fr>, primarily serves as a platform to connect Muslim religious entities and communities in France. However, it also a good example of a site that covers and tackles Islamist extremism-related topics. As seen in the screen shot of the CFCM website, articles such as 'Terrorism is not part of religion' explain how extremists misinterpret words like jihad for violent means, which the CFCM does not support. Though the site is primarily static and offers few active functions, it still receives a reasonably high volume of traffic and ranks within the top 100,000 sites in France.[146]

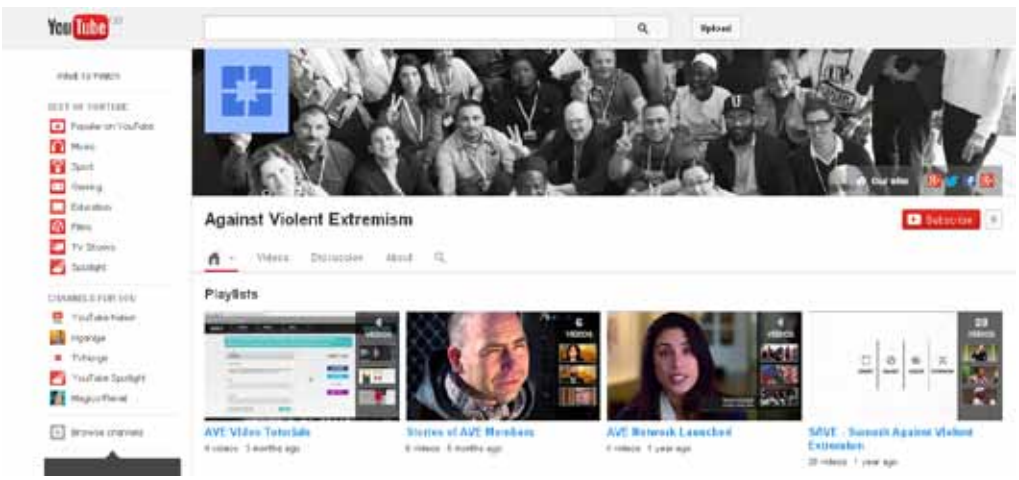
The site itself is well maintained though some sections are better functioning than others. The media section includes photo and video capabilities, though the photo section is under construction and only a few videos are presented. The news (*communiqué*) sections of the site are the most updated with frequent posts on CFCM actions along with more general French Muslim related updates. The site does not have social networking integration, with platforms such as Facebook and Twitter, and it also lacks a chat room or forum.

[146] Basic traffic data as shown by Alexa.com traffic ratings.

Against Violent Extremism (AVE)

In June 2011 Google Ideas, a think tank attached to the technology company Google, held a high profile event in Dublin called 'Summit Against Violent Extremism'. This event brought together a wide range of individuals who had previously been involved in extremist, violent or criminal organisations and had now reformed. Many of these individuals, who were collectively termed 'formers', were also using their experiences to help young people move away from extremist or criminal groups and influences. The summit, which received a great deal of media coverage at the time, sought to share the experiences of such individuals and develop a network called Against Violent Extremism that would allow them to share ideas and practices.

Following the launch of the AVE network in June 2012, a YouTube channel, which shared many video testimonies of former extremists, including Islamist extremists, was also created. This channel shares videos from the June 2011 summit that included discussions around extremism and radicalisation. The channel also shares videos that discuss the work of the AVE network as well as video tutorials for members of the network, which help them to create social media profiles.



The AVE YouTube channel is certainly an innovative and bold initiative that deserves widespread support. Using video testimonies of former and reformed extremists can be a powerful way of promoting positive counter messages and initiating much needed debate around extremism-related topics. The channel is also laid out and presented in a visually

appealing manner. It is easy to navigate and integrated with social media. The fact that most of the videos on the channel have attracted a relatively low amount of views, therefore, comes as a bit of a surprise.

For example, with the exception of the testimony of a Canadian former white supremacist, which has received over 16,000 views, other video testimonies have attracted less than 1,000 views over a two and a half year period. Similarly, most videos showing speeches from the summit have attracted fewer than 100 views and, with the exception of a video chronicling the story of the AVE network, which has attracted an impressive 63,000 views, other viewing figures are quite low. The Twitter account of the AVE network has just over 500 followers and the Facebook page has just under 300 likes.

These viewing figures suggest the AVE network did have a successful launch, and managed to attract early traffic to its channel, however, it appears most viewers do not continue to explore the channel once they have viewed the introductory video. The videos that do offer counter-messaging from former extremists are not always being widely shared and discussed whilst the social media penetration is also weak. As such, the AVE YouTube channel is not achieving its full potential, and not gaining the traction it deserves.

Digital Disruption

Digital Disruption is the name of an online counter-extremism and counterspeech initiative run by creative agency Bold Creative. This initiative is different to web-based initiatives in that online resources are designed to be used by educators in a classroom setting, and are complimented by lesson plans. These resources are designed to train young people, typically aged 11 to 19, and equip them with the skills needed to think critically and sceptically, ultimately empowering them to tackle online extremism.

These resources include a series of creative and impactful animations, entitled ‘The Propaganda Machine’, that seek to expose a number of common propaganda techniques used by websites to manipulate people’s views and the way that they think about certain issues. The resources also include a section on the website called ‘Source Check’, which demonstrates how there are fictional facts on the Internet and explains why people should not believe everything they see online. It also contains videos that offer examples of

political, commercial and historical instances of falsified facts and thus attempts to engage the user with critical thinking in order for them to be able to distinguish between fact and fiction. Another section of the website, entitled 'Click and share', attempts to educate users about the dangers of sharing online materials and the dangers of sharing inaccurate content.

Overall, the digital disruption project seems to be imparting very valuable teaching tools and, to date, these tools have reached 600,000.[147] The materials used in this project are easy to follow and effective in delivering their message. With young people increasingly turning to online materials for knowledge about the outside world, there is a strong argument for investing more resources in such educational tools and introducing them into classrooms.

A Note on Governmental and Non-Governmental 'Hacktivists'

Certain Islamist sites have also experienced cyber terrorism in recent years, whereby vigilante online disruption is carried out by anonymous online 'hacktivists'. Online vigilante activism aiming to counter extremist and terrorist efforts uses both negative and positive measures, sometimes taking down and replacing content on extremist sites or interacting within extremist forums. Hacktivism taking place outside of government has produced both

[147] Briggs, Rachel & Feve, Sebastian (2013) 'Review of Programs to Counter Narratives of Violent Extremism', *Institute of Strategic Dialogue*: London, p. 47.

praise and critique from onlookers. Table 4.1 on the following page discusses the pros and cons of vigilante hacktivism.

Table 4.1 Vigilante Anti-Jihadist 'Hacktivism': Pros and Cons

Pros	Cons
Hacktivists can get around bureaucratic red tape and quickly disable or interfere with jihadist sites.	Hacktivist interference could disrupt existing intelligence operations.
Hacktivists sometimes work in parallel to governments, thus, they are able to give them valuable terrorism-related information.	Hacktivist operations could spook important online targets.
Vigilante work is not attached to governments so there is no blame upon national institutions.	Vigilantes can shut down extremist websites that are secretly monitored by agencies for tips/contacts.
Hacktivists can target extremist sites and content that governments are unable to target.	What hacktivists target might not be considered extremist or threatening to wider audiences.

Regardless of the pros and cons, these grassroots actions are on-going and could be increasingly supported by government bodies in the future. In line with these trends, the US government has already developed the Center for Strategic Counterterrorism Communications (CSCC). On their official website it states that the CSCC was established to coordinate and inform 'government-wide foreign communications activities targeted against terrorism and violent extremism', particularly concerning al-Qaeda and its affiliates.

In explaining the types of activities the CSCC conducts it states: "The Digital Outreach Team actively and openly engages in Arabic, Urdu, Punjabi, and Somali to counter terrorist propaganda and misinformation about the United States across a wide variety of interactive digital environments that had previously been ceded to extremists."[148] Examples of the CSCC's work were disclosed by Secretary of State Hillary Clinton in May 2012, which included hacking a Yemen-based website and replacing pro-al-Qaeda images on the site with banners displaying Yemeni civilians killed in al-Qaeda attacks.[149] While online counter-terrorist efforts using hacktivism remain controversial, it is perhaps a step in the right direction to choose active engagement over centralised negative measures.

[148] Center for Strategic Counterterrorism Communications Site*, U.S. Department of State*.
[149] Bennett, Brian (2012) 'Civilian "Hacktivists" Fight Terrorists Online', *Los Angeles Times*, 8 September.

Summary

Although they offer some utility, negative measures, as outlined in this section, do not represent a real solution to countering online extremism. The large-scale implementation of negative measures can have potential financial and political costs as well as legal implications. It is also difficult to assess if negative measures are having a positive effect on counter-extremism in general. Even then, an individual determined to access certain websites can circumvent such measures. Furthermore, extremists can continue to exploit social media, and other forms of interactive online tools, without being detected by negative measures. Hence, the many negative consequences of such censorship need to be weighed against their limited utility.

Engagement with and access to extremist online content also informs the work of counter-extremist organisations who use this information to develop counterspeech. Thus, it should not be treated as though it is analogous to CSAI and we need to recognise that 'extremist content' is not always necessarily illegal. The existence of such content can also inform the work of the police and intelligence agencies who are engaged in counter-terrorist efforts.

With negative measures shown to be surmountable and potentially counter-productive it is necessary to explore existing online counter-extremism measures and assess their efficacy. Whilst the preceding section does not represent an all-inclusive overview of such initiatives, it does highlight the fact that current efforts in this regard do exist but could benefit from better content production and upkeep. There are very few, if any, counter-extremism websites that are widely popular in the UK or France.

The content contained within many of these sites can be used effectively to undermine extremist narratives. However, with infrequent updating and a limited range of content, these sites have not yet reached their full potential. Many of the sites are also aimed at audiences that might not include young Muslims who are struggling with difficult faith-based questions and identity. As such, in the current environment young people are more likely to frequent sites of a more extremist orientation since these sites not only target the youth directly and provide more interactive online social functions, but also offer a firm sense of identity and deal with difficult topics.

These counter-extremist sites also lack a broader social media presence. In an interview with the founder of the Afghanistan and Central Asian Association (ACAA), Dr. Nooralhaq Nasimi noted that funding was a major obstacle in promoting and mirroring their offline efforts into the online sphere.[150] Many times, innovative grassroots counter-extremist efforts do not have in-house tech personnel to maintain and update websites and social media platform. The only initiative that does seem to have had an impact on social media involves the work of the Digital Outreach Team discussed earlier. According to a report published in March 2013, the team has made 17,000 online interventions since being established in 2006.[151]

It is clear that there remains a large scope to develop online counter narratives. This can be done by helping grassroots initiatives that already try to tackle extremism make better use of the tools available to them online. There is also space for governments and the private sector to help the development of new online initiatives at both the local and national level.

[150] Interview with Dr Nashimi ACAA, 26 February 2014.
[151] Briggs, Rachel & Feve, Sebastian (2013) 'Review of Programs to Counter Narratives of Violent Extremism', *Institute of Strategic Dialogue*: London, p. 30.

Chapter 5. Countering Extremism Online: Recommendations

Islamist extremists are now using the Internet in ever more creative and innovative ways, often leaving counter-extremist practitioners and policy makers lagging behind. The most recent threat to European societies has come in the form of jihadist groups in Syria, Somalia and Pakistan using online tools to propagandise and recruit jihadist fighters based in Europe. Although online extremist material is rarely, if ever, the initial spark in the process of radicalisation, previous chapters have shown that the Internet can be used to educate, indoctrinate and socialise those seeking out extremist ideology. As such, online extremist content requires a proactive and efficacious response.

Countering online extremism is about providing alternative narratives on a range of issues that extremists seek to monopolise and contesting ideological or political spaces that are currently being occupied by extremist content. In essence, counter-extremist efforts should seek to dominate the online content consumed by audiences that are vulnerable to Islamist extremist counter cultures. In addition, counter-extremist content must be as relevant, appealing and impactful as extremist messaging, whilst also having the intellectual rigour and accuracy that extremist messaging clearly lacks currently.

Existing efforts to counter online extremism remain inadequate. Governments have a tendency to focus on censorship which, as illustrated in Chapter 4, has many technical, legal and political limitations as well as other negative side-effects. Civil society-led initiatives, with very few exceptions, are not currently living up to their full potential online and tend to lack the energy and commitment exhibited by their extremist counter-parts. Private sector actors, on the other hand, often lack the expertise required to tackle online extremism efficiently and are thus reliant on strategic partnerships with those in government and civil society.

Countering online extremism must be a joint effort between governments, civil society and the private sector. Within the private sector, technology corporations are particularly potent actors with an underutilised capacity to work with governments and leading civil society actors. Indeed, various forms of technical, political and religious expertise need to combine

in order to facilitate effective online counter-extremism. It is equally important to prevent counter-productive steps, such as broad negative measures, from being taken.

Based on the findings of the research conducted for this report, this chapter lays out what the authors of the report believe can and should be done to turn the tide against extremist activities online. This will involve discussing three key areas:

- The nature of effective counter-extremism.
- The specific roles and tasks of governments, private sector organisations and civil society actors as well as how all three can better collaborate.
- Specific initiatives which would be effective in the fight against online extremism and how these could be practically implemented.

5.1 Effective Counter-Extremism

Countering extremism, whether online or offline, cannot be done effectively without an understanding of the extremist ideology and strategies. Understanding the narratives of extremists includes understanding the different components of such narratives and how fact and fiction are weaved to construct them. The Islamist extremist narrative centres around a binary and divisive 'us vs. them worldview that, broadly speaking, contains political, historical and theological components, which are all inter-connected. Through the Islamist lens, Muslims are perceived as a monolithic global community that is being threatened, attacked, exploited and controlled by hegemonic Western powers driven by self-interest and corporate greed.

A global expansionist Muslim empire, or Caliphate, governed by a medieval interpretation of Shariah is, subsequently, presented as the solution to this western onslaught.[152] Theologically, the establishment of an expansionist Caliphate, and subsequent efforts to spread Islam through offensive warfare, are deemed, by Islamist extremists, an Islamic obligation that Muslims are sinful to neglect. Terrorist acts against strategic civilian and

[152]Al-Zawahiri, cited in: Mansfield, Laura (2006) *His Own Words: Translation and Analysis of the Writings of Dr. Ayman Al Zawahiri*, TLG Publications: United States.

military targets around the world are viewed as means through which these final objectives can be achieved.[153]

Counter-extremist efforts, therefore, must remain cognisant of the fact that extremists think they have scripture on their side. Counter-messaging must seek to address theological arguments too and contextualise the scriptural references that are used by extremists with a view to undermining their theological credibility. The binary Islamist worldview can also be undermined with a more nuanced reading of political reality that exposes the many forces and factors that have shaped the world in recent years. In particular, it is necessary to expose the one-dimensional fixation Islamist extremists have with attributing all the world's ills to western hegemonic powers.

Extremist groups cannot always be taken at face value since they often have distinct public and private faces, as illustrated in Chapter Two. Publicly, many extremist websites and known extremist preachers will seek to tailor their narrative, depending on the social or political context they find themselves in, and present it to audiences in a manner that makes it appeal. This involves re-branding many of their more harsh ideas to make them sound benign and selecting emotive issues in order to elicit public sympathy.

The duplicitous nature of extremist propaganda has deep implications for counter-extremism practitioners. It means that extremist narratives should not only be countered but also exposed. Often, presenting such narratives in their raw and unembellished form can contribute towards discrediting them. Since messages and narratives are presented a certain way in order to appeal to target audiences, stripping them of their re-branding would make them look less appealing and inauthentic.

In addition to offering highly embellished narratives, extremists seek to monopolise specific issues in order to ensure that their interpretation of events becomes the dominant one. The Tweet-clash between International Security Assistance Force (@ISAFmedia) in Afghanistan and the Islamic Emirate of Afghanistan (@ABalkhi), discussed in Chapter 2, is a significant illustrative example of the importance of how a struggle to tell a certain version of a story can become a space for narrative clashing and authenticating.

[153] Ibid.

The promotion of extremist content is often aided by the fact that others are rarely forthcoming with credible alternatives whilst lurid, conspiratorial and cynical interpretations of important international events can also be found in non-extremist discourse. This also makes challenging extremism difficult since the public version of the extremist narrative is able to garner wider sympathy. Such sympathy is often gained from audiences that are unaware of the underlying purpose behind the extremist narrative.

This highlights the importance of counter-propaganda and the need to critically address topics that extremists tend to monopolise. Conflict zones and the motives of rebel and government fighters in areas such as Syria, Israel-Palestine, Afghanistan, and Somalia, are contemporary examples of such topics that need to be discussed openly with all points of view exposed. In each of these cases, narratives that contradict the extremist perspective should be developed and disseminated to audiences targeted by extremists, particularly young individuals who are vulnerable to counter cultures. These narratives need to be accurate, nuanced and resonate with the target audience. Counter-narratives also need to be highly visible and accessible.

Counter-extremism is not only about exposing the true face of extremism and competing with them by using credible counter-narratives; it is also about being pro-active. Extremists spot and exploit opportunities in socio-political developments at the local and international level in order to further entrench their worldview. They are also conscious of the morale of their opposition and seek to undermine it at every opportunity, often via direct threats and intimidation. Thus, counter-extremism efforts should also be about further explaining and discussing developments in the world with a view to undermining the extremist narrative and the morale of extremist activists.

Extremist failures and defections should be highlighted and used to portray extremism as a failing project. This technique is currently being explored by the US Government's team of online Twitter users, as discussed in Chapter 4, who aim to exploit misinformation being disseminated by jihadist networks. In this regard, humour can also be a powerful tool and comic ridicule, within limits, can be used to focus attention on the absurd and anachronistic nature of extremist discourse and activity.

However, all of the above require having an activist mindset that recognises the significance of defending and justifying a set of values. In addition, this requires a clear understanding of what standpoint is being protected and what values are at stake. Counter-extremism cannot be conducted as a purely academic or bureaucratic exercise by those of a non-activist or value-neutral background. Rather, counter-extremist efforts are best led by those that are imbued with passion for their work, a familiarity with activist methods and a desire to defend a set of values.

The ultimate aim of counter-extremism is to take the glamour and allure away from extremist messaging with a view to rendering extremism unfashionable and something that elicits a civil society-led challenge in the same way racism does today. Extremism should be rendered intolerable amongst target audience members and mental obstacles that allow extremism to go unchallenged need to be removed. These obstacles include fears of being deemed culturally insensitive or even racist and misunderstanding the extremist narrative and viewing it as a noble anti-imperialist cause.

5.2 Public, Private and Third Sector: Who Does What?

Effective online counter-extremism must be a coordinated effort in which public and private sector bodies work with third sector organisations in order to develop and implement a variety of initiatives. At the same time, actors in each sector must remain cognisant of their specific roles and remain aware of their strengths, weaknesses and limitations. As such, it is important to highlight what actors in each sector can do before discussing specific initiatives or ideas.

The Public Sector

Our analysis of negative measures illustrates that new nationwide legislation and policies to implement further filtering, censoring or blocking of extremist content should not be introduced. As seen in Chapter 4, broad negative measures are not only inefficient in ridding the Internet of controversial content, but have potentially unwanted and negative effects. Governments should continue targeting explicitly illegal materials that contravene existing terrorism legislation whilst accepting that even this approach has severe limitations. Overall

the emphasis should not be on censorship but on how extremist propaganda and narratives can be challenged and discredited.

Censorship aside, governments can use their influence to bring different parties together and convene events that allow various organisations and individuals to meet and collaborate. Indeed, there is a need for a platform that brings representatives from all sectors together so that concerns can be shared, channels of communication established and initiatives developed. In particular, governments need to have established channels of communication with private sector technology companies, such as Google, YouTube and Facebook. These channels will allow them to raise concerns and establish procedures through which dialogue over contentious content or polices can be held.

Government also needs be aware of third sector initiatives so that it can offer its support when needed. Government figures can use their profile and influence to make statements that encourage civil society initiatives and help popularise counter-narratives without being the initiators of such narratives. They need to stand for the values being defended and not get mired in moral or cultural relativity for political expediency.

Government-funded initiatives have their drawbacks since they can be discredited and construed as crude government propaganda. That is not to say governments should avoid using public funds for such efforts altogether, rather, specific counter-messaging initiatives should be free from public funding. Public funds can and should be used to fund research projects that add to the knowledge base as a resource for all parties. They should also fund digital literacy and critical consumption skills in schools and communities, so that young people are able to see through extremist propaganda independently.

In the past, certainly in a British context, the public sector was seen as the primary sponsor of counter-extremism initiatives that, inadvertently, meant that civil society actors were at the mercy of policy trends. This created an inconsistency in output and often sent confused messages since a small handful of government officials with strong views on the subject could push a specific agenda. Ultimately, it should not be for governments to decide which initiatives get off the ground, nor the direction of counter-extremism messaging. In this regard, civil society should have a life of its own.

However, independently of third or private sector initiatives, governments should offer transparency and clarity on their foreign and domestic policies, especially on those policy decisions that are used by extremists. They should also challenge misrepresentations of their actions and issue clarifications when necessary. This should be done in an organised and systematic way so that messaging is pro-active and utilises social media in order to reach the target audience. In all cases the importance of respecting individual liberties and basic human rights should be borne in mind.

The Private Sector

The private sector in general and technology companies in particular, such as Google, Facebook, Twitter and YouTube, have an inherent interest in making sure their platforms are not used for extremist propaganda. At the same time they have an interest in protecting free speech and individual liberties, especially since they often rely on user-generated content. These technology platforms should reflect a wide range of viewpoints in order to be credible as a resource. They also should incorporate a large volume of content and attract high volumes of traffic in order to remain viable as a business.

As such, it is important that they have established channels of communication with public sector bodies that are responsible for ensuring the Internet is not used for promoting illegal activities. They should, therefore, make sure they are part of the policy debate in central government and remain approachable and transparent about their own policies with regards to content. Currently, channels of communication between the British government and private sector technology companies are underdeveloped and they remain even less developed in France, as discussed in an interview with Marc Hecker of the French Institute for International Relations.[154]

Beyond maintaining conduits for public sector concerns, the private sector has a great deal of resources and expertise that the third sector could benefit from. The technical expertise in particular can prove useful for initiatives that are seeking to generate and popularise online content. Hence, training workshops and seminars that share relevant expertise that

[154] Interview with Marc Hecker 6 March 2014.

allows third sector parties to develop and disseminate quality counter-extremist content would be useful.

These companies could also use their own sites and applications to promote counter-extremist content or websites. Search engines should not alter algorithms; however, they could promote counterspeech through advertisement links that naturally come up in relation to certain searches or results i.e. searches for 'jihad' or 'al-Qaeda' could more actively advertise links that promote counterspeech. Popular social media platforms, such as Twitter or Facebook, could similarly promote certain tweets or posts to users that follow or write about extremism-related issues, whether for or against.

The larger technology companies mentioned above are very resourceful and often in a position to fund initiatives directly. This kind of funding is also a lot less problematic than public sector funding, since there are fewer bureaucratic hurdles in the application process and a higher likelihood of consistency, since private companies are less susceptible to sudden changes to policy direction and personnel. As such, private companies should consider offering seed funding for online counter-extremism initiatives. This could prevent their platforms from being transformed into mediums for unchallenged extremist propaganda and help reduce calls for the blunt instrument of censorship.

The Third Sector

Ideally, counter-extremism should be a civil society led effort and, as such, online initiatives should be led and implemented by third sector organisations. Counter-messaging needs to appear organic and authentic; driven by ordinary individuals and activists that are motivated by a desire to uphold and defend the values they hold dear. Civil society, in this context, also needs to be free of governmental and corporate control in order to develop a life of its own built by the energy and creativity of ordinary members of society.

Well-placed civil society actors are often the only ones that have the appropriate level of understanding and experience of activism and extremist ideologies to challenge it online. This is because extremists themselves are also civil society actors and adopt activist techniques; hence extremists need to be beaten at their own game. Actors that have been

involved in extremist groups are even better placed to counter their messaging because they are familiar with the extremist worldview and aware of its weaknesses.

However, civil society, whilst maintaining its free and independent spirit, needs to work with partners in the public and private sectors in order to have a greater impact. Public sector co-operation could give initiatives greater influence if public figures offer their support for the ideas being espoused. The private sector could act as a resource from which expertise can be extracted and funds raised. Co-operation with private sector organisations, especially popular social media platforms and search engines, would also allow third sector initiatives to achieve maximum output.

The misconception that counter-extremism, in an Islamist context, is a uniquely theological issue also needs to be challenged. Of course, theology has a role to play, but much of extremist rhetoric revolves around geo-politics and a specific political framework used to interpret world events. Hence, counter-messaging does not have to revolve around theology alone and can focus on deconstructing political or historical strands of the grand extreme Islamist narrative, or highlighting the inconsistencies of the political vision being offered by Islamist extremists.

Finally, a civil society led challenge should seek to make Islamist extremism unpopular. Civil society should use online tools to deconstruct and discredit the extremist manipulation of religion and world events to deconstruct narratives of hate and division. Civil society efforts should seek to present a broadly united front against extremism online and encourage a general society-wide intolerance of extremist ideas so that they lose their potency and appeal.

5.3 Policies and Initiatives to Counter Online Radicalisation

Based on the findings of this report, along with Quilliam's prior understanding and experience with counter-extremism activism, a number of key proposals, that would help turn the tide against online extremism, are presented below. These proposals, if implemented, would not only make target audiences and those vulnerable to counter cultures more resilient to extremist messaging, but also increase the presence of counter-extremism content online. These proposals include:

- Establishing a forum that deals with online extremism and brings stakeholders from key sectors together in order to do so.
- Improving digital literacy and critical consumption skills in schools and communities.
- Encouraging the establishment of a social media outlet that clarifies government policies and debunks propaganda.
- A mapping exercise that explores current efforts to tackle extremism online and identifies partners that could be given support to develop an effective online presence.
- Establishing a central body that offers seed funding and training for grassroots online counter-extremism initiatives.
- More research into how the radical-right is using the Internet to propagandise.

Forum for Dealing with Online Extremism

While some of these proposals are directed specifically at certain sectors, others are meant as collaborative proposals that would require all three sectors to unite and work together. Numerous counter-extremism and counter-terrorist experts interviewed for this report agreed that national and international cooperation between government bodies and private companies is essential in combating online extremism. Other reports on combating online extremism have also flagged the necessity for better private and public sector communication pathways.[155] In addition, mentors interviewed agreed there should be further cooperation between sectors to better understand perceptions of threat and ways of countering the spread of radicalisation.

With the above in mind, the authors propose the establishment of an online counter-extremism forum convened by governments that brings stakeholders together on a regular basis. Ideally, this forum would have key representatives from government departments, technology companies and third sector organisations that have a strong online presence. Representatives from these sectors should meet regularly to share ideas and challenges as well as establish regular channels of communication. Meetings would also serve to better establish procedures through which common issues can be resolved amicably.

[155] See: Briggs, Rachel and Sebastian Feve (2013) *Policy Briefing: Inspire, Radicalise, Recruit*, (Institute for Strategic Dialogue). See also: Neumann, Peter (2012) *Countering Online Radicalisation in America*, (Bipartisan Policy Center).

Digital Literacy and Critical Consumption

As well as challenging extremist propaganda, counter-extremist efforts must first ensure that target audiences are less receptive to extremist messaging in the first place. This involves investing in digital literacy and critical consumption training at an early age and, ideally, introducing such training programmes into classrooms as part of the national curriculum. Parents, primary carers, youth leaders and other people that come into contact with young people on a regular basis also need awareness of online extremist materials.

For young people, the skills gained from such training can enable them to understand the importance of verifying sources, along with distinguishing between media reporting and extremist propaganda. This would also serve to create awareness on how tragedies and conflicts are easily exploited by those that wish to use them for their own agenda. For adults, similar training could help prepare them for discussions about extremist content and they, in turn, could use their knowledge to prevent young people from viewing materials that are not age-appropriate.

Magnus Ranstorp, a leading terrorism expert, reiterated in an interview: "Critical thinking is key. It is necessary to educate on critical thinking and the consequences of going down the wrong route."[156] Maura Conway, whose research specializes in terrorism and the Internet, suggested that the same standards that education boards apply for current subjects should be applied to Internet literacy as a new and necessary course for students: "In Ireland, the UK, Europe and the world we need formal education of the Internet."[157]

Social Media Outlet

Much of extremist propaganda relies on distortions and mischaracterisations of European and American foreign policy, as well as some valid critiques. Extremists are often able to get away with doing this, especially in a British and French context, because governments are generally quite poor at communicating their policies abroad to domestic audiences. It is for these reasons that a social media outlet that clarifies foreign policy decisions and actions, whilst debunking distortions and propaganda, is necessarily for both Britain and France.

[156] Interview with Magnus Ranstorp conducted on 5 February 2014.
[157] Interview with Maura Conway conducted on 12 March 2014.

Such an outlet would need to be pro-active in identifying issues that need clarity, such as efforts to resolve the conflict in Syria and on-going operations in Afghanistan. It would also need to be reactive on occasions, deconstructing extremist propaganda that relies on instrumentalising foreign policy decisions. A single outlet that offers on-going commentary on international and domestic counter-terrorism developments, incorporating discussions on relevant foreign policy issues, should also be considered, for the sake of simplicity and in order to focus expertise.

Currently this is being done competently by the US State Department through its Digital Outreach Team, as discussed in Chapter 4. Alberto Fernandez, coordinator for the Center of Strategic Counterterrorism Communications (CSCC) said: "In overt communications we confront al-Qaeda everyday... Al-Qaeda set up a team to go after us on Twitter, to confront us, and take us down. We have seen repeated evidence that we get under their skin and want to shut us down."[158] While the CSCC works primarily in Urdu, Somali and Arabic with some English content, the UK and France would benefit from working in native languages.

Mapping Exercise

A mapping exercise that identifies relevant organisations and individuals that are capable and willing to be involved in online counter-extremism work is an important first step if such work is to be commissioned. This would require exploring how such groups or individuals are currently using online tools, if at all, assessing what impact those efforts are having and what they lack in terms of expertise and resources. This mapping exercise would allow the current counter-extremist landscape to come into sharp focus and shed light on where resources and efforts could be further developed.

Central Body Offering Grants and Support

In order to reclaim online ground conceded to extremists over the past decade, it is important that a large number of varied online counter-extremism initiatives are launched and maintained. This much needed wave of activism could be instigated and supported by a grant-making body that offers seed funding and training for grassroots online counter-extremism projects. These projects should aim to deconstruct and discredit extremist

[158] Interview with Alberto Fernandez on 12 February 2014.

narratives whilst promoting alternative paradigms through which grievances can be construed and identity calibrated.

Ideally these would be smaller grant sums (ranging between £500 and £2,000) that would go towards helping existing initiatives improve their online presence and further develop their social media outreach. Larger grants should also be considered if the project in question proves to have a significant impact and requires further support. Specific online initiatives could include fully-fledged websites, social media campaigns, a series of videos hosted on video-sharing platforms such as YouTube, and forums that discuss pertinent topics related to extremism.

These initiatives could be set-up and run by individuals, small community groups, student societies and other small to medium sized networks. The role of the grant-making body would be to assess applications, offer grants, provide support and training (both technical and strategic) as well as monitor impact and success. The grant-making body would, in turn, be the beneficiary of a much larger grant, from which the smaller grants are offered, and be accountable for the smaller initiatives it decides to fund. Funding for such an intiative should ideally come from both government and private sector bodies.

Funding and support could also be given to counter-extremist organisations and initiatives that already have an online presence with a view to further developing online work. Such initiatives, some of which were discussed in Chapter 4, often have the necessary ideas and content but lack resources, technical skills and marketing expertise to disseminate their ideas to a broader audience. Hence, training and sharing of expertise would form a key part of this strand of work.

Continuing Research on Online Extremism

As governments are proposing to target extremism online there is a need to better understand a wide range of extremist networks online. With far-right groups growing in influence across Europe, including in the UK and France, it is important to further explore how they use the Internet to propagandise and recruit. This research would focus on far-right websites, social media accounts, video-channels and forums, with a view to mapping the online footprint of such organisations and individuals. The ultimate aim would be to

assess the extent to which this online presence is efficacious and how it affects offline far-right activity.

Furthermore, the symbiotic nature of far-right and extreme Islamist activism needs to be elucidated so that counter-extremist activists can discredit their efforts. The extent to which the far-right incorporates the rhetoric of Islamist extremists into their propaganda, and vice-versa, is important to know. If evidence that the two extremes are feeding off each other in order to justify their respective worldviews can be found, it could prove very useful in the fight against extremism.

Additionally, in order to avoid accusations of bias, consistency in activism is also important and efforts should be focused on a broad spectrum of extremism. In the UK, anti-racism campaigners often attack the far-right whilst making alliances with extreme Islamists in order to do so. Such activism can easily be discredited and undermines the struggle against extremism as a whole. Similarly, in France, an emerging alliance between far-right elements and Muslim conservatives, based on mutual beliefs in homophobia and anti-Semitism, is increasingly being exposed and it highlights the politically expedient and unscrupulous nature of some extremism activism. [159]

Summary

An understanding of the extremist mindset and the strategies used to popularise extremist ideas needs to be gained before the job of challenging extremism online can truly commence. It is important that practitioners identify weaknesses and inconsistencies in the extremist narratives and, ultimately, exploit them. Counter-extremism initiatives should seek to reverse the monopoly extremists currently hold over certain topics. The ultimate aim should be to render extremism unfashionable whilst the importance and relevance of democratic values is emphasised.

Challenging extremism online should be a joint effort between public, private and third sector stakeholders. However, it is important that each sector is aware of the role they can play and the ways in which they can assist actors in other sectors. Third sector organisations

[159] Saltman, Erin (2014) ' The Far-Right and Radical Islamists are Finding Common Ground in Homophobia and Conspiracy Theories', *Left Foot Forward*, March.

and individuals should be viewed as the front line in counter-messaging and their efforts should be organic and free from external influences and pressures. However, the private sector can use its resources and expertise to assist such efforts, whilst the public sector should use its influence and role in society to support key messages and ensure unnecessary legislative steps that hinder Internet freedoms are not taken.

This report has recommended six key measures that the authors think would help turn the tide against online extremism. These measures require resources, expertise, passion and, most importantly, cooperation across various sectors. This cooperation is vital and sectors must work together to create a wave of activism that will powerfully confront extremist efforts online.

BIBLIOGRAPHY

Books and Articles

Al-Zawahiri, cited in: Mansfield, Laura (2006) *His Own Words: Translation and Analysis of the Writings of Dr. Ayman Al Zawahiri*, TLG Publications: United States.

Bakker, Edwin & de Graaf, Beatrice 'Lone Wolves: How to Prevent this Phenomenon?', *Expert Meeting Paper*, November 2010, International Centre for Counter-Terrorism: The Hague.

Beckford, Joly & Khosrokhavar, Farhad (2005) *Muslims in Prison: Challenge and Change in Britain and France*, Palgrave Macmillan: New York.

Behr, Ines, Von; Reding, Anais; Edward, Charlie & Gribbons, Luke (2013) 'Radicalisation in the Digital Era The Use of the Internet in 15 Cases of Terrorism and Extremism' *RAND Europe*: Cambridge.

Berman, Gavin & Dar, Aliyah (2012) 'Prison Population Statistics', *Social and General Statistics*.

Bertholee, Rob (2012) *Jihadism on the Web: A Breeding Ground for Jihad in the Modern Age*, General Intelligence and Security Service - Ministry of the Interior and Kingdom Relations of the Netherlands, January.

Beyler, Clara (2006) 'The Jihadist Threat in France'**,** *Current Trends in Islamist Ideology***,** (3) pp.89-113.

Boyer, Alain (2000) *L'Islam dans la République - La Documentation Française*, Haut conseil à l'intégration.

Brandon, James (2009)'Unlocking Al-Qaeda: Islamist Extremism in British Prisons', *Quilliam*: London.

Briggs, Rachel & Feve, Sebastian (2013) 'Review of Programs to Counter Narratives of Violent Extremism', *Institute of Strategic Dialogue*: London.

Burke, Jason (2004) 'Think Again Al Qaeda' Foreign Policy, 142, (May- June), p.18-24.

Burton, Fred & Stewart, Scott (2008) 'The "Lone Wolf" Disconnect', *Statfor Global Intelligence*, 30 January ,accessed at : http://www.stratfor.com/weekly/lone_wolf_disconnect>, [Accessed: January 2014].

Carter, Joseph, Shiraz Maher and Peter Neumann (2014) '#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks', *ICSR*, London.

Center for Strategic Counterterrorism Communications Site, U.S. Department of State, Available at: http://www.state.gov/r/cscc/ [Accessed: March 2014].

Cortes, Carlos (1986) 'Minorities: Insinuating Images Influence Perceptions', *Media & Values*, (35).

Edwards, Charlie & Gribbon, Luke (2013) 'Pathways to Violent Extremism in the Digital Era', *The RUSI Journal*, 158(5), pp. 40 – 47.

Fighel, Jonathan (2007) 'Radical Islamic Internet Propaganda: Concepts, Idioms and Visual Motifs', Cited in: Ganor, Boaz; Van Knop, Katharina & Duarte, Carlos (2007) *Hypermedia Seduction for Terrorist Recruiting*, NATO Science for Peace and Security, IOS Press: Eliat Israel.

Ganor, Boaz; Van Knop, Katharina & Duarte, Carlos (2007) *Hypermedia Seduction for Terrorist Recruiting*, NATO Science for Peace and Security, IOS Press: Eliat Israel.

Google Inside Search: How Search Works, Available at: http://www.google.com/intl/en_us/insidesearch/howsearchworks/algorithms.html [Accessed January 2014].

Guéant, Claude Cited in: Djamila, Gérard (2012) 'La sur-représentation des musulmans dans les prisons françaises est très importante et indéniable', *Riposte Laïque*, 10 October, Available at: http://ripostelaique.com/la-sur-representation-des-musulmans-dans-les-prisons-francaises-est-tres-importante-et-indeniable.html [Accessed: March 2014].

Hannah, Greg; Clutterbuck, Lindsey & Rubin, Jennifer (2008) 'Radicalisation or Rehabilitation: Understanding the Challenge of Extremist and Radicalised Prisoners'. *Rand Corporation:* Santa Monica CA.

Hewitt, Christopher (2003) *Understanding Terrorism in America: From the Khan to Al Qaeda* , Routledge: London & New York.

HM Government (2013) 'Tackling Extremism in the UK: Report from the Prime Minister's Task Force on Tackling Radicalisation and Extremism', 4 December, *Crown Press*: London, Available at: https://www.gov.uk/government/speeches/tackling-extremism-in-the-uk-report-from-the-prime-ministers-task-force-on-tackling-radicalisation-and-extremism [Accessed: March 2014].

Janis, Irving (1983) *Groupthink: psychological studies of policy decisions and fiascos,* Houghton Mifflin.

Johnson, Toni *(2011)* 'Threat of Homegrown Islamist Terrorism', *Council on Foreign Relations,* September 30.Availabe at: http://www.cfr.org/terrorism/threat-homegrown-islamist-terrorism/p11509 [Accessed: March 2014].

Livingston, Brian (2000) 'AOL's 'Youth Filters' Protect Kids from Democrats', 24 April, *CNet News.* P. 9 Cited in: Heins, Marjorie, Cho, Christina and Feldman, Ariel (2006) 'Internet Filters a Public Policy Report', Brennan Centre for Justice. Available at: http://www.fepproject.org/policyreports/filters2.pdf [Accessed: March 2014].

'Lone-Wolf Terrorism' (2007) Instituut voor Veiligheids- en Crisismanagement, Available at: http://www.transnationalterrorism.eu/tekst/publications/Lone-Wolf%20Terrorism.pdf [Accessed on March 2014].

Lowes, Nick & Mulhall, Joe (2013) *Gateway to Terror: Anjem Choudary and the al-Muhajiroun Network*, Hope Not Hate.

Khosrokhavar, Farhad (2004) *L'Islam dans les Prisons: Voix et Regard*s, Balland: Paris.

Koch, François (2011) 'Islam en prison: le rapport qui pointe les discriminations', *L'Express*, 13 April.

Kushner, Harvey (2003) *Encyclopedia of Terrorism*, Sage: Thousand Oaks and London.

Marranci, Gabriele (2007) 'Faith Ideology and Fear: The Case of Current and Former Muslim Prisons', British Academy.

Mirza, Munira; Senthilkumaran, Abi & Ja'far , Zein (2007) 'Living apart Together – British Muslims and the Paradox of Multiculturalism', *Policy Exchange:* London.

Moniquet, Claude (2005) The Radicalisation of Muslims Youth in Europe: The Reality and the Scale of the Threat, Testimony of Claude Moniquet, *United States House of Representative.*

Mueller III, Robert (2003) 'War on Terrorism', *Testimony of Robert S. Mueller, III, Director, FBI, Before the Select Committee on Intelligence of the United State Senate*, Washington Available at: http://www.fbi.gov/news/testimony/war-on-terrorism [Accessed: March 2014].

Musawi, Mohammed (2010) 'Cheering for Osama: How Jihadists use Internet Discussion Forums', *Quilliam:* London.

Nacos, Brigitte & Torres-Reyna, Oscar (2003) 'Framing Muslim-Americans Before and After 9/11', Cited in: Norris, Pippa. Kern, Montague & Just, Marion. (2013) *Framing Terrorism: The News Media, The Government and the Public*, Taylor & Francis: London.

Neumann, Peter (2012) 'Countering Online Radicalisation in America', *Bipartisan Policy Center*: Washington DC.

Neumann, Peter (2010) 'Prison and Terrorism: Radicalisation and De-Radicalisation in 15 Countries' *ICSR*: London.

'NW CTU Case Study – Operation Monmorth', *North West Counter Terrorism Unit*, GMP Police Report , Available at: http://www.gmp.police.uk/content/WebAttachments/FE4CCAF04F57230580257B01002FAB34/$File/Operation%20Monmorth%20Case%20Study%20final.pdf [Accessed: March 2014].

O'Neill, Sean & McGrory, Daniel (2010) *The Suicide Factory: Abu Hamza and the Finsbury Park Mosque*, Harper Perennial: London and New York.

Pantucci, Raffaello (2011) 'Wolves: Preliminary Analysis of Lone Islamist Terrorism', *ISCR*: London.

Pargeter, Alison (2008) *The New Frontiers of Jihad: Radical Islam in Europe*, IS Tauris: London.

Precht, Tom (2007), 'Home Grown Terrorism and Islamist Radicalisation in Europe: From Conversion to Terrorism', *Danish Ministry of Justice*.

'Public Perceptions about Minorities and Immigrants: the Role of the Media', (31 May 2011), *European Policy Centre*, (Event Report S49/11).

'Religion in England and Wales 2011', *Office for National Statistics,* (11 December 2012), Available at: http://www.ons.gov.uk/ons/rel/census/2011-census/key-statistics-for-local-authorities-in-england-and-wales/rpt-religion.html [Accessed on March 2014].

Rogan, Hanna (2006) 'Jihadism Online – A study of how al-Qaida and radical Islamist Groups use the Internet for Terrorist Purposes', *Norwegian Defence Research Establishment*: Kjeller.

Rogers, Brooke & Neumann, Peter (2007) 'Recruitment and Mobilisation for the Islamist Militant Movement in Europe' *Kings College London*: London.

'Roots of Violent Radicalisation' (2012) *House of Commons Home Affairs Committee*, (19th Report of Session 2010-12, Vol. 1).

Rosen, Jeffrey (2012) 'The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google', *Fordham Law Review* (80), pp. 1525-1538.

Ryan, Jonathan (2007) *Countering Militant Islamist Radicalisation on the Internet*, Cromwell Press: Trowbridge.

Sageman, Marc (2008) *Leader Jihad: Terror Networks in the Twenty-First Century*, University of Pennsylvania Press: Philadelphia.

Spaaij, Ramon (2012) *Understanding Lone Wolf Terrorism: Global Patterns, Motivations and Prevention*, Springer: London and New York.

Stevens, Tim & Neumann, Peter (2009) 'Countering Online Radicalisation: A Strategy for Action', *ICSR*: London.

'Terrorism and the Internet: Should Web Sites that Promote Terrorism be Shut Down?' Pp. 445 – 468. Cited in: (2011) 'Issues in Peace and Conflict Studies', *Sage*: Thousand Oaks.

Torok, Rohyn (2013) 'Developing an explanatory model for the process of online radicalization and terrorism', *Security Informatics*, 2(6).

Vliegenthart, Rens (2007) *Framing Immigration and Integration: Facts, Parliament, Media and Anti-Immigrant Party Support in the Netherlands*. Vrije Universiteit: Amsterdam.

Sanderson, D. & Fortin, A. (2001) 'The Projection of Geographical Communities into Cyberspace' in Munt, SR. ed. *Technospaces: Inside the New Media* Continuum: London.

Schmid Alex and Jongman, Albert (1988) *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature*. Transaction Publishers, Rutgers University: New Brunswick, New Jersey.

Weimann, Gabriel (2011) 'Terror, Facebook, Twitter, and YouTube', *Brown Journal of World Affairs*, 16 (2) pp. 45-55.

Wiktorowicz, Quintan (2004), *Islamic Activism: A Social Movement Theory Approach,* Indiana University Press.

Zittrain, Jonathan & Palfrey, John (2008), 'Introduction', in Deibert, Ronald; Palfrey, John; Rohozinski, Rafal & Zittrain, Jonathan (2008) *Access Denied: The Practice and Policy of Global Internet Filtering*, MIT Press: Cambridge, pp. 1-4.

'9th Curcuit En Banc Panel Rules Against Yahoo in French Internet Censorship Case', *Tech Law Journal,* (12 January 2006).

Newspaper Articles, Blogs and Websites

Aziz, Farieha (2013) 'Bolo Bhi Amicus Reports on YouTube Case Hearing', *Bolo Bhi*, (1May), < http://bolobhi.org/bolo-bhi-amicus-reports-on-youtube-case-hearing/>.

Aims and Objectives of the Organisation', *Finsbury Park Mosque Website,* Available at: http://www.finsburyparkmosque.org [Accessed: March 2014]

'Airport Terrorist in Flaming Jeep was Born in UK', *Edinburgh News* (4 July 2007) Available at: http://www.edinburghnews.scotsman.com/news/airport-terrorist-in-flaming-jeep-was-born-in-uk-1-1323744 [Assessed on: March 2014]

Al-Awalaki, Anwar (2009) '44 ways to support jihad', January. Available at: http://forums.islamicawakening.com/f18/44-ways-supporting-jihad-anwar-al-awlaki-20312/ [Accessed: March 2014].

Alex, Chris (2012) 'Top 10 Search Engines in the World', *ReliableSoft.net*, Available at: http://www.reliablesoft.net/top-10-search-engines-in-the-world/ [Accessed: January 2014].

Alonso, Pierre (2012) 'Twitter: The New Frontline in Global Cyber-Jihad', *OWNI.eu*, Available at: http://owni.eu/2012/01/10/twitter-the-new-frontline-in-global-cyber-jihad-al-qaeda-somalia/ [Accessed: March 2014].

'Ansar al-Haqq, le forum islamiste française fermé suite à l'arrestation de 12 suspects' *La Libellule*, 11 October 2012. Available at: http://therese-zrihen-dvir.over-blog.com/article-ansar-al-haqq-le-forum-islamiste-fran-ais-ferme-suite-a-l-arrestation-de-12-suspects-111149261.html [Accessed: March 2014].

'As it Happened: Two Guilty of Lee Rigby Murder – Key Points', *BBC News*, Available at: http://www.bbc.co.uk/news/uk-25451695 [Accessed: March 2014].

Barnett, David (2013) 'Are You Looking at an Official Shabaab Twitter Account?', *Threat Matrix: A Blog of the Long War Journal*, 25 September, Available at: http://www.longwarjournal.org/threat-matrix/archives/2013/09/are_you_looking_at_an_official.php [Accessed March 2014].

Bennett, Brian (2012) 'Civilian "Hacktivists" Fight Terrorists Online', *Los Angeles Times*, 8 September, Available at: http://articles.latimes.com/2012/sep/08/nation/la-na-terror-hacker-20120909 [Accessed: March 2014].

Blachere Emilie & Peytavin, Gregory (2013) 'Alexandre, 22 ans, Français, Djihadiste', *Paris Match*, 7 June, Available at: http://www.parismatch.com/Actu/Societe/Alexandre-22-ans-francais-djihadiste-517746 [Accessed: March 2014]

'Bomb Plot Doctor Jailed for Life', *BBC News*, (17 December 2008), Available at: http://news.bbc.co.uk/1/hi/7786884.stm, [Accessed: March 2014]

Burns, John & Helft, Miguel (2010) 'YouTube Withdraws Cleric's Videos', *New York Times World,* 4 November, Available at: http://www.nytimes.com/2010/11/05/world/05britain.html?_r=0 [Accessed: March 2014].

Claude, Guéant Cited in: Djamila Gérard, (2012), 'La sur-représentation des musulmans dans les prisons françaises est très importante et indéniable', *Riposte Laïque*, 10 October, Available at: http://ripostelaique.com/la-sur-representation-des-musulmans-dans-les-prisons-francaises-est-tres-importante-et-indeniable.html [Accessed: March 2014] .

Center for Strategic Counterterrorism Communications Site, U.S. Department of State, Available at : http://www.state.gov/r/cscc/ [Accessed: March 2014].

Conway, Maura & McInerney, Lisa (2008) *Jihadi Video & Auto-Radicalisation: Evidence from an Exploratory YouTube Study*, December, First European Conference on Intelligence and Security Informatics.

Cosgrove, Michael (2011) 'How Does France Count its Muslim Population?', *Le Figar,* 7 April, Available at: http://plus.lefigaro.fr/note/how-does-france-count-its-muslim-population-20110407-435643 [Accessed: March 2014].

Cruickshank, Paul & Lister, Tim (2012) 'French Killings Refocus Fears on Solo Acts of Terror', *CNN Europe*, 22 March, Available at: http://edition.cnn.com/2012/03/21/world/europe/france-solo-terror/ [Accessed: March 2014] .

Dodd, Vikram & Howden, Daniel (2013) 'Woolwich Murder: What Drove Two Men to Kill a Soldier in the Street?', *The Guardian*, 19 December, Available at: http://www.theguardian.com/uk-news/2013/dec/19/woolwich-murder-soldier-street-adebolajo-radicalised-kenya [Accessed: March 2014].

Dodd, Vikram (2010) 'Profile: Roshonara Choudhry', *The Guardian*, 2 November, Available at: http://www.theguardian.com/uk/2010/nov/02/profile-roshonara-choudhry-stephen-timms [Accessed: March 2014].

Duportail, Judith (2013) 'Ansar Al-Haqq, le visage du djihadisme à la française', *Le Figaro*, 1 October, Available at: http://www.lefigaro.fr/actualite-france/2013/10/01/01016-20131001ARTFIG00499-ansar-al-haqq-le-visage-du-djihadisme-a-la-francaise.php [Accessed: March 2014].

'Facebook's Statement of Right and Responsibilities', *Facebook Legal Terms, (*SRR last updated 15 November 2013), Available at: https://www.facebook.com/legal/terms [Accessed: March 2014].

Freedom House (2014) 'Freedom in the World', Available at: http://www.freedomhouse.org/report-types/freedom-world [Accessed: March 2014].

Freedom House (2013) 'Freedom in the World: France', Available at: http://www.freedomhouse.org/report/freedom-world/2013/france [Accessed: March 2014].

'French Soldier Stabbing: Man on Terrorism-Linked Charges', *BBC News*, 31 May 2013, Available at: http://www.bbc.co.uk/news/world-europe-22735883 [Accessed: March 2014].

Gammell, Caroline (2008) 'Britain's Youngest Teenage Terrorist: A Wake Up Call for Parents', *The Telegraph*, 19 September, Available at: http://www.telegraph.co.uk/news/2988926/Britains-youngest-teenage-terrorist-a-wake-up-call-for-parents.html [Accessed: March 2014].

Garside, Juliette (2013) 'Ministers will order ISPs to Block Terrorist and Extremist Websites', *The Guardian*, 27 November, Available at: http://www.theguardian.com/uk-news/2013/nov/27/ministers-order-isps-block-terrorist-websites [Accessed: March 2014].

Gerard, Djamila (2012) 'La sur-représentation des musulmans dans les prisons françaises est très importante et indéniable', 10 october, Available at: http://ripostelaique.com/la-sur-representation-des-musulmans-dans-les-prisons-francaises-est-tres-importante-et-indeniable.html [Accessed: March 2014].

Gertz, Bill (2013) 'Al Qaeda Opens First Official Twitter Account', *The Washington Free Beacon*, 27 September, Available at: http://freebeacon.com/al-qaeda-opens-first-official-twitter-account/ [Accessed: March 2014].

Hilburn, Matthew (2014) 'Turkey's Twitter Ban Backfires as Millions Find Workarounds', *Voice of America: Middle East*, (March 21), <http://m.voanews.com/a/turkeys-twitter-ban-backfires/1876424.html>.

'Homegrown British Terrorist Bride Jailed over Jewish Plot', *The Telegraph*, 20 July 2012, Available at: http://www.telegraph.co.uk/news/uknews/crime/9415695/Homegrown-British-terrorist-bride-jailed-over-Jewish-plot.html [Accessed: March 2014].

Index on Censorship (2013) 'France: Strict Defamation and Privacy Laws', 19 February. Available at: http://www.indexoncensorship.org/2013/08/france-faces-restrictions-on-free-expression/ [Accessed: March 2014].

'Jail for Suicide Vest Student', *BBC News*, (17 July 2009). Available at: http://news.bbc.co.uk/1/hi/8155978.stm [Accessed: March 2014].

Le Bars, Stéphanie (2013) 'La radicalisation dans les mosquées est devenue quasiment impossible', *Le Monde Blog*, 31 May, Available at: http://religion.blog.lemonde.fr/2013/05/31/la-radicalisation-dans-les-mosquees-est-devenue-quasiment-impossible/ [Accessed: March 2014].

Lunden, Ingrid (2012) 'Analyst: Twitter Passed 500M Users in June 2012', *Tech Crunch*, 30 July, Available at: http://techcrunch.com/2012/07/30/analyst-twitter-passed-500m-users-in-june-2012-140m-of-them-in-us-jakarta-biggest-tweeting-city/ [Accessed: March 2014].

Manber, Undi (2011) 'Google Lied about Manually Changes', 4 February, SEO Black Cat. Available at: http://seoblackhat.com/ [Accessed: March 2014].

'Man Jailed over Suicide Bomb Book', *BBC News*, (15 December 2009) Available at: http://news.bbc.co.uk/1/hi/england/derbyshire/8414527.stm [Accessed: March 2014].

Matinde, Vincent (2014) 'Somalia's al Shabaab Threatens to Cut Internet Connectivity', *IT Web Africa*, 9 January, Available at: http://www.itwebafrica.com/ict-and-governance/394-somalia/232200-somalias-al-shabaab-threatens-to-cut-internet-connectivity [Accessed: March 2014].

Mediametrie, Available at: http://www.mediametrie.fr/internet/communiques/l-audience-de-la-video-sur-internet-en-mars-2013.php?id=861#.UZ0qFGR5xH0 [Accessed: March 2014].

Mohamed, Hamza (2013) 'Al-Shabab Say they are Back on Twitter', *Al Jazeera*, Available at: http://www.aljazeera.com/news/africa/2013/12/al-shabab-claim-they-are-back-twitter-201312161045332757 8.html [Accessed: February 2014].

'Muslim who Stabbed Jew to be Detained in Hospital', *The Guardian*, 19 September 2002, Available at: http://www.theguardian.com/uk/2002/sep/19/race.world [Accessed: March 2014].

'Nail-Bomber Given Life Sentence', *BBC News*, (30 January 2009) Available at: http://news.bbc.co.uk/1/hi/uk/7859887.stm [Accessed: March 2014].

'NatWest Handed Al Qaeda Terrorist 100% Mortgage to Buy £93,000 Home He Turned into Bomb Factory', *Daily Mail*, (16 December 2009), Available at: http://www.dailymail.co.uk/news/article-1236301/Bank-blasted-giving-Al-Qaeda-terrorist-100-mortgage.html [Accessed: March 2014].

Odula Tom & Hui, Sylvia (2013), Kenya: UK Soldier Killing Suspect Arrested in 2010', *Associated Press*, 26 May, Available at: http://bigstory.ap.org/article/uk-sets-task-force-target-radical-preachers, [Accessed: March 2014].

Pipes, Daniel (2008) 'Sudden Jihad Syndrome – It's Now Official', *Middle Eastern Forum*, 2 January, Available at: http://www.danielpipes.org/blog/2008/01/sudden-jihad-syndrome-its-now-official>. [Accessed: March 2014] .

Koch, François (2011) 'Islam en prison: le rapport qui pointe les discriminations', *L'Express*, 13 April, Available at: http://www.lexpress.fr/actualite/societe/justice/islam-en-prison-le-rapport-qui-pointe-les-discriminations_982039.html [Accessed: March 2014].

Ross, Gartenstein, Daveed (2005) 'Christians on Paltalk Chat Service Tracked by Radical Islamic Website', New York the Sun, (31 January), Available at: http://www.nysun.com/national/christians-on-paltalk-chat-service-tracked-by/8455/ [Accessed: January 2014].

Salaf-us-Saalih.com (2013) 'Liberalism, Secularism, and Globalization', Available at: http://salaf-us-saalih.com/2013/08/28/liberalism-secularism-and-globalization-explained-by-shaykh-uthaymeen/ [Accessed: February 2014].

Saltman, Erin (2014) ' The Far-Right and Radical Islamists are Finding Common Ground in Homophobia and Conspiracy Theories', *Left Foot Forward*, March. Available at: http://www.leftfootforward.org/2014/03/relations-between-the-radical-right-and-radical-islam/ [Accessed: March 2014].

Schneier, Bruce (2013) 'Evading Internet Censorship, Schneier on Security', Available at https://www.schneier.com/blog/archives/2013/08/evading_interne.html [Accessed: March 2014].

Sengupta, Kim & Milmo, Cahal (2007) 'Police Link Suspects Held over Failed Attacks', *The Independent*, 5 July.

Smith, Mike Deri, (2013) 'Porn Filters Block Sex Education Websites', *BBC Newsnight*, 18 December, Available at: http://www.bbc.co.uk/news/uk-25430582 [Accessed: March 2014].

Swinford, Steven (2011) 'WikiLeaks: How Britain Became a Haven for Migrant Extremists', *The Telegraph,* 25 April.

The Gay and Lesbian Alliance against Defamation (1999) 'Access Denied, Version 2.0: The Continuing Threat Againist the Internet Access and Privacy and its Impact on the Gay, Lesbian, Bisexual and Transsexual Community' p. 9. Cited in: Heins, Marjorie, Cho, Christina and Feldman, Ariel (2006) 'Internet Filters a Public Policy Report', Brennan Centre for Justice. Available at: http://www.fepproject.org/policyreports/filters2.pdf [Accessed: March 2014].

Travis, Alan (2013) 'Hundreds of Young People have Received Anti-Radicalisation Support', *The Guardian*, 26 March, Available at: http://www.theguardian.com/uk/2013/mar/26/hundreds-people-anti-radicalisation-support [Accessed: March 2014].

Travis, Alain (2012) 'MP Call Communications Data Bill 'Honeypot for Hackers and Criminals', 31 October, *The Guardian*. Available at: http://www.theguardian.com/technology/2012/oct/31/communications-data-bill-honeypot-hackers-criminals [Accessed: March 2014].

'Terrorism Gang Jailed for Plotting to Blow Up London Stock Exchange', *The Telegraph*, (9 February 2012), Available at: http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9072455/Terrorism-gang-jailed-for-plotting-to-blow-up-London-Stock-Exchange.html [Accessed: March 2014].

UMPF, Available at: http://www.umpf.co.uk/blog/social-media/social-media-usage-in-the-uk-the-findings/ [Accessed: March 2014].

Valls, Maunal. Cited in: Marchive, Valery (2013) 'France Considers Stepping Up Internet Monitoring to Fight Terrorism', *Vive la Tech*, 4 June, Available at: http://www.zdnet.com/france-considers-stepping-up-internet-monitoring-to-fight-terrorism-7000016315/, [Accessed: March 2014].

Ward, Mark (2014) 'UK Government Tackles Wrongly Blocked Websites', *BBC News*, Available at: http://www.bbc.co.uk/news/technology-25962555 [Accessed: March 2014].

Ward, Victoria (2012) 'Website Allowed Terrorists to Come Together to Plot Carnage', *The Telegraph*, 1 February, Available at: http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9054531/Website-allowed-terrorists-to-come-together-to-plot-carnage.html [Accessed: March 2014].

Whitehead, Tom (2013) 'Hoax Bomber Researched Real Bombs Just Months after Leaving Prison', *The Telegraph*, 30 January, Available at: http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9837261/Hoax-bomber-researched-real-bombs-just-months-after-leaving-prison.html [Accessed: March 2014].

YouTube Community Guidelines, Available at: http://www.youtube.com/t/community_guidelines [Accessed: March 2014].

'2014 Video Share Websites Comparisons', *Top Ten Reviews*, (January 2014) Available at: http://video-share-review.toptenreviews.com/ [Accessed: March 2014].

'Youtube Stats: Sites Has 1 Billion Active Users Each Month', Huffington Post, (20 March 2013) Available: www.huffingtonpost.com/2013/03021/youtube-statsn2922543.html [Accessed: March 2014].

Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it
Quilliam, May 2014

ISBN number: 978--1--906603--99--1

Disclaimer: The views of individuals and organisations used in this report do not necessarily reflect those of Quilliam

QUILLIAM